Tiger Lake-H Intel® Converged Security and Management Engine Firmware 15.0

Corporate Firmware Bring Up Guide

March 2020

Revision 0.8

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 lTigernse 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 INTL 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 notTiger. 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 notTiger.

The Tiger Lake Platform and Tiger 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 lTigernse and may only be used or copied in accordance with the terms of that lTigernse.

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 lTigernses 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 © 2014-2020, 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 10
- 1.5 Format and Notation 10
- 1.6 Kit Contents 11
- 1.7 External Hardware Requirements for Bring Up 15

2 Image Creation: Intel® Flash Image Tool 16
- 2.1 Start Intel®FIT 16
- 2.2 Step-by-Step Guide to Build SPI Flash Image with Intel® FIT Interface 16

3 Programming SPI Flash Devices and Checking Firmware Status 129
- 3.1 Flash Burner/Programmer 129
  - 3.1.1 In-Circuit SPI Flash Programming for CRB 129
- 3.2 Flash Programming Tool (Intel® FPT) 129
  - 3.2.1 Intel® FPT Windows* Version 130
- 3.3 Checking Intel® ME Firmware Status 130
- 3.4 Common Bring Up Issues and Troubleshooting Table 132

A Appendix — Flash Configurations 133

B Appendix — Intel® ICCS SKU Support Matrix 134

C Appendix — Boot Guard Configuration 136

D Appendix — Intel® Platform Trust Technology 138

E Appendix — Integrated Sensor Hub (ISH) Public Key Settings 139

Figures

Tables

1-1 Number Format Notation 10
1-2 Data Format Notation 10
1-3 Kit Contents 11
2-1 - Initial Screen Layout 17
2-2 - Build Settings 26
2-3 - Flash Layout 28
2-4 - Flash Settings 34
2-5 - Intel® ME Kernel 44
2-6 - Intel® AMT 48
2-7 - Platform Protection 56
2-8 - Integrated Clock Controller 62
2-9 - Networking & Connectivity 71
2-10- Internal PCH Buses 75
2-11- Power 80
2-12- Integrated Sensor Hub 82
2-13- Camera 84
2-14- Debug 85
2-15- CPU Straps 91
2-16- Flex I/O Straps 93
2-17- GPIO 114
2-18- Intel® Precise Touch and Stylus 120
2-19- Download and Execute 121
2-20- FW Update Image Build 123
2-21- Intel® FIT - Build Image 128
3-1 Common Bring Up Issues and Troubleshooting Table 132

Revision History

Document Number	Revision Number	Description	Revision Date
	0.7	Initial Release	November 2019
	0.8	Updated with latest UI changes	March 2020

§ §

1 Introduction

This document covers the Intel® Converged Security and Management Engine Firmware (Intel® ME) 15.0 - Consumer / Corporate Firmware bring up procedure. Intel® ME 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 **Tiger Lake-H / LP 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 Corporate 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 Corporate FW Release Notes (included with this Intel® ME Corporate 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 Tiger Lake LP/H 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®ME)
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.The end user may not be aware to the fact that the platform is managed by Intel® AMT.
Host or Host CPU	The processor that is running the operating system. This is different than the management processor running the Intel® 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® AMT Firmware	The Intel® AMT Firmware running on the embedded processor
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® ME	Intel® Converged Security and Management Engine: The embedded processor residing in the chipset MCP
Intel® MEBx	Intel® Management Engine BIOS Extensions
MECI	ME-VE Communication Interface
NVM	Non-Volatile Memory: A type of memory that will retain its contents even if power is removed. In the Intel® AMT current implementation, this is achieved using a FLASH memory device.
OOB Interface	Out Of Band interface: This is WSMAN interface over secure or non-secure TCP protocol.

Acronym or Term	Definition
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: • 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.
Un-configured state	The state of the Intel® Management Engine Firmware when it leaves the OEM factory. At this stage the Intel® Management Engine Firmware is not functional and must be configured.

1.3.3 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*
Tiger Lake Intel® Converged Security and Management Engine (Intel® CSME) and Embedded Controller Interaction Product Specification Revision 0.5	549024 / CDI
Intel® Converged Security and Management Engine BIOS Writers Guide	TBD / *
Intel® Converged Security and Management Engine (Intel® CSME) 15 SKU Firmware Corporate *Compliance Guide for Tiger Lake PCH-H/LP Chipset Family - Tiger Lake Platform Compliancy and Testing Guide - Revision x.x*	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 Corporate FW kit can be downloaded from VIP (https://platformsw.intel.com/). The contents of this kit are detailed below (Note that only key files are listed).

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

File or [Directory]	Content Description
[root]	Root directory
	This document
	How to program SPI device parameters and descriptor region details. Also contains a complete SPI Flash softstrap reference.
	How to program SPI device parameters and descriptor region details. Also contains a complete SPI Flash softstrap reference.
	BIOS image only for Intel CRB.
	Intel® LAN PHY LPT-H firmware image.
	Intel® LAN PHY LPT-H firmware image.
	Intel® ME firmware image (**Non Production FW Rom Bypass**) - supports **unfused** Kabylake PCH-LP Platform I/O MCP steppings: • Unfused (Super SKU) **Note: For PAVP Testing**, you must match Production FW with Production Part and Non Production FW with Non Production Parts.
	Intel® ME Software installation Guide.

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

File or [Directory]	Content Description
	XML file
	XML file
	ICC Tools User Guide
	Exe file
	Ini file
	Exe file
	CCT for EFI
	Sybase Open Watcom Public LTigernse version 1.0 document.
	System Tools User Guide
	Intel® Flash Image Tool (Intel® FIT)
	FITC Configuration XML file
	Binary containing the supported SPI parts
	Documentation listing the SPI parts supported by vscccommn.bin
	List of supported SPI Flash devices with specific Flash parameters
	Intel® FPT for DOS
	List of supported SPI Flash devices with specific Flash parameters
	Intel® FPT for EFI
	List of supported SPI Flash devices with specific Flash parameters

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

File or [Directory]	Content Description
	Intel® FPT for Windows*
	List of supported SPI Flash devices with specific Flash parameters
	Intel® FPT for Windows* (64-bit) OS
	FW Update Tool (EFI version)
	FW Update Tool (DOS version)
	FW Update Tool (Windows* version 32bit)
	FW Update Tool (Windows* version 64bit)
	Intel® Manifest Extension Utility (MEU) executable file that allows input of FW binary and outputs and independent updatable partition that is compressed and signed.
	Intel® ME Information Tool (DOS version)
	Intel® ME Information Tool (EFI version)
	Intel® ME Information Tool (Windows* version 32bit)
	Intel® ME Information Tool (Windows* version 64bit)

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

File or [Directory]	Content Description
	Intel®ME Manufacturing Tool (DOS version)
	Binary containing the supported SPI parts
	Documentation listing the SPI parts supported by vscccommn.bin
	Documentation listing the SPI parts supported by vscccommn.bin
	Intel®ME Manufacturing Tool (EFI version)
	Binary containing the supported SPI parts
	Intel®ME Manufacturing Tool (Windows* version 32bit)
	Binary containing the supported SPI parts
	Documentation listing the SPI parts supported by vscccommn.bin
	Intel®ME Manufacturing Tool (Windows* version 64bit)
	Binary containing the supported SPI parts
	Documentation listing the SPI parts supported by vscccommn.bin

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
Equipment: • Laptop or desktop that supports win32 applications **Purpose:** • Will run firmware image assembly and build process software.	**Equipment:** • (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 **Purpose:** • Will burn firmware images onto the target system Flash device(s).	**Equipment:** • A DOS Bootable USB Key (Size > 512 MB) **Purpose:** • Acting as a bootable device and will be used to run Intel® FPT (fpt.exe) directly on the system that is undergoing Bring Up process. • Or will be used to transfer a firmware image onto a Flash burner.

§ §

2 Image Creation: Intel® Flash Image Tool

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

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

Note: The Flash Image Tool may be updated throughout the release cycles. As a general rule, please ensure you use the tools, images and other content from the same kit and refrain from using different version tools.

2.1 Start Intel®FIT

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

Table 2-1. - Initial Screen Layout (Sheet 1 of 9)

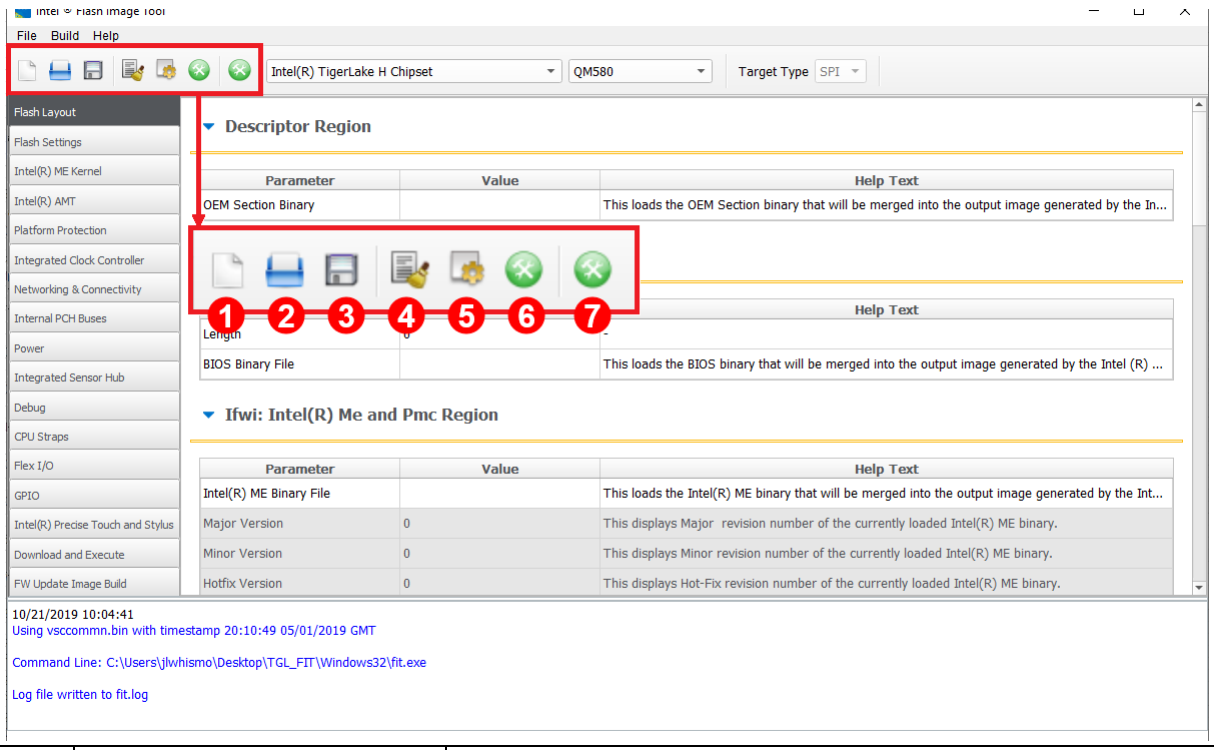
#	Label	Contents
		
1	**New**	This button labeled 'New' on rollover allows opening of a new session with default values
2	**Open**	This button labeled 'Open' on rollover allows opening of an xml or bin file
3	**Save**	This button labeled 'Save' on rollover allows saving of xml file
4	**Clear Console**	This button labeled 'Clear Console' clears the console area (see page 23)
5	**Build Settings**	This button labeled 'Build Settings' brings up the build settings popup Window see (Table 2-2)
6	**Build Image**	This button labeled 'Build Image' on rollover allows build of the image
7	**Build Image For FWUpdate**	This button labeled 'Build Image For FWUpdate' allows the user to build separate firmware update binaries.

Table 2-1. - Initial Screen Layout (Sheet 2 of 9)

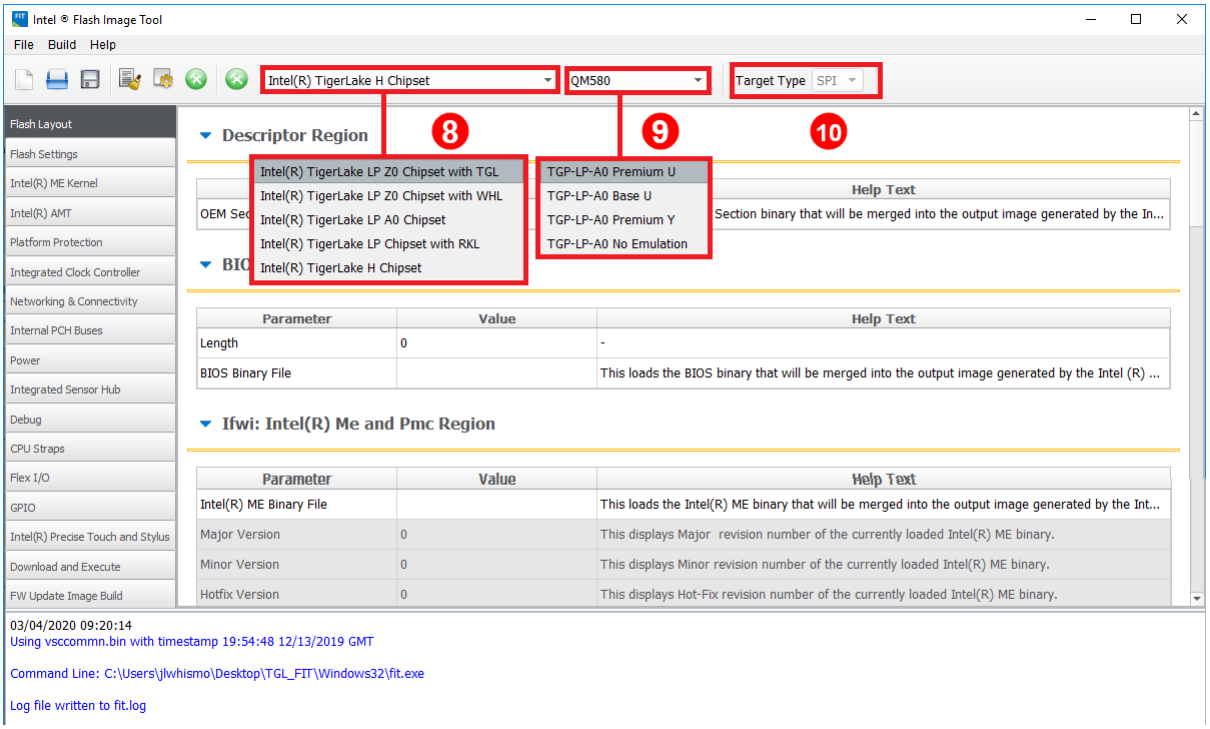
#	Label	Contents
		
8	**Drop Down Selector**	This drop down allows selection of platform
9	**Drop Down Selector**	This drop down allows selection of SKU within platform selected
10	**Indicator**	This displays the type of Boot Media Target based on FW being used

Table 2-1. - Initial Screen Layout (Sheet 3 of 9)

#	Label	Contents

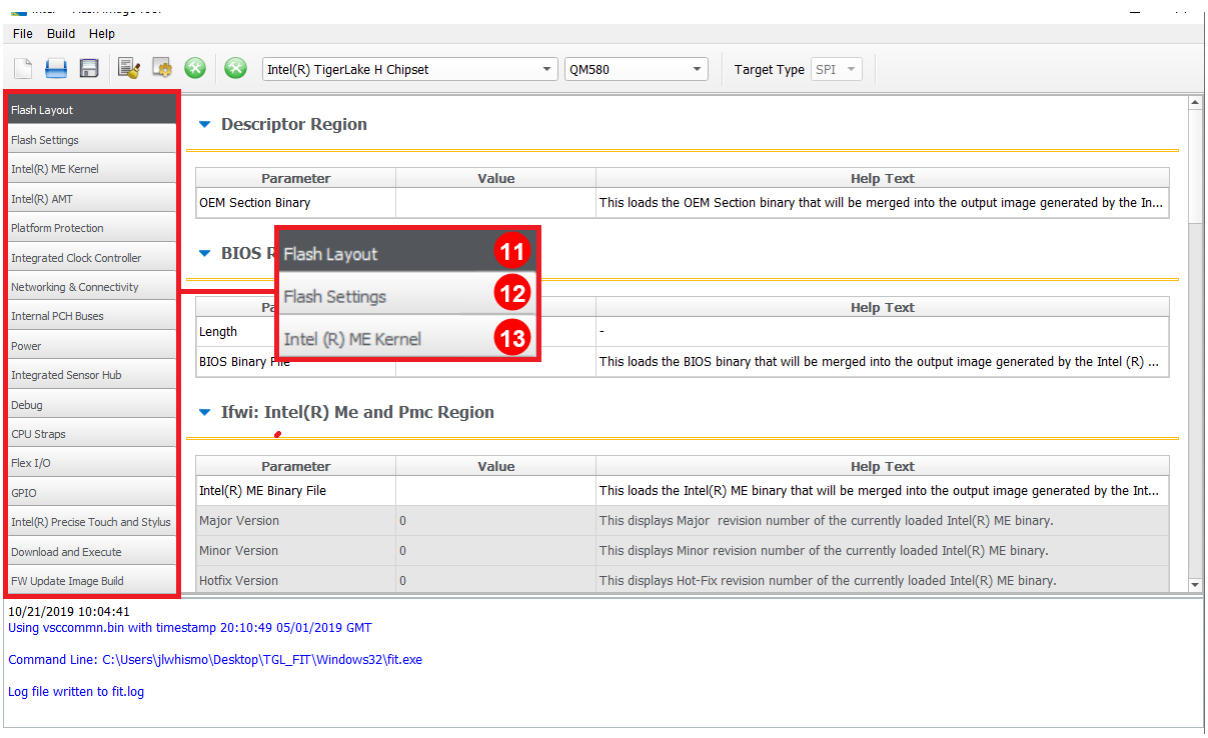


Table 2-1. - Initial Screen Layout (Sheet 4 of 9)

#	Label	Contents
11	**Flash Layout Tab**	Flash Layout which contains (see Table 2-3): • Descriptor Region • BIOS Region • IFWI: Intel® ME and PMC Region • EC Region • GBE Region • SubPartitions • PDR Region
12	**Flash Settings Tab**	Flash Settings which contains (see Table 2-4): • Flash Components • Host CPU/ BIOS Master Access • Intel® ME Master Access • GBE Master Access • EC Master Access • Flash Configuration • Legacy VSCC Table - VSCC Entries • BIOS Configuration • FPF Configuration
13	**Intel® ME Kernel Tab**	Intel® ME Kernel which contains (see Table 2-5): • Processor • Intel® ME Firmware Update • Image Identification • Firmware Diagnostics • End of Manufacturing Configuration • MCTP Configuration • Intel® ME Boot Configuration • Intel® ME Assisted Boot Configuration • Reserved

Table 2-1. - Initial Screen Layout (Sheet 5 of 9)

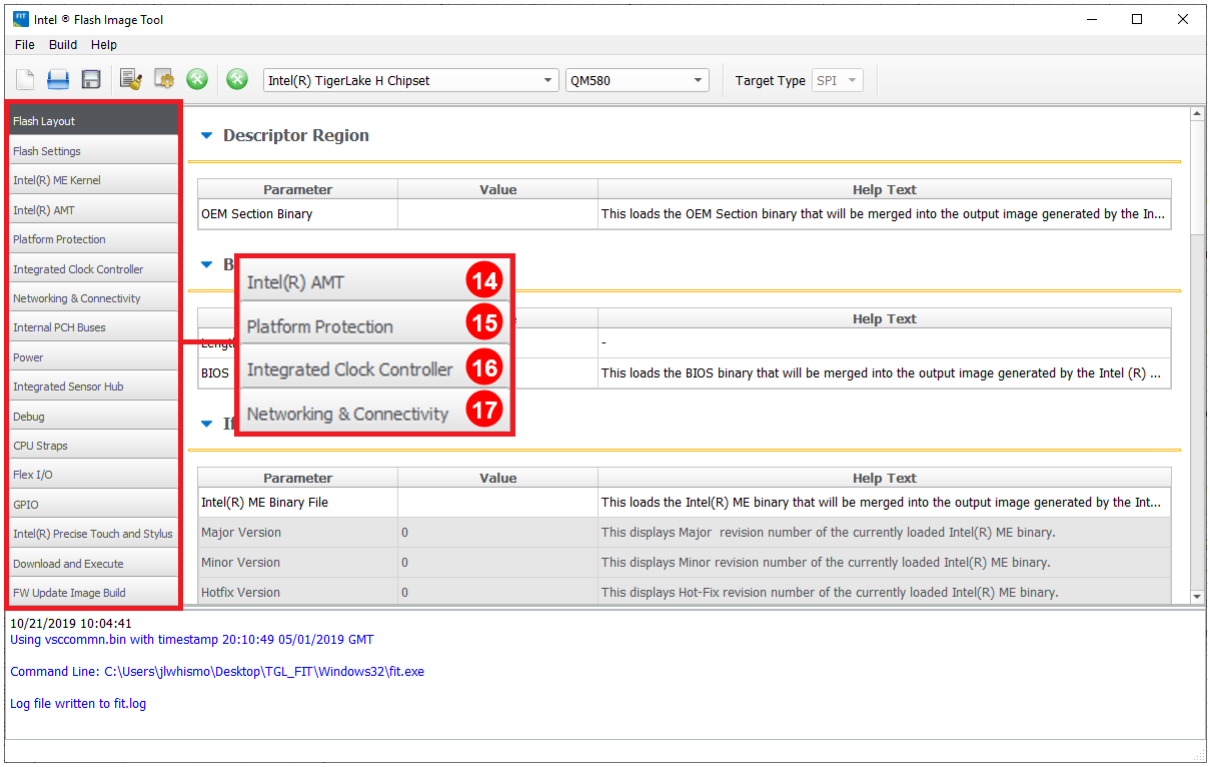
#	Label	Contents
		
14	**Intel® AMT Tab**	Intel® AMT which contains (see Table 2-6): • Intel® AMT Configuration • KVM Configuration • Provisioning Configuration • OEM Customizable Certificates (1, 2, 3) • OEM Default Certificates (1, 2, 3, 4, 5) • Redirection Configuration • TLS Configuration
15	**Platform Protection Tab**	Platform Protection which contains (see Table 2-7): • Content Protection • Graphics uController • Hash Key Configuration for Bootguard / ISH • Boot Guard Configuration • Type-C Firmware Anti-Rollback Configuration • Intel® PTT Configuration • TPM Over SPI Bus Configuration • BIOS Guard Configuration • TXT Configuration • Crypto Hardware Support • Platform Trusted Device Setup Support • Intel FPF Anti-Rollback Configuration
16	**Integrated Clock Controller Tab**	Integrated Clock Controller which contains (see Table 2-8): • Integrated Clock Controller Policies • Profiles

Table 2-1. - Initial Screen Layout (Sheet 6 of 9)

#	Label	Contents
17	**Networking & Connectivity Tab**	Networking & Connectivity which contains (see Table 2-9): • Platform vPro NIC • Docking Station • Wired LAN Configuration • Wireless LAN Configuration • Time Sensitive Networking Configuration

Table 2-1. - Initial Screen Layout (Sheet 7 of 9)

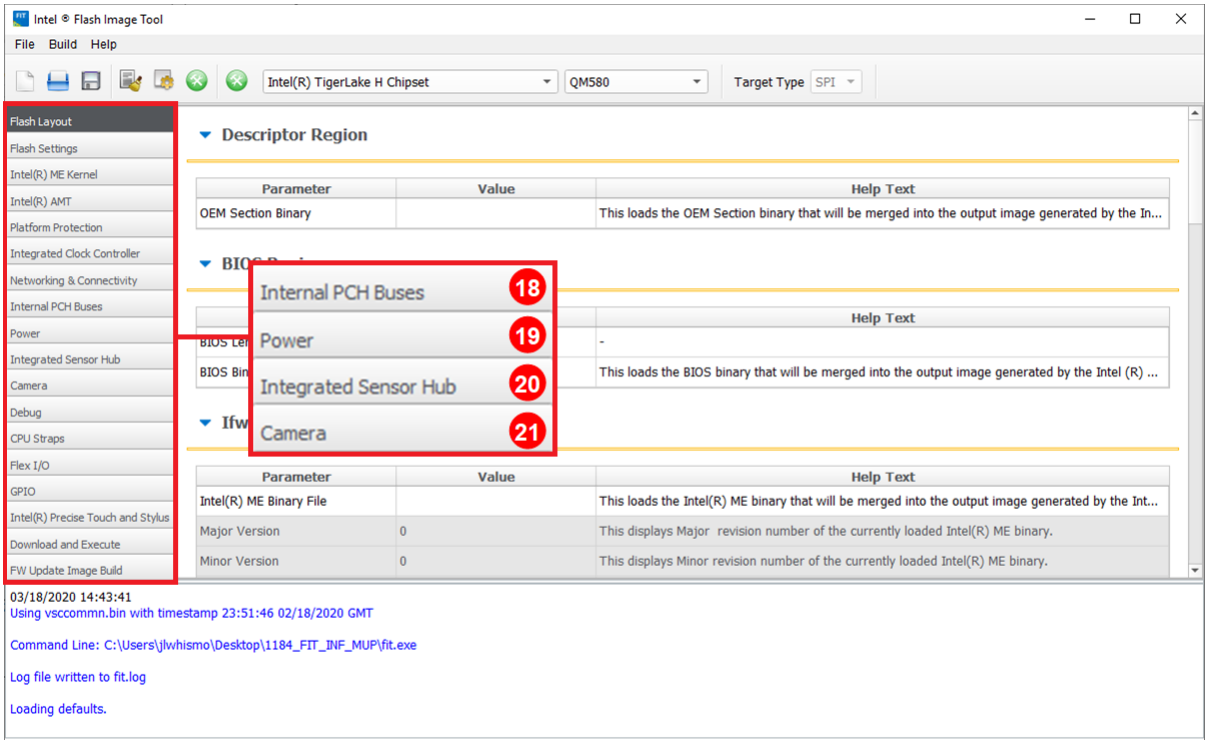
#	Label	Contents
		
18	**Internal PCH Buses Tab**	Internal PCH Buses which contains (see Table 2-10): • PCH Timer Configuration • SMBus / SMLink Configuration • DMI Configuration • OPI /DMI Configuration • eSPI Configuration
19	**Power Tab**	Power which contains (see Table 2-11): • Platform Power • Deep Sx • PCH Thermal Reporting
20	**Integrated Sensor Hub Tab**	Integrated Sensor Hub which contains (see Table 2-12): • Integrated Sensor Hub • ISH Image • ISH Data
21	**Camera**	• IPU Security (see Table 2-13):

Table 2-1. - Initial Screen Layout (Sheet 8 of 9)

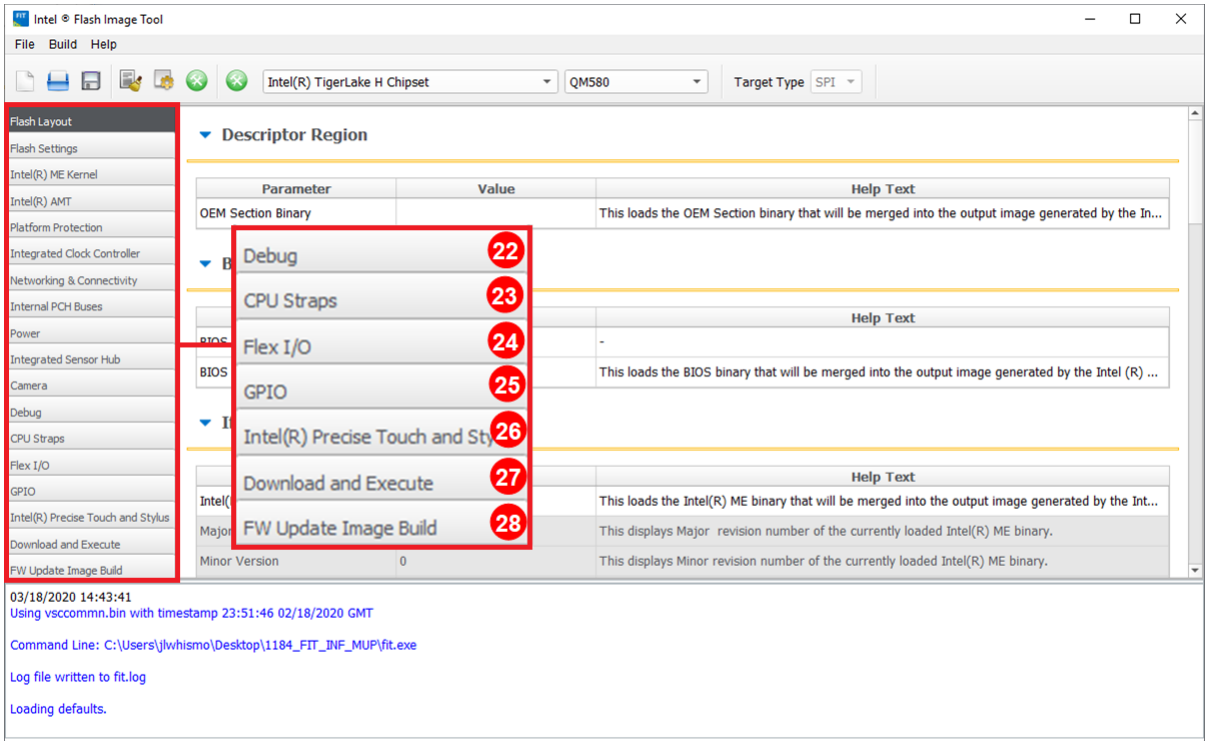
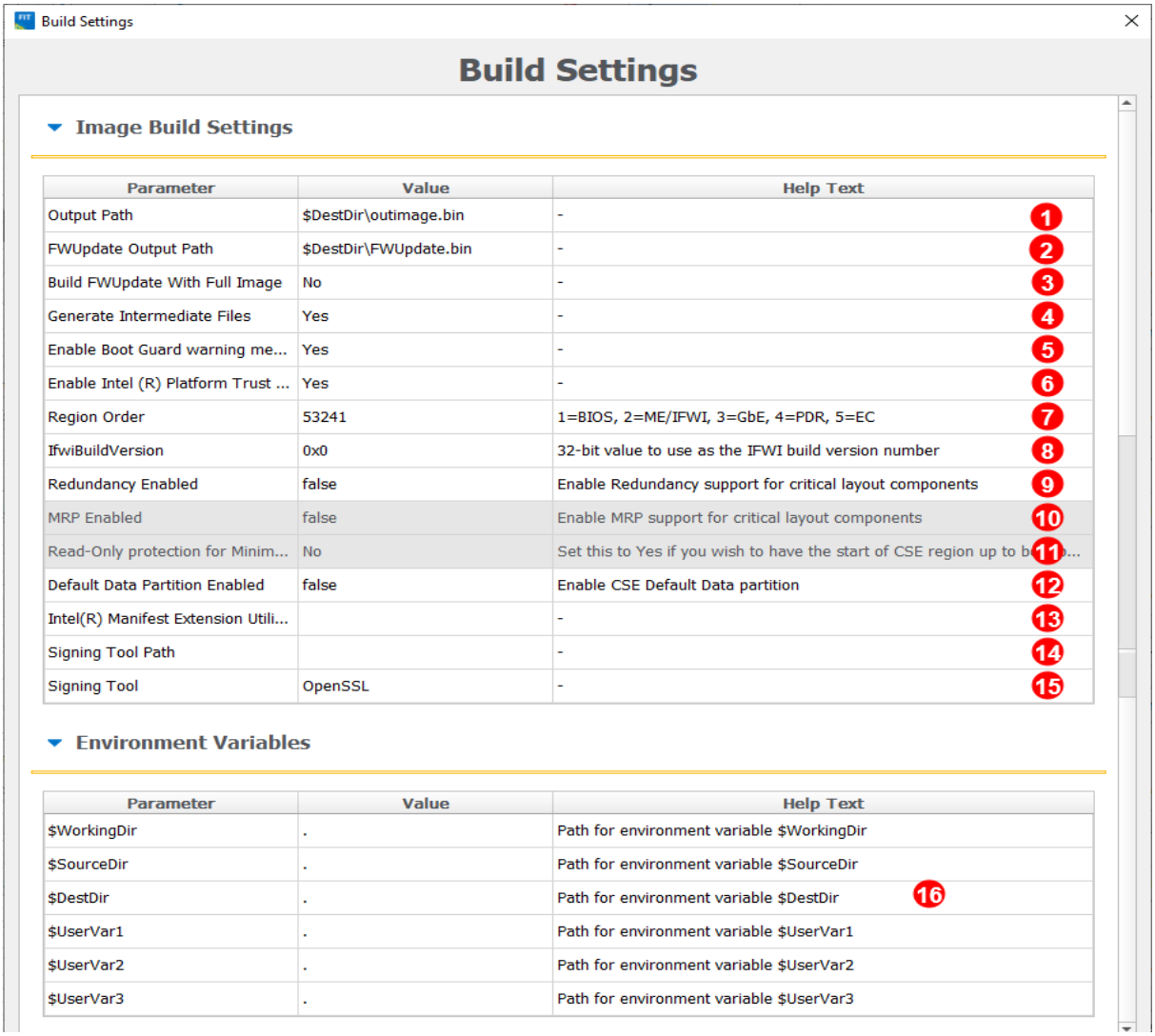
#	Label	Contents
		
22	**Debug Tab**	• Debug which contains (see Table 2-14): • IDLM • Delayed Authentication Mode Configuration • Intel® Trace Hub Technology • Intel® ME Firmware Debugging Overrides • Direct Connection Interface Configuration • eSPI Feature Overrides • Early USB DBC over Type-A Configuration • TRC Emulation
23	**CPU Straps Tab**	CPU Straps which contain a detailed list of parameters (see Table 2-14): • CPU Straps
24	**Flex I/O Tab**	Flex I/O which contains (see Table 2-15) • PCIe Lane Reversal Configuration • PCIe Port Configuration • SATA / PCIe Combo Port Configuration • USB3 Port Configuration • USB2 Port Configuration • Type-C Subsystem Configuration • Thunderbolt Configuration • Power Delivery PD Controller Configuration

Table 2-1. - Initial Screen Layout (Sheet 9 of 9)

#	Label	Contents
25	**GPIO Tab**	GPIO which contains (see Table 2-16): • ME Feature Pins • Touch Controller Pins • GPIO VCCIO Voltage Control • Thunderbolt LSx/BSSB-LS Configuration
26	**Intel® Precise Touch and Stylus**	Intel® Precise Touch and Stylus which contains (see Table 2-17): • Integrated Touch Configuration • Intel® Integrated Touch and Stylus Configuration
27	**Download and Execute**	Download and Execute which contains (see Table 2-18): • DnX Configuration • USB Descriptor
28	**FW Update Image Build**	FW Update Image Build which contains (see Table 2-19): • ME Image • PMC Image • OEM KM Image • IOM Image • NPHY Image • TBT Image • ISH Image • INUIT Image • PCHC Image
	Console Window Area	Displays opening messages, log file entries, and build activity messages

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

Click on Build Button in the top menu bar> Build Settings window pop up is displayed:



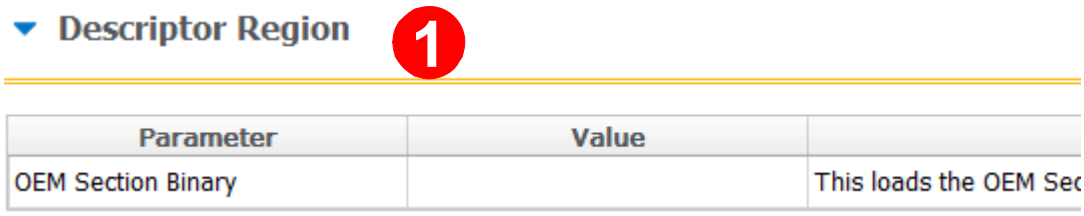
#	Parameter	CRB	Values
1	**Output Path**		Double click to the right of outimage.bin and click to get browse button to specify path and name of file to create for the build - default is outimage.bin in the same folder as Intel® FIT tool
2	**FWUpdate Output Path**		Double click to the right of FWUpdate.bin and click to get browse button to specify path and name of file to create for the build - default is FWUpdate.bin in the same folder as Intel® FIT tool
3	**Build FWUpdate With Full Image**	No	Yes/No - No is default

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

Click on Build Button in the top menu bar> Build Settings window pop up is displayed:			
4	**Generate Intermediate Files**	Yes	Yes/No - Yes is default
5	**Enable Boot Guard warning message at build time**	Yes	Yes/No - Yes is default
6	**Enable Intel (R) Platform Trust Technology warning message at build time**	Yes	Yes/No - Yes is default
7	**Region Order**	Yes	53241 - is default
8	**IFWI Build Version**	Yes	32-bit value to use as the IFWI build version number.
9	**Redundancy Enabled**	Yes	This setting enabled Redundancy support for critical layout components.
10	**MRP Enabled**	false	Enable MRP support for critical layout components.
11	**Read-Only protection for Minimal Recovery code**	No	Set this to Yes if you want to have the start of the Intel® CSE to be read-only at boot.
12	**Default Data Partition Enabled**	Yes	Enable Intel® CSME Default Data partition
13	**Intel® Manifest Extension Utility Path**	Yes	
14	**Signing Tool Path**	Yes	
15	**Signing Tool**	Yes	
16			$WorkingDir and $DestDir can be left at the default '.' Click on $SourceDir Value field and type in path where the Image Components are located for the Manageability Engine kit

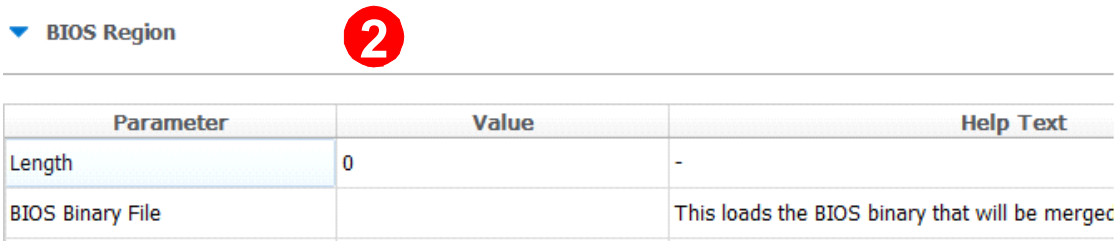
Table 2-3. - Flash Layout (Sheet 1 of 6)

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



#	Parameter	Platform	Settings
1	**OEM Section Binary** This loads the OEM Section binary that will be merged into the output image generated by the Intel® FIT tool.	TGL-H	OEM Binary (optional)

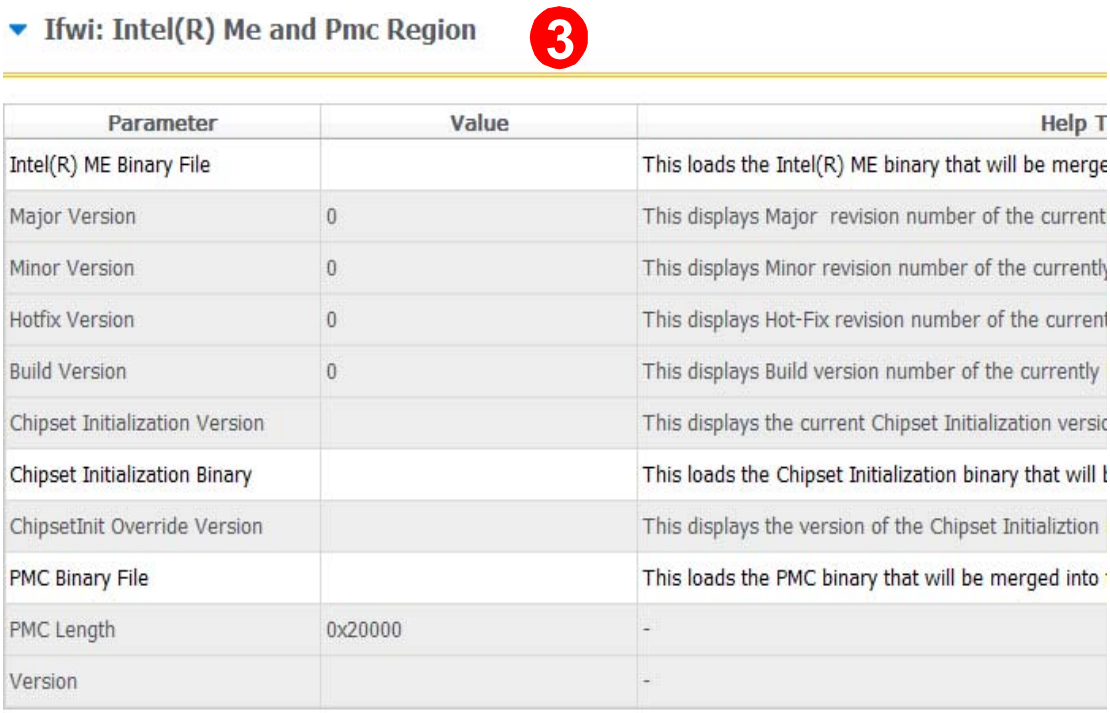
Click on Flash Layout in the left tabs menu> BIOS Region is expanded by default:



#	Parameter	Platform	Settings
2	**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.	TGL-H	biosimage.bin

Click on Flash Layout in the left tabs menu> Ifiw: Intel® ME and PMC Region is expanded by default:

Table 2-3. - Flash Layout (Sheet 2 of 6)



Ifwi: Intel(R) Me and Pmc Region 3

Parameter	Value	Help T
Intel(R) ME Binary File		This loads the Intel(R) ME binary that will be merge
Major Version	0	This displays Major revision number of the current
Minor Version	0	This displays Minor revision number of the currently
Hotfix Version	0	This displays Hot-Fix revision number of the current
Build Version	0	This displays Build version number of the currently
Chipset Initialization Version		This displays the current Chipset Initialization versic
Chipset Initialization Binary		This loads the Chipset Initialization binary that will l
ChipsetInit Override Version		This displays the version of the Chipset Initializtion
PMC Binary File		This loads the PMC binary that will be merged into
PMC Length	0x20000	-
Version		-

#	Parameter	Platform	Settings
3	**Ifwi: Intel® ME and PMC Region**		
	Intel® CSME 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 Intel® FIT tool. **Note:** You may choose to build the Intel® CSME Region only. To do so, the **Number of Flash Components** in **Flash Settings> Flash Components** must be set to 0. **Note:** If loading meimage.bin file, check that the ME region is enabled in tool before building image.	TGL-H	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.		
	Chipset Initialization Version - This displays the current Chipset Initialization version contained in the currently loaded Intel® CSME binary.		

Table 2-3. - Flash Layout (Sheet 3 of 6)

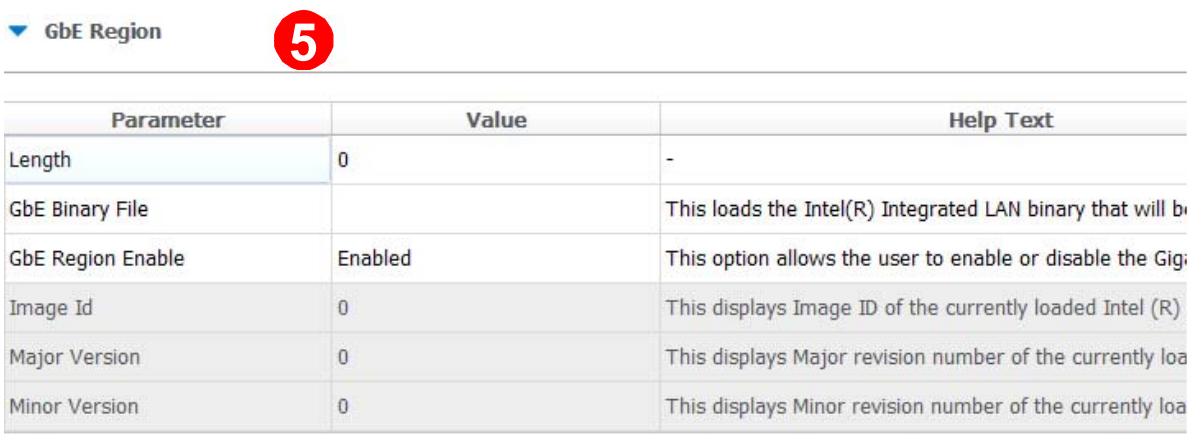
	Chipset Initialization Binary - This loads the Chipset Initialization binary that will be merged into the output image generated by the Intel® FIT. If specified, this will override the version contained in the Intel® CSME binary to align with the values programmed by BIOS. ***Note:*** When BIOS passes new Chipset Initialization settings to ME, a Global Reset is initiated (only required on the first boot, subsequent boots will not incur a global reset). This allows for the new settings to be stored in the ME Region and programmed into the PCH. This global reset can be avoided by loading the proper chipset initialization binary in to the ME Region when building the image that aligns with the values in BIOS. The Chipset Initialization Binary will be included in BIOS RC package. If BIOS contains an older version of Chipset Initialization settings ME will be updated at boot with the older settings regardless of any newer settings being present in firmware. In order to avoid this problem and the additional Global Reset customers should ensure that both BIOS and ME are updated with same Chipset Initialization binary.	TGL-H	Chipset.bin (Optional)
	ChipsetInit Override Version - This displays the version of the Chipset Initialization Binary override if specified.		
	PMC Binary File - This loads the PMC binary that will be merged into the output image generated by the Intel® FIT tool.	TGL-H	PMC.bin
	PMC Length - This displays the length of the PMC binary. ***Note:*** This value will be automatically populated by Intel® FIT during image build.		
	Version - This displays the version of PMC		
Click on Flash Layout in the left tabs menu> EC Region is expanded by default:			

EC Region 4

Parameter	Value	Help Text
Length	0	-
EC Binary File		This loads the Embedded Controller binary used for eSPI that will
EC Region Enable	Disabled	This option allows the user to enable or disable the Embedded Co
EC Region Pointer File		This loads a binary containing the 16 byte value to be written in th

#	Parameter	Platform	Settings
4	**EC Region**	TGL-H	0
	EC Region - Length ***Note:*** This value will be automatically populated by Intel® FIT during image build.		
	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.	TGL-H	EC Binary
	EC Region Enable **Values: Enabled / Disabled** This option allows the user to enable or disable the Embedded Controller data region.	TGL-H	Enabled
	EC Region Pointer File This loads a binary file containing the 16 byte Embedded Controller pointer value at the start of the flash descriptor	TGL-H	EC Pointer Binary
Click on Flash Layout in the left tabs menu> GbE Region is expanded by default:			

Table 2-3. - Flash Layout (Sheet 4 of 6)

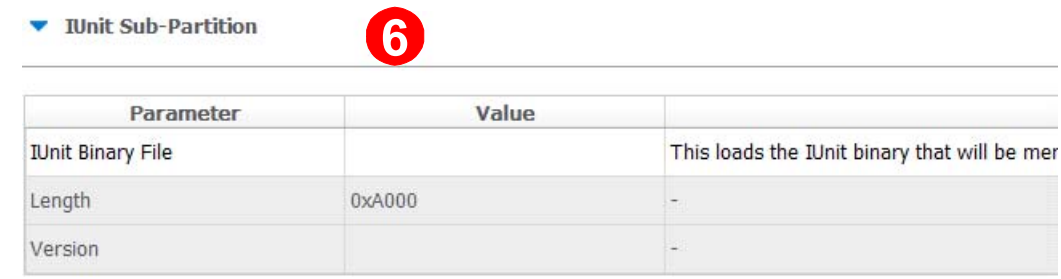


GbE Region 5

Parameter	Value	Help Text
Length	0	-
GbE Binary File		This loads the Intel(R) Integrated LAN binary that will b
GbE Region Enable	Enabled	This option allows the user to enable or disable the Gig
Image Id	0	This displays Image ID of the currently loaded Intel (R)
Major Version	0	This displays Major revision number of the currently loa
Minor Version	0	This displays Minor revision number of the currently loa

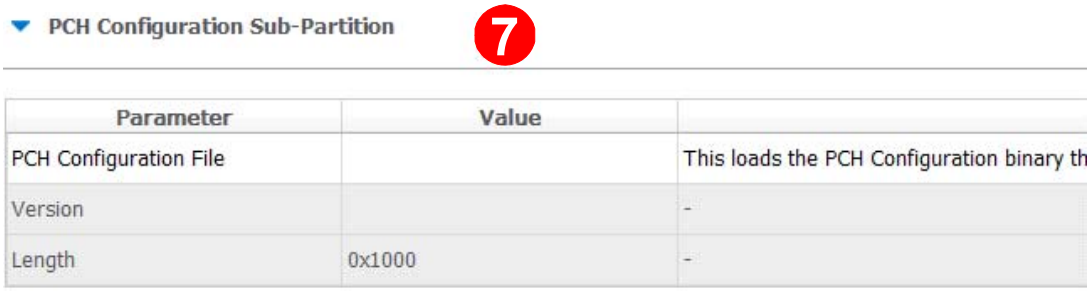
#	Parameter	Platform	Settings
5	**GbE Region** This loads the Intel® Integrated LAN binary that will be merged into the output image generated by the Intel® FIT tool.		
	GbE Region - Length ***Note:*** This value will be automatically populated by Intel® FIT during image build.		
	GbE Binary File Navigate 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.	TGL-H	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 MAC SMBus Address: No** **Intel® PHY over PCIe Enabled: No** **LAN PHY Power Control GDP11 Signal Configuration: Enable as GDP11**	TGL-H	Enabled
	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.		
Click on Flash Layout in the left tabs menu> IUnit Sub-Partion is expanded by default:			

Table 2-3. - Flash Layout (Sheet 5 of 6)



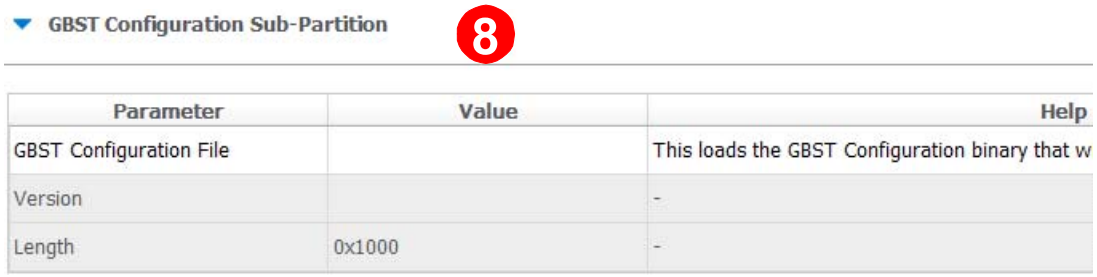
#	Parameter	Platform	Settings
6	**IUNIT Sub-Partition Binary** This loads the IUnit Sub Partition binary that will be merged into the output image generated by the Intel® FIT tool.	TGL-H	Iunit.bin (Optional)
	Length - This displays the length of the IUNIT Sub-Partition. ***Note:*** This value will be automatically populated by Intel® FIT during image build.		
	Version - This displays the version number of the IUNIT Sub-Partition		

Click on Flash Layout in the left tabs menu> PCH Configuration Sub-Partion is expanded by default:



#	Parameter	Platform	Settings
7	**PCH Configuration Sub-Partition** 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.	TGL-H	PCHC.bin
	Version - This displays the version number of the PCHC Configuration Sub-Partition		

Click on Flash Layout in the left tabs menu> GBST Configuration Sub-Partion is expanded by default:

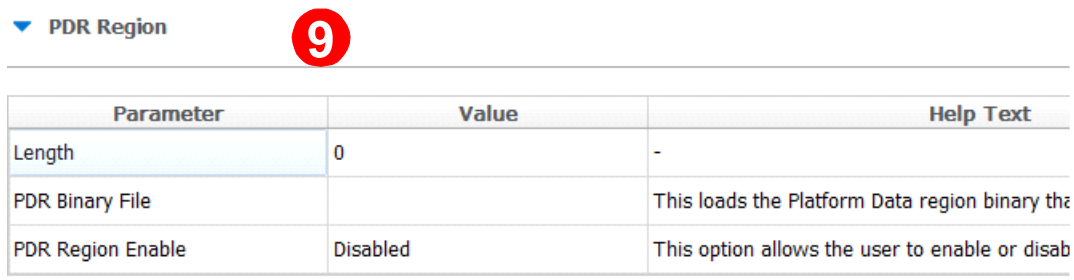


#	Parameter	Platform	Settings

Table 2-3. - Flash Layout (Sheet 6 of 6)

8	**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.		
	GBST Configuration File Navigate to path to load GBST.bin file. This loads the GBST Configuration binary.	TGL-H	GBST.bin (Optional)
	Version - This displays the version number of the GBST Configuration Sub-Partition		
	Length - This displays the length of the GBST Configuration Sub-Partition. ***Note:*** This value will be automatically populated by Intel® FIT during image build.		

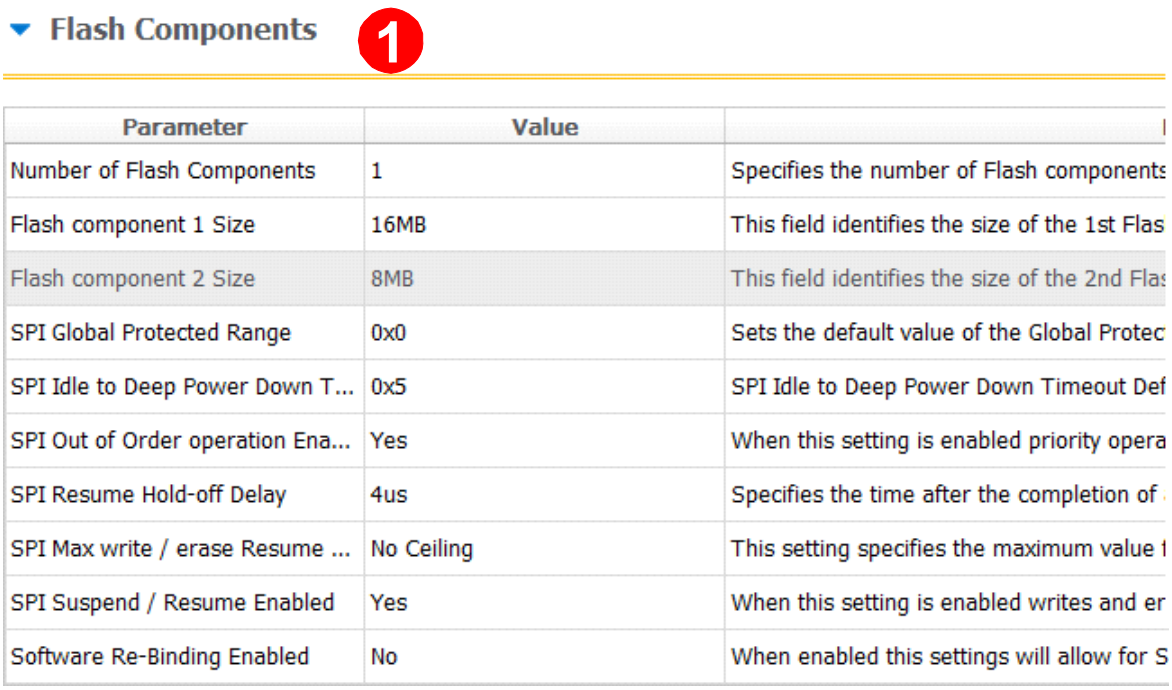
Click on Flash Layout in the left tabs menu> PDR Region is expanded by default:



#	Parameter	Platform	Settings
9	**PDR Region -** This loads the Platform Data region binary that will be merged into the output image generated by the Intel® FIT tool.		
	PDR Region - Length Region is disabled by default. Displays Region size information when **Binary input file** is specified.		
	PDR Binary File Navigate to path to load pdrimage.bin file if required and available.	TGL-H	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.	TGL-H	Disabled

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

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



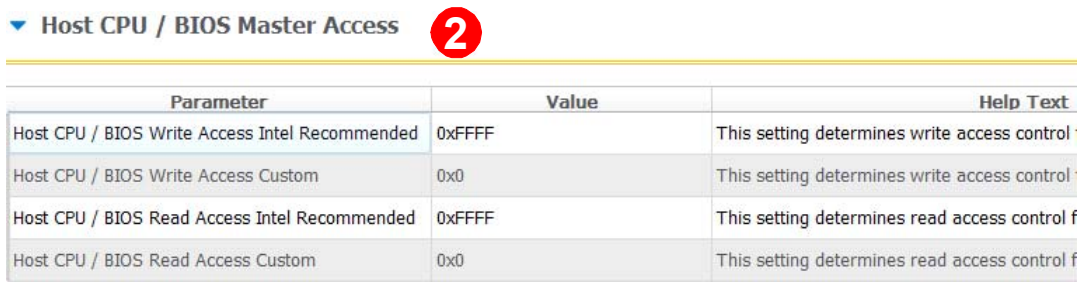
Flash Components

Parameter	Value	
Number of Flash Components	1	Specifies the number of Flash components
Flash component 1 Size	16MB	This field identifies the size of the 1st Flas
Flash component 2 Size	8MB	This field identifies the size of the 2nd Flas
SPI Global Protected Range	0x0	Sets the default value of the Global Protec
SPI Idle to Deep Power Down T...	0x5	SPI Idle to Deep Power Down Timeout Def
SPI Out of Order operation Ena...	Yes	When this setting is enabled priority opera
SPI Resume Hold-off Delay	4us	Specifies the time after the completion of
SPI Max write / erase Resume ...	No Ceiling	This setting specifies the maximum value t
SPI Suspend / Resume Enabled	Yes	When this setting is enabled writes and er
Software Re-Binding Enabled	No	When enabled this settings will allow for S

#	Parameter	Platform	Settings
1	**Flash Components**		
	Number of Components **Values: 0, 1, 2 -** This setting configures the total number of flash components for the platform. **Note:** Choosing a selection of '0' part will cause the Intel® FIT tool to build an output image containing only the Intel® ME region.	TGL-H	1
	Flash component 1 Size **Values: 512KB, 1MB, 2MB, 4MB, 8MB, 16MB, 32MB, 64MB** - This setting determines the size of Flash component 1 for the platform image.	TGL-H	32MB
	Flash component 2 Size **Values: 512KB, 1MB, 2MB, 4MB, 8MB, 16MB, 32MB, 64MB** - This setting determines the size of Flash component 2 for the platform image. **Note:** This setting is only applicable when the Number of Flash Components option is set to '2'.	TGL-H	Greyed Out
	SPI Global Protected Range - This sets the default value of the Global Protected Range register in the SPI Flash Controller.	TGL-H	0x0
	SPI Idle to Deep Power Down Timeout - This sets SPI Idle to Deep Power Down Timeout Default Specifies the time in microseconds that the Flash Controller waits after all activity is idle before commanding the flash devices to Deep Power down, time = 2^N microseconds.	TGL-H	0x5
	SPI Out of Order operation Enabled - When this setting is enabled priority operations may be issued while waiting for write / erase operations to complete on the flash device. When this setting is disabled all write / erase type operations in order.	TGL-H	Yes
	SPI Resume Hold-off Delay - This specifies the time after the completion of a pri_op before the flash controller sends the resume instruction. If a new pri_op is eligible to be issued prior to the end of this delay time then the pri_op is issued and the timer is reinitialized to tRHD. 3-bit field encodes count with range 0-7. tRHD = count * 2us.	TGL-H	4us

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

	SPI Max write / erase Resume to Suspend intervals - This setting specifies the maximum value for the write and erase Resume to Suspend intervals.	TGL-H	No Ceiling
	SPI Suspend / Resume Enabled - When this setting is enabled writes and erases may be suspended to allow a read to be issued on the flash device. When this setting is disabled no transaction will be allowed to the busy flash device.	TGL-H	Yes
	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.	TGL-H	No
Click on Flash Layout in the left tabs menu> BIOS Region is expanded by default:			

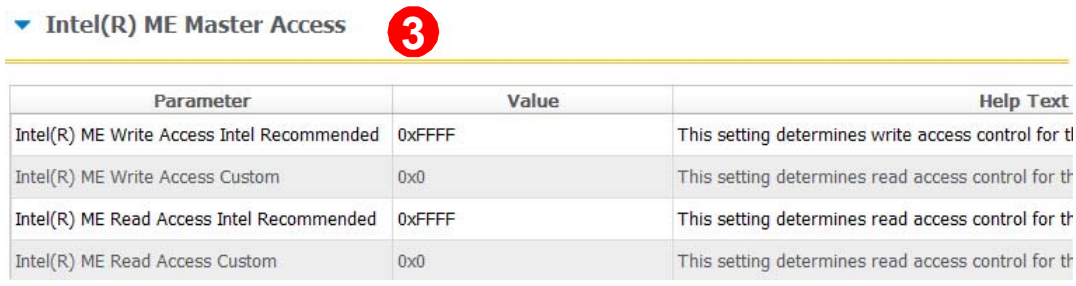


#	Parameter	Platform	Settings
2	**Host CPU / BIOS Master Access**		
	Host CPU / BIOS Write Access Intel Recommended **Values: 0xFfFF, 0x000A, 0x001A, 0x010A, 0x011A** - This setting determines write access control for the BIOS region. **0xFfFF** = Debug/Manufacturing **0x000A** = Production **0x001A** = Production with access to PDR (should ONLY be used if PDR region is implemented). **0x010A** = Production with access to EC **0x011A** = Production with access to EC and PDR **Custom** = User custom Host / BIOS Write Access values For further details on Region Access Control see Tiger Lake H SPI Programming guide further details.	TGL-H	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**	TGL-H	Hex Input

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

	Host CPU / BIOS Read Access **Values: 0xFFF, 0x00F, 0x01F, 0x10F, 0x11F** - This setting determines read access control for the BIOS region. **0xFFF** = 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 Tiger Lake H SPI Programming guide.	TGL-H	0xFFFF
	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**	TGL-H	Hex Input

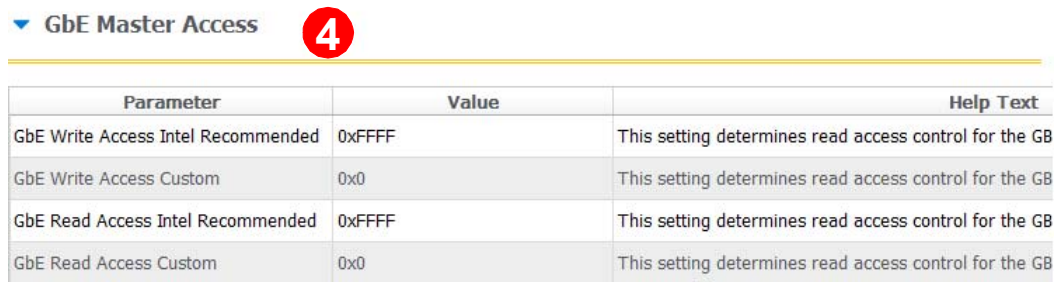
Click on Flash Settings in the left tabs menu> Intel® ME Master Access is expanded by default:



#	Parameter	Platform	Settings
3	**Intel® ME Master Access**		
	Intel® ME Write Access Intel Recommended **Values: 0xFFFF, 0x0004**- This setting determines write access control for the ME region. **0xFFFF** = Debug/Manufacturing **0x0004** = Production **Custom** = User custom Intel® ME Write Access values For further details on Region Access Control see Tiger Lake H SPI Programming guide further details.	TGL-H	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® ME Write Access Intel Recommended drop down menu. ***Warning:*** **Setting region access permission values outside of Intel recommendation could result in compromised platform security**	TGL-H	Hex Input

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

	Intel® ME Read Access Intel Recommended **Values: 0xFFFF, 0x000D** - This setting determines read access control for the ME region. **0xFFFF** = Debug/Manufacturing **0x000D** = Production **Custom** = User custom Intel® ME Read Access values For further details on Region Access Control see Tiger Lake LP SPI Programming guide further details.	TGL-H	0xFFFF 0xFFFF
	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® ME Read Access Intel Recommended drop down menu. ***Warning:*** **Setting region access permission values outside of Intel recommendation could result in compromised platform security**	TGL-H	Hex Input
Click on Flash Settings in the left tabs menu> GbE Master Access is expanded by default:			

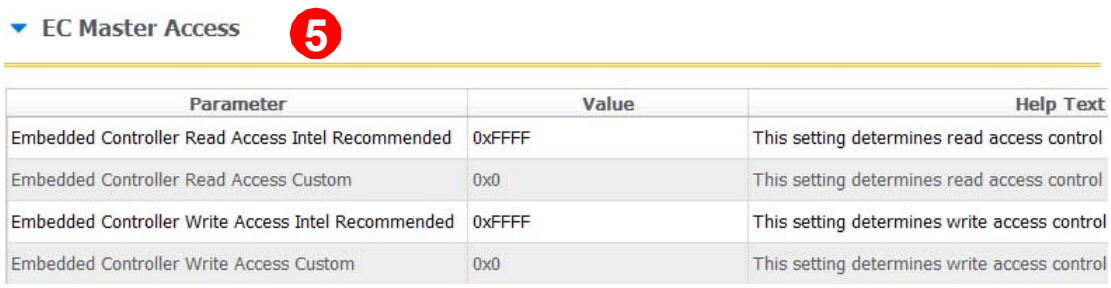


#	Parameter	Platform	Settings
4	**GbE Master Access**		
	GbE Write Access Intel Recommended **Values: 0xFFFF, 0x0008** - This setting determines write access control for the Gigabit Ethernet Region. **0xFFFF** = Debug/Manufacturing **0x0008** = Production **Custom** = User custom GbE Write Access values For further details on Region Access Control see Tiger Lake LP SPI Programming guide further details.	TGL-H	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**	TGL-H	Hex Input

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

	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 For further details on Region Access Control see Tiger Lake LP SPI Programming guide further details.	TGL-H	0xFFFF
	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**	TGL-H	Hex Input

Click on Flash Settings in the left tabs menu> EC Master Access is expanded by default:



#	Parameter	Platform	Settings
5	**EC Master Access**		
	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 For further details on Region Access Control see Tiger Lake LP SPI Programming guide further details.	TGL-H	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**	TGL-H	Hex Input

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

	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 For further details on Region Access Control see Tiger Lake LP SPI Programming guide further details.	TGL-H	0xFFFF
	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**	TGL-H	Hex Input

Click on Flash Layout in the left tabs menu> IUnit Sub-Partion is expanded by default:

Flash Configuration 6

Parameter	Value	Help Text
Dual I/O Read Enable	Yes	This soft-strap only has effect if Dual I/O Read is discovered as suppo
Dual Output Read Enable	Yes	This soft-strap only has effect if Dual Output Read is discovered as su
Fast Read Clock Frequency	50MHz	This setting allows customers to configure the flash component clock
Fast Read Supported	Yes	This setting allows customers to enable support for Fast Read capabil
Invalid Instruction 0	0x21	This setting allows customers to configure invalid instruction to protec
Invalid Instruction 1	0x42	This setting allows customers to configure invalid instruction to protec
Invalid Instruction 2	0x60	This setting allows customers to configure invalid instruction to protec
Invalid Instruction 3	0xAD	This setting allows customers to configure invalid instruction to protec
Invalid Instruction 4	0xB7	This setting allows customers to configure invalid instruction to protec
Invalid Instruction 5	0xB9	This setting allows customers to configure invalid instruction to protec
Invalid Instruction 6	0xC4	This setting allows customers to configure invalid instruction to protec
Invalid Instruction 7	0xC7	This setting allows customers to configure invalid instruction to protec
Quad I/O Read Enable	Yes	This soft-strap only has effect if Quad I/O Read is discovered as supp
Quad Output Read Enable	Yes	This soft-strap only has effect if Quad Output Read is discovered as s
Read ID and Read Status Clock Frequency	50MHz	This setting allows customers to configure the flash component clock
Write and Erase Clock Frequency	50MHz	This setting allows customers to configure the flash component clock

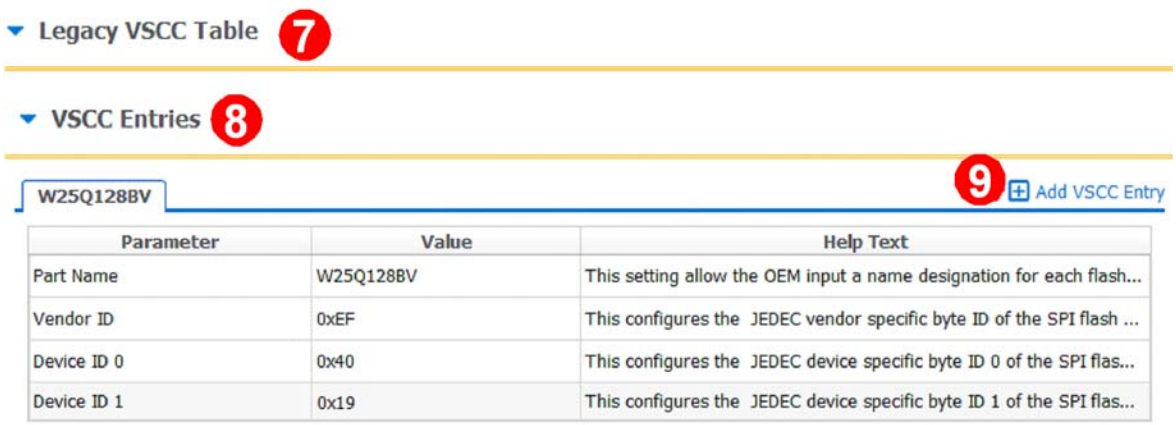
#	Parameter	Platform	Settings
6	**Flash Configuration**		

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

	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 Tiger Lake LP SPI Programming guide for further details.	TGL-H	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 Tiger Lake LP SPI Programming guide for further details.	TGL-H	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 Rocket Lake LP SPI Programming guide for further details. ***Note:*** The 100MHz frequency setting not valid on client platforms	TGL-H	50MHz
	Fast Read Supported **Values: Yes/No** - This setting allows the customer to enable support for Fast Read capabilities for flash components. See Tiger Lake LP SPI Programming guide for further details. **Note:** If fast read supported is set to **"No"** any changes made to Dual I/O, Quad I/O, Dual Output, or Quad Output will not be affected if set to yes. Fast read supported should also be set to enable frequencies greater than 20MHz.	TGL-H	Yes
	Invalid Instruction 0 - This setting allows the customer to configure invalid instruction to protect against Chip Erase. See Tiger Lake LP SPI Programming guide for further details. **Note:** This setting should be set to '0' if there are not Invalid instructions.	TGL-H	0x00000021
	Invalid Instruction 1 - This setting allows the customer to configure invalid instruction to protect against Chip Erase. See Tiger Lake LP SPI Programming guide for further details. **Note:** This setting should be set to '0' if there are not Invalid instructions.	TGL-H	0x00000042
	Invalid Instruction 2 - This setting allows the customer to configure invalid instruction to protect against Chip Erase. See Tiger Lake LP SPI Programming guide for further details. **Note:** This setting should be set to '0' if there are not Invalid instructions.	TGL-H	0x00000060
	Invalid Instruction 3 - This setting allows the customer to configure invalid instruction to protect against Chip Erase. See Tiger Lake LP SPI Programming guide for further details. **Note:** This setting should be set to '0' if there are not Invalid instructions.	TGL-H	0x000000AD
	Invalid Instruction 4 - This setting allows the customer to configure invalid instruction to protect against Chip Erase. See Tiger Lake LP SPI Programming guide for further details. **Note:** This setting should be set to '0' if there are not Invalid instructions.	TGL-H	0x000000B7
	Invalid Instruction 5 - This setting allows the customer to configure invalid instruction to protect against Chip Erase. See Tiger Lake LP SPI Programming guide for further details. **Note:** This setting should be set to '0' if there are not Invalid instructions.	TGL-H	0x000000B9
	Invalid Instruction 6 - This setting allows the customer to configure invalid instruction to protect against Chip Erase. See Tiger Lake LP SPI Programming guide for further details. **Note:** This setting should be set to '0' if there are not Invalid instructions.	TGL-H	0x000000C4
	Invalid Instruction 7 - This setting allows the customer to configure invalid instruction to protect against Chip Erase. See Tiger Lake LP SPI Programming guide for further details. **Note:** This setting should be set to '0' if there are not Invalid instructions.	TGL-H	0x000000C7
	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 Tiger Lake LP SPI Programming guide for further details.	TGL-H	Yes
	Quad Output Read Enabled **Values: Yes/No** - This setting allows the customer to enable support for Quad Output Read capabilities for flash components. See Tiger Lake LP SPI Programming guide for further details.	TGL-H	Yes

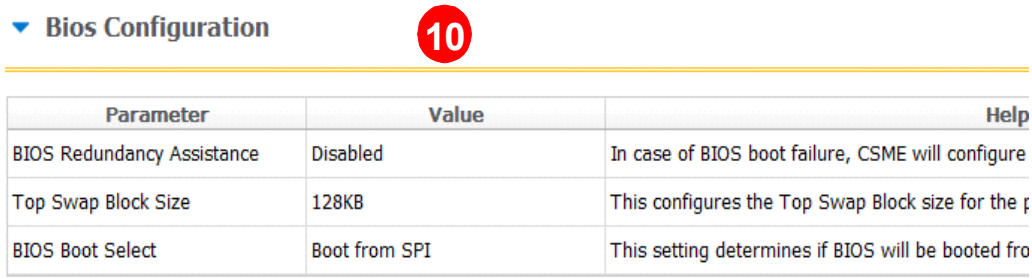
Table 2-4. - Flash Settings (Sheet 8 of 10)

	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 Rocket Lake LP SPI Programming guide for further details. ***Note:*** The 100MHz frequency setting not valid on client platforms	TGL-H	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 Rocket Lake LP SPI Programming guide for further details. ***Note:*** The 100MHz frequency setting not valid on client platforms	TGL-H	50MHz
Click on Flash Settings in the left tabs menu> Legacy VSCC Table is expanded by default:			

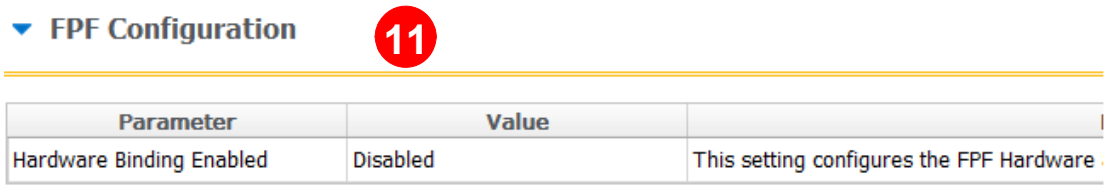


#	Parameter	Platform	Settings
7	**Legacy VSCC Table** **VSCC Entries**		
	W25Q128BV		
8	**VSCC Entries**	TGL-H	
	Name - This setting allow the OEM input a name designation for each flash component being used. **Note:** This is a free form entry field it does not affect actual flash component operation.	TGL-H	Winbond
	Vendor ID - This configures the JEDEC vendor specific byte ID of the SPI flash component. See Tiger Lake LP SPI Programming guide for further details.	TGL-H	0xEF
	device ID 0 - This configures the JEDEC device specific byte ID 0 of the SPI flash component. See Tiger Lake LP SPI Programming guide for further details.	TGL-H	0x40
	device ID 1 - This configures the JEDEC device specific byte ID 1 of the SPI flash component. See Tiger Lake LP SPI Programming guide for further details.	TGL-H	0x19
9	**+ Add VSCC Entry**		
Click on Flash Settings in the left tabs menu> BIOS Configuration is expanded by default:			

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

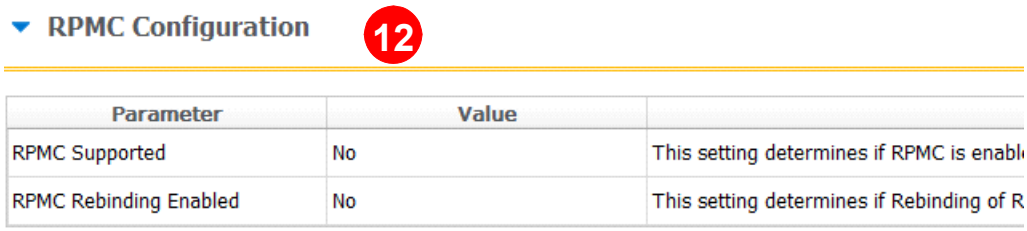


#	Parameter	Platform	
10	**BIOS Configuration**		
	BIOS Redundancy Assistance **Values: Enabled, Disabled** In cases of BIOS boot failure, Intel®CSME will configure the platform to boot with backup BIOS using Top Swap when this setting is enabled. ***Note:*** This option is only applicable when Boot Guard is enabled.	TGL-H	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 Tiger Lake LP Platform Controller Hub EDS.	TGL-H	128KB
	BIOS Boot Select **Values: Boot from SPI / Boot from LPC** This setting determines if BIOS will be booted from LPC or SPI.	TGL-H	Boot from SPI
Click on Flash Settings in the left tabs menu> BIOS Configuration is expanded by default:			



11	**FPF Configuration**		
	Hardware Binding Enabled **Values: Enabled / Disabled** This setting configures the FPF Hardware binding behavior for the platform image. If this setting is enabled FPF Hardware binding will occur when platform close manufacturing flow is executed with Intel® FPT. If this setting is disabled FPF Hardware binding will not take place when close manufacturing flow is executed. For Revenue parts this setting will be ignored and FPF Hardware binding will take place when close manufacturing flow is executed.	TGL-H	Disabled
Click on Flash Settings in the left tabs menu> RPMC Configuration is expanded by default:			

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



12	**RPMC Configuration**		
	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.	TGL-H	No
	RPMC Rebinding Enabled **Values: Yes / No** This setting determines if Rebinding of RPMC enabled SPI parts is enabled.	TGL-H	No

Table 2-5. - Intel® ME Kernel (Sheet 1 of 4)

Click on Intel® ME Kernel in the left tabs menu> Processor is expanded by default:

▼ Processor (1)

Parameter	Value	Help Text
Processor Emulation	No Emulation	-

#	Parameter	Platform	Settings
1	**Processor**		
	Processor Emulation **Values: No Emulation** **EMULATE Intel® vPro (TM) capable Processor** **EMULATE Intel® Core (TM) branded Processor** **EMULATE Intel® Celeron (R) branded Processor** **EMULATE Intel® Pentium (R) branded Processor** **EMULATE Intel® Xeon (R) branded Processor** **EMULATE Intel® Xeon (R) Manageability capable Processor** This setting determines processor type to be emulated on pre-production silicon. Set this parameter to the type of processor that the target system will use during production. This field will emulate that processor class for pre-production silicon. It is necessary to set this to Emulate Intel® vPro™ Processor in order to enable Intel® AMT.	TGL-H	EMULATE Intel® Core (TM) branded Processor

Click on Intel® ME Kernel in the left tabs menu> Intel® ME Firmware Update is expanded by default:

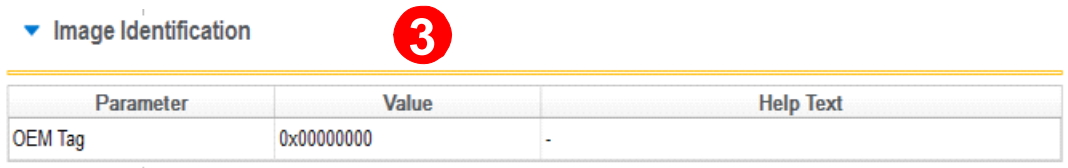
▼ Intel (R) ME Firmware Update (2)

Parameter	Value	Help Text
Firmware Update OEM ID	00000000-0000-0000-0000-000...	-
Hide MEBx Firmware Update ...	No	-
Intel(R) ME Region Flash Prot...	Yes	-

#	Parameter	Platform	Settings
2	**Intel® ME Firmware Update**		
	Firmware Update OEM ID - This setting allows configuration of an OEM unique ID to ensure that customers can only update their platform with images from the OEM of the platform.	TGL-H	0 string
	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.	TGL-H	No
	Intel® ME Region Flash Protection Override **Values: Yes/No** - This setting enables descriptor unlock of the Intel® CSME Region when the HMRFPO message is sent to firmware prior to BIOS End of POST.	TGL-H	Yes

Click on Intel® ME Kernel in the left tabs menu> Image Identification is expanded by default:

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

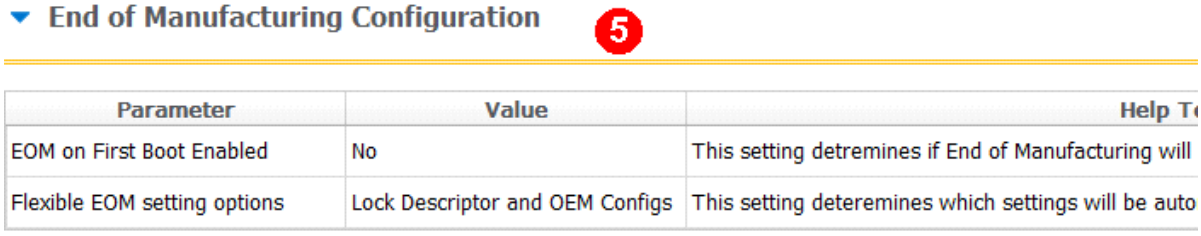


#	Parameter	Platform	Settings
3	**Image Identification**		
	OEM Tag - This is a free form 32bit field that allows the OEM to configure their own unique identifier in the firmware image.	TGL-H	0x00000000

Click on Intel® ME Kernel in the left tabs menu> Firmware Diagnostics is expanded by default:

#	Parameter	Platform	Settings
4	**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.	TGL-H	Disabled

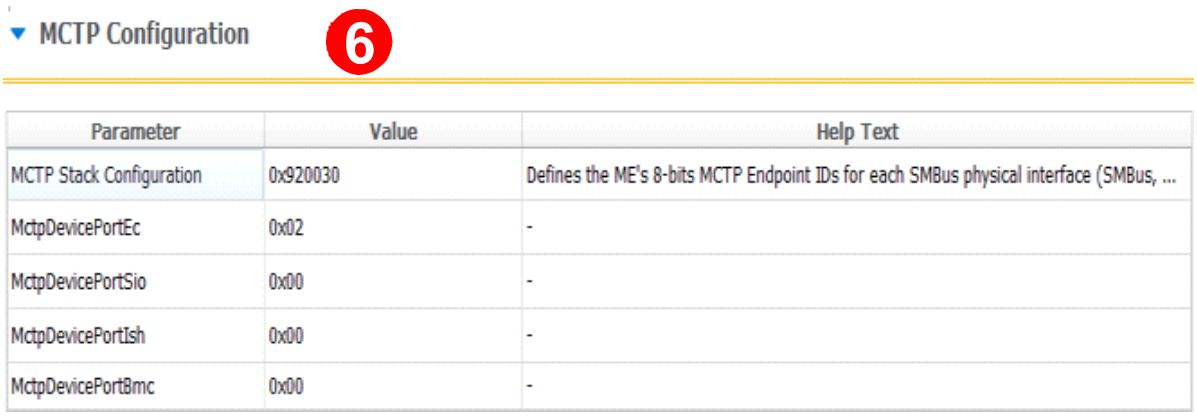
Click on Intel® ME Kernel in the left tabs menu> End of Manufacturing Configuration is expanded by default:



#	Parameter	Platform	Settings
5	**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.	TGL-H	No

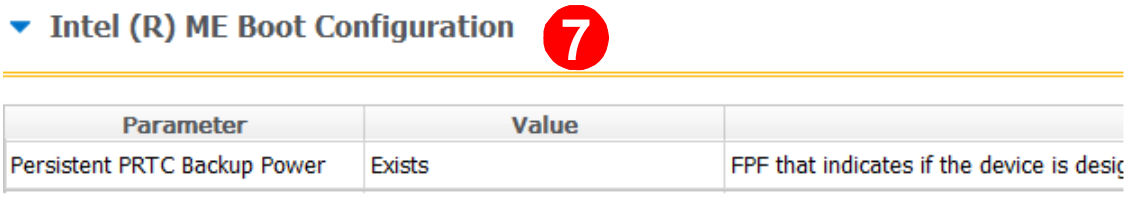
Table 2-5. - Intel® ME Kernel (Sheet 3 of 4)

	EOM of First Boot Enabled **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.	TGL-H	Lock Descriptor and OEM Configs
Click on Intel® ME Kernel in the left tabs menu> MCTP Configuration is expanded by default:			



Parameter	Value	Help Text
MCTP Stack Configuration	0x920030	Defines the ME's 8-bits MCTP Endpoint IDs for each SMBus physical interface (SMBus, ...
MctpDevicePortEc	0x02	-
MctpDevicePortSio	0x00	-
MctpDevicePortIsh	0x00	-
MctpDevicePortBmc	0x00	-

#	Parameter	Platform	Settings
6	**MCTP Configuration**		
	MCTP Stack Configuration Defines the Intel® ME's 8-bits MCTP Endpoint ID's 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.	TGL-H	0x920030
	MctpdevicePortEc	TGL-H	0x02
	MctpdevicePortSio	TGL-H	0x00
	MctpdevicePortIsh	TGL-H	0x00
	MctpdevicePortBmc	TGL-H	0x00
Click on Intel® ME Kernel in the left tabs menu> Intel® ME Boot Configuration is expanded by default:			



Parameter	Value	
Persistent PRTC Backup Power	Exists	FPF that indicates if the device is desig

#	Parameter	Platform	Settings
7	**Intel® ME Boot Configuration**		

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

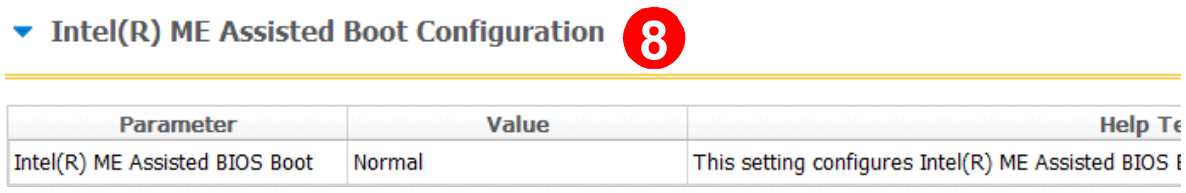
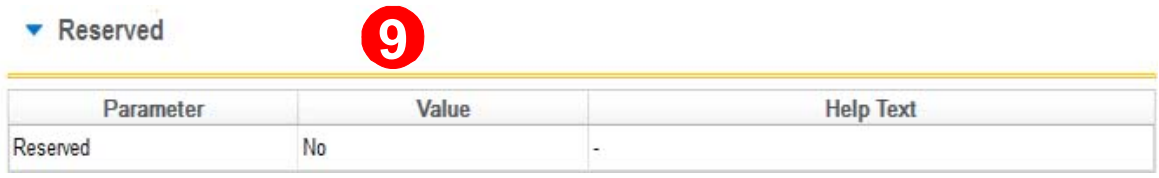
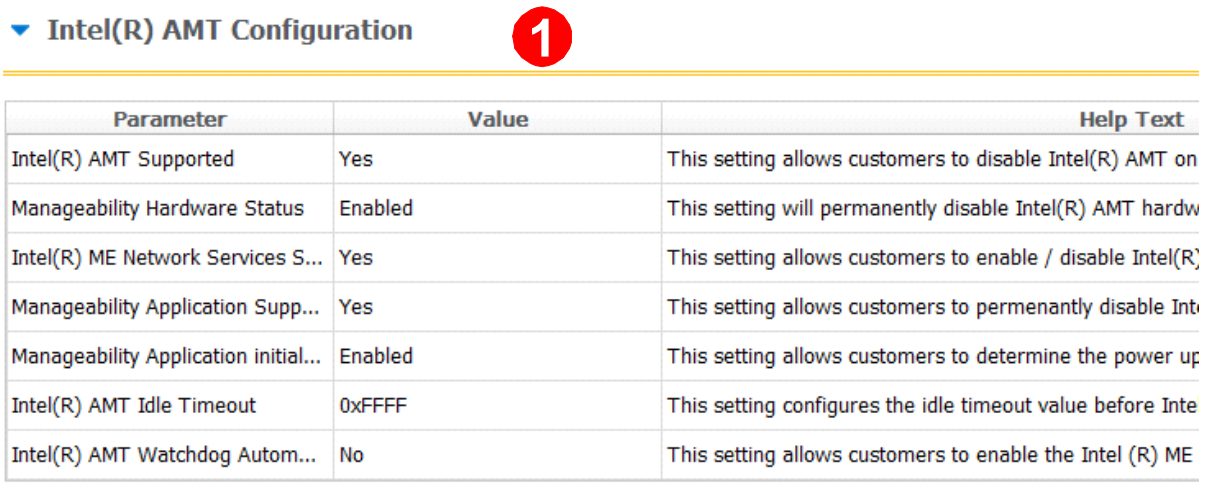
	Persistent PRTC Backup Power **Values: None / Exists** FPF that indicates if the device is designed such that it may lose PRTC power more than 10 times throughout the normal life-cycle of the product and hence has no persistent time or AR protection. At EOM this value is burned to the FPF, and can never be changed	TGL-H	Exists
Click on Intel® ME Kernel in the left tabs menu> Intel® ME Assisted Boot Configuration is expanded by default:			
			
8	**Intel® ME Assisted Boot Configuration**		
	Intel **Values: Normal / Intel® ME Assisted** This setting configures Intel® ME Assisted BIOS Boot capabilities. ***Note:*** Leave this setting configured to "Normal"	TGL-H	Normal
Click on Intel® ME Kernel in the left tabs menu> Reserved is expanded by default:			
			
9	**Reserved**		
	Reserved **Values: Yes / No**	TGL-H	No

Table 2-6. - Intel® AMT (Sheet 1 of 8)

Click on Intel® AMT in the left tabs menu> Intel® AMT is expanded by default:



#	Parameter	Platform	Settings
1	**Intel® AMT Configuration**		
	Intel® AMT Supported **Values: Yes / No** - This setting allows customers to disable Intel® AMT on the platform and force the platform into Standard Manageability mode. ***Note:*** If this setting has been set to disabled Intel® AMT cannot be re-enabled once the descriptor has been locked. This setting applies to Desktop and Workstation only.	TGL-H	Yes Yes
	Manageability Hardware Status **Values: Enabled / Disabled -** This setting will permanently disable Manageability hardware through platform FPFs. At End-of-Manufacturing (EOM), enable/disable policy value is committed to FPF and can never be changed. Permanently disabling Manageability hardware with this setting requires "Manageability Application Supported" and "Disabled" and "Intel® ME Network Services Supported" are set to "No". ***Note:*** When "Manageability Application Hardware Status" is Enabled but "Manageability Application Supported" and "Intel® ME Network Services Supported" are set to "No", Manageability Hardware will be disabled by the Intel®CSME through CVAR.	TGL-H	Enabled
	Intel® ME Network Services Supported **Values: Yes / No -** This setting allows customers to enable / disable Intel® ME Network Services on the platform. ***Note:*** This setting and TLS needs to be enabled for proper operation of Intel® Authenticate (Corporate Only). In addition if this setting is disabled Intel® AMT will also be disabled.	TGL-H	Yes Yes
	Intel® Manageability Application Supported **Values: Yes / No -** This setting allows customers to force Intel® AMT enabled platforms to operate in Standard Manageability mode. ***Note:*** This setting only applies to Desktop and Workstation platforms.	TGL-H	Yes Yes
	Manageability Application initial power-up state **Values: Enabled / Disabled** This setting allows customers to determine the power up state for Intel® AMT or Standard Manageability. ***Note:*** If this setting is disabled Intel® AMT or Standard Manageability can still be re-enabled through the Intel® MEBx interface.	TGL-H	Yes Yes

Table 2-6. - Intel® AMT (Sheet 2 of 8)

#	Parameter	Platform	Settings
	Intel® AMT Idle Timeout **Values: 0xFFFF** - This setting configures the idle timeout value before Intel® AMT enters into an off state.	TGL-H	0xFFFF
	Intel® AMT Watchdog Automatic Reset Enabled **Values: Yes / No** - This setting allows customers to enable the Intel® ME firmware to trigger an automatic platform reset if either the MEI or Agent Presence are in a hung state. ***Note:*** This feature only allows one reset at a time when the watchdog expires. After this feature has triggered a reset, it must be re-armed for reuse via management console.	TGL-H	No

Click on Intel® AMT in the left tabs menu> KVM Configuration is expanded by default:

KVM Configuration 2

Parameter	Value	Help Text
Firmware KVM Screen Blanking	No	-
KVM Redirection Supported	Yes	-

#	Parameter	Platform	Settings
2	**KVM Configuration**		
	Firmware KVM Screen Blanking **Values: Yes / No -** This setting enables KVM Screen blanking capabilities in the firmware image. ***Note:*** This feature is dependent on processor level support.	TGL-H	No No
	KVM Redirection Supported **Values: Yes / No** - This setting allows OEMs to enable / disable the KVM Redirection capabilities of the firmware. ***Note:*** If this setting has been set to disabled it cannot be re-enabled once the descriptor has been locked.	TGL-H	Yes Yes

Click on Intel® AMT in the left tabs menu> Provisioning Configuration is expanded by default:

Provisioning Configuration 3

Parameter	Value	Help Text
Embedded Host Based Config...	No	-
PKI Domain Name Suffix		-

#	Parameter	Platform	
3	**Provisioning Configuration**		

Table 2-6. - Intel® AMT (Sheet 3 of 8)

	Embedded Host Based Configuration **Values: Yes / No** - This setting allows customers to enable / disable Embedded Host Based Configuration. Important - EHBC is primarily intended for use in embedded systems as it offers less user privacy/security protection than may be appropriate for business client systems. ***Note:*** The Intel® FIT tool will not adjust the Redirection Privacy/Security value based on selection here. Please set security level as needed.	TGL-H	No
	PKI Domain Name Suffix - This setting allow OEMs to pre-configure the Domain Name Suffix used for PKI provisioning in their firmware image. ***Note:*** For normal out-of-box provisioning functionality this setting should be left empty.	TGL-H	-
Click on Intel® AMT in the left tabs menu> OEM Customizable Certificate 1 is expanded by default:			
OEM Customizable Certificate 1 (4)			

Parameter	Value	Help Text
Certificate Enabled	No	This setting allows customers to enable PKI provisioning Custo...
Certificate Friendly Name		This setting allows customers to assign a user friendly name for...
Certificate Stream		This setting allows customers to input hash stream for PKI provi...

#	Parameter	Platform	Settings
4	**OEM Customizable Certificate 1**		
	Certificate Enabled **Values: Yes / No** - This setting allows customers to enable PKI provisioning Custom Certificate 1.	TGL-H	No
	Certificate Friendly Name - This setting allows customers to assign a user friendly name for PKI provisioning Custom Certificate 1. Maximum of 32 characters.	TGL-H	-
	Certificate Stream - This setting allows customers to input hash stream for PKI provisioning Custom Certificate 1. If enabled the certificate will be used in addition to those already pre-loaded in base firmware during provisioning. ***Note:*** If the platform is un-configured the Custom Certificate Hash will be deleted.	TGL-H	-
Click on Intel® AMT in the left tabs menu> OEM Customizable Certificate 2 is expanded by default:			
OEM Customizable Certificate 2 (5)			

Parameter	Value	Help Text
Certificate Enabled	No	This setting allows customers to enable PKI provisioning Custo...
Certificate Friendly Name		This setting allows customers to assign a user friendly name for...
Certificate Stream		This setting allows customers to input hash stream for PKI provi...

#	Parameter	Platform	Settings
5	**OEM Customizable Certificate 2**		

Table 2-6. - Intel® AMT (Sheet 4 of 8)

	Certificate Enabled **Values: Yes/No** - This setting allows customers to enable PKI provisioning Custom Certificate 2.	TGL-H	No
	Certificate Friendly Name - This setting allows customers to assign a user friendly name for PKI provisioning Custom Certificate 2. Maximum of 32 characters.	TGL-H	-
	Certificate Stream - This setting allows customers to input hash stream for PKI provisioning Custom Certificate 2. If enabled the certificate will be used in addition to those already pre-loaded in base firmware during provisioning. ***Note:*** If the platform is un-configured the Custom Certificate Hash will be deleted.	TGL-H	-
Click on Intel® AMT in the left tabs menu> OEM Customizable Certificate 3 is expanded by default:			

#	Parameter	Platform	Settings
6	**OEM Customizable Certificate 3**		
	Certificate Enabled **Values: Yes/No** - This setting allows customers to enable PKI provisioning Custom Certificate 3.	TGL-H	No
	Certificate Friendly Name - This setting allows customers to assign a user friendly name for PKI provisioning Custom Certificate 3. Maximum 32 characters.	TGL-H	-
	Certificate Stream - This setting allows customers to input hash stream for PKI provisioning Custom Certificate 3. If enabled the certificate will be used in addition to those already pre-loaded in base firmware during provisioning. ***Note:*** If the platform is un-configured the Custom Certificate Hash will be deleted.	TGL-H	-
Click on Intel® AMT in the left tabs menu> OEM Default Certificate 1 is expanded by default:			

#	Parameter	Platform	Settings
7	**OEM Default Certificate 1**		

Table 2-6. - Intel® AMT (Sheet 5 of 8)

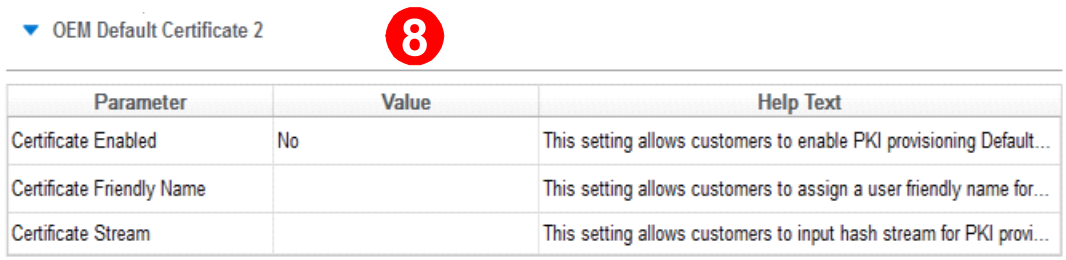
	Certificate Enabled **Values: Yes/No** - This setting allows customers to enable PKI provisioning Default certificate 1.	TGL-H	No
	Certificate Friendly Name - This setting allows customers to assign a user friendly name for PKI provisioning Default Certificate 1. Maximum 32 characters.	TGL-H	-
	Certificate Stream - This setting allows customers to input hash stream for PKI provisioning custom certificate 1. ***Note:*** Default Certificates if enabled will be used in addition to those already pre-loaded in firmware during provisioning. Unlike Customizable Certificates the Default Certificates are not deleted when the platform is un-provisioned.	TGL-H	-
Click on Intel® AMT in the left tabs menu> OEM Default Certificate 2 is expanded by default:			
			
#	**Parameter**	**Platform**	**Settings**
8	**OEM Default Certificate 2**		
	Certificate Enabled **Values: Yes/No** - This setting allows customers to enable PKI provisioning Default certificate 2.	TGL-H	No
	Certificate Friendly Name - This setting allows customers to assign a user friendly name for PKI provisioning Default Certificate 2. Maximum 32 characters.	TGL-H	-
	Certificate Stream - This setting allows customers to input hash stream for PKI provisioning custom certificate 2. ***Note:*** Default Certificates if enabled will be used in addition to those already pre-loaded in firmware during provisioning. Unlike Customizable Certificates the Default Certificates are not deleted when the platform is un-provisioned.	TGL-H	-
Click on Intel® AMT in the left tabs menu> OEM Default Certificate 3 is expanded by default:			
#	**Parameter**	**Platform**	**Settings**

Table 2-6. - Intel® AMT (Sheet 6 of 8)

9	**OEM Default Certificate 3**		
	Certificate Enabled **Values: Yes/No** - This setting allows customers to enable PKI provisioning Default certificate 3.	TGL-H	No
	Certificate Friendly Name - This setting allows customers to assign a user friendly name for PKI provisioning Default Certificate 3. Maximum 32 characters.	TGL-H	-
	Certificate Stream - This setting allows customers to input hash stream for PKI provisioning custom certificate 3. ***Note:*** Default Certificates if enabled will be used in addition to those already pre-loaded in firmware during provisioning. Unlike Customizable Certificates the Default Certificates are not deleted when the platform is un-provisioned.	TGL-H	-
Click on Intel® AMT in the left tabs menu> OEM Default Certificate 4 is expanded by default:			

#	Parameter	Platform	Settings
10	**OEM Default Certificate 4**		
	Certificate Enabled **Values: Yes/No** - This setting allows customers to enable PKI provisioning Default certificate 4.	TGL-H	No
	Certificate Friendly Name - This setting allows customers to assign a user friendly name for PKI provisioning Default Certificate 4.	TGL-H	-
	Certificate Stream - This setting allows customers to input hash stream for PKI provisioning custom certificate 4. ***Note:*** Default Certificates if enabled will be used in addition to those already pre-loaded in firmware during provisioning. Unlike Customizable Certificates the Default Certificates are not deleted when the platform is un-provisioned.	TGL-H	-
Click on Intel® AMT in the left tabs menu> OEM Default Certificate 5 is expanded by default:			

#	Parameter	Platform	Settings

Table 2-6. - Intel® AMT (Sheet 7 of 8)

11	**OEM Default Certificate 5**		
	Certificate Enabled **Values: Yes/No** - This setting allows customers to enable PKI provisioning Default certificate 5.	TGL-H	No
	Certificate Friendly Name - This setting allows customers to assign a user friendly name for PKI provisioning Default Certificate 5.	TGL-H	-
	Certificate Stream - This setting allows customers to input hash stream for PKI provisioning custom certificate 5. ***Note:*** Default Certificates if enabled will be used in addition to those already pre-loaded in firmware during provisioning. Unlike Customizable Certificates the Default Certificates are not deleted when the platform is un-provisioned.	TGL-H	-

Click on Intel® AMT in the left tabs menu> Redirection Configuration is expanded by default:

Redirection Configuration 12

Parameter	Value	Help Text
Redirection Localized Language	English	This setting allows customers to configure which localized langu...
Redirection Privacy / Security ...	Default	This setting allows customers to configure the Privacy and Secu...

#	Parameter	Platform	Settings
12	**Redirection Configuration**		
	Redirection Localized Language - This setting allows customers to configure which localized language will be used initially by firmware for user consent output information (Examples: May be displayed before SOL / KVM session starts).	TGL-H	English
	Redirection Privacy / Security Level - This setting allows customers to configure the Privacy and Security level for redirection operations. **Default** enables all redirection ports (User consent is configurable). **Enhanced** - Enables all redirection ports. (User consent is required and cannot be disabled). **Extreme -** Disables Redirection and Remote Configuration / Client Control Mode. ***Note:*** The Intel® FIT tool will not adjust the Embedded Host Based Configuration value based on selection here. Please set EHBC to yes or no as needed.	TGL-H	Default

Click on Intel® AMT in the left tabs menu> TLS Configuration is expanded by default:

TLS Configuration 13

Parameter	Value	Help Text
Transport Layer Security Supp...	Yes	This setting allows customers to enable / disable firmware Trans...

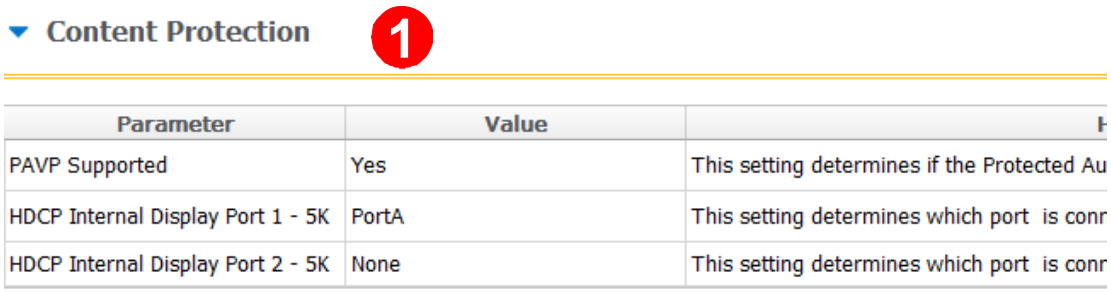
#	Parameter	Platform	Settings
13	**TLS Configuration**		

Table 2-6. - Intel® AMT (Sheet 8 of 8)

	Transport Layer Security Supported **Values: Yes/No** - This setting allows customers to enable / disable firmware Transport Layer Security support. ***Note:*** If this is disabled TLS will be permanently disabled in the firmware image. This setting needs to be enabled along with along with the Intel® ME Network Services Supported for proper operation of the Intel® Authenticate (Corporate Only) feature.	TGL-H	No

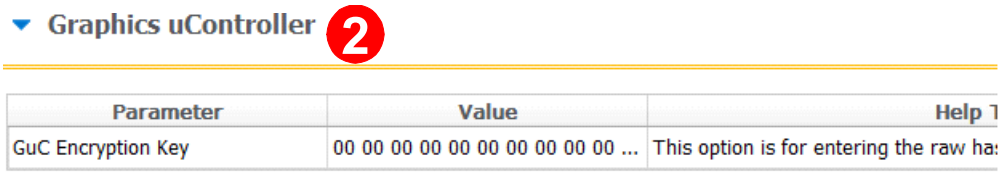
Table 2-7. - Platform Protection (Sheet 1 of 6)

Click on Platform Protection in the left tabs menu> Content Protection is expanded by default:



#	Parameter	Platform	Settings
1	**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.	TGL-H	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.Intel® AMT KVM is not supported if both HDCP Internal Display ports are used.	TGL-H	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.Intel® AMT KVM is not supported if both HDCP Internal Display ports are used.	TGL-H	None

Click on Platform Protection in the left tabs menu> Graphics uController is expanded by default:



#	Parameter	Platform	Settings
2	**Graphics UController**		
	GuC Encryption Key **Values:** This option is for entering the raw hash 256 bit string or certificate file for the Graphics uController.	TGL-H	0x00000000

Click on Platform Protection in the left tabs menu> Hash Key Configuration for Bootguard / ISH is expanded by default:

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

Hash Key Configuration for Bootguard / ISH 3

Parameter	Value	Help Text
OEM Public Key Hash	00 00 00 00 00 00 00 00 00 00 ...	Raw hash string for the SHA-384 hash of the OEM public
OEM Key Manifest Binary		Signed manifest file containing hashes of keys used for si
Second OEM key hash	00 00 00 00 00 00 00 00 00 00 ...	-
Oem Key Revocation Enable	No	Enabling the OEM key revocation mechanism requires 'OE

#	Parameter	Platform	
3	**Hash Key Configuration for Bootguard / ISH**		
	OEM Public Key Hash **Values:** This option is for entering the raw hash string or certificate file for Boot Guard and ISH. This 384-bit field represents the SHA-384 hash of the OEM public key corresponding to the private key used to sign the BIOS-SM or ISH image. Please see Appendix F for further details.	TGL-H	0x00000000
	OEM Key Manifest Binary Signed manifest file containing hashes of keys used for signing components of image. This setting is only configurable when OEM signing is enabled (See PlatformIntegrity / OemPublicKeyHash).	TGL-H	
	Second OEM Key hash **Values:** This option is for entering a secondary raw hash string or certificate file for Boot Guard and ISH used in instances of OEM Key Revocation. This 384-bit field represents the SHA-384 hash of the OEM public key corresponding to the private key used to sign the BIOS-SM or ISH image. Please see Appendix F for further details. ***Note:*** This setting is greyed out and not configurable until the Second OEM Key Revocation Enable is set to Yes.	TGL-H	0x00000000
	OEM Key Revocation Enabled **Values: Yes/No** This setting enables firmware OEM Key Revocation capabilities. ***Note:*** This setting requires that both OEM Public Key Hash and Second OEM Key Hash are configured.	TGL-H	No

Click on Platform Protection in the left tabs menu> Boot Guard Configuration is expanded by default:

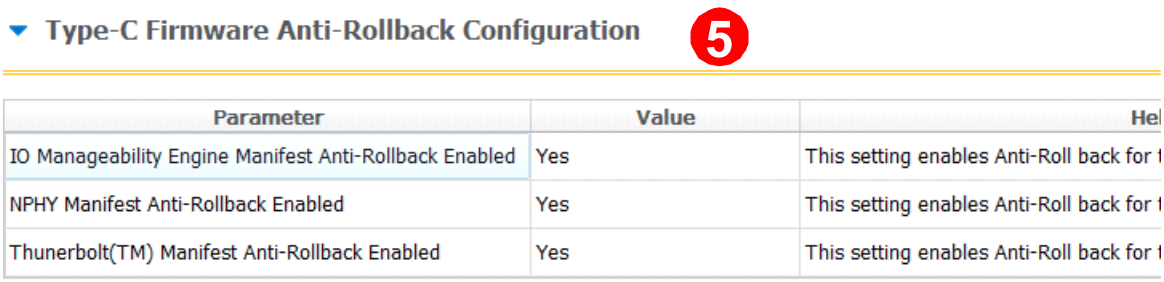
Boot Guard Configuration 4

Parameter	Value	
Key Manifest ID	0	ODM identifier used during th
Boot Guard Profile Configuration	Boot Guard Profile 0 - No_FVME	Boot Guard Profile 0 - Legacy
CPU Debugging	Enabled	This setting determines if CPU
BSP Initialization	Enabled	This setting determines BSP I
S3 Optimization	Enabled	This setting overrides Boot Gu

Table 2-7. - Platform Protection (Sheet 3 of 6)

#	Parameter	Platform	Settings
4	**Boot Guard Configuration**		
	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.	TGL-H	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.	TGL-H	Boot Guard Profile 0 - No_FVME
	CPU Debugging **Values: Enabled / Disabled** This setting determines if CPU debug modes will be displayed. When set to 'Enabled' CPU debugging is enabled.	TGL-H	Enabled Enabled
	BSP Initialization **Values: Enabled / Disabled** This setting determines BSP behavior when it receives an INIT signal. When set to 'Enabled' BSP will behave normally if it receives an INIT (Disabled BSP Initialization (DBI) bit=0). When set to 'Disabled' BSP will shutdown if it receives an INIT ("DBI" bit=1).	TGL-H	Enabled
	S3 Optimization **Values: Enabled / Disabled** This setting overrides Boot Guard S3 optimization. ***Note:*** This setting is for testing purposes only.	TGL-H	Enabled

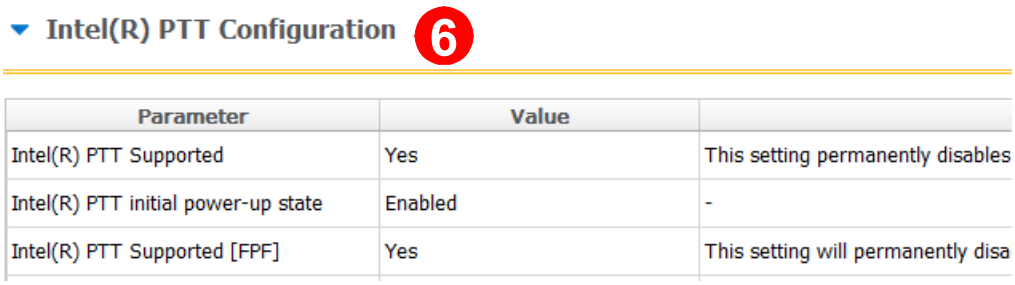
Click on Platform Protection in the left tabs menu> Type-C Firmware Anti-Rollback Configuration is expanded by default:



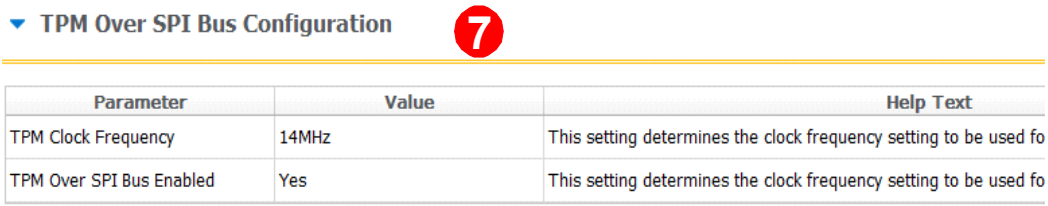
#	Parameter	Platform	Settings
5	**Type-C Firmware Anti-Rollback Configuration**		
	IO Manageability Engine Manifest Anti-Rollback Enabled **Values: Yes / No** This setting enables Anti-Rollback for the Type-C Subsystem I/O Manageability Engine binary.	TGL-H	Yes
	NPHY Manifest Anti-Rollback Enabled **Values: Yes / No** This setting enabled Anti-Rollback for the Type-C Subsystem NPHY binary.	TGL-H	Yes

Table 2-7. - Platform Protection (Sheet 4 of 6)

	Thunerbolt(TM) Manifest Anti-Rollback Enabled **Values: Yes/No** This setting enabled Anti-Rollback for the Type-C Subsystem Thunerbolt(TM) binary.	TGL-H	Yes
Click on Platform Protection in the left tabs menu> Intel® PTT Configuration is expanded by default:			

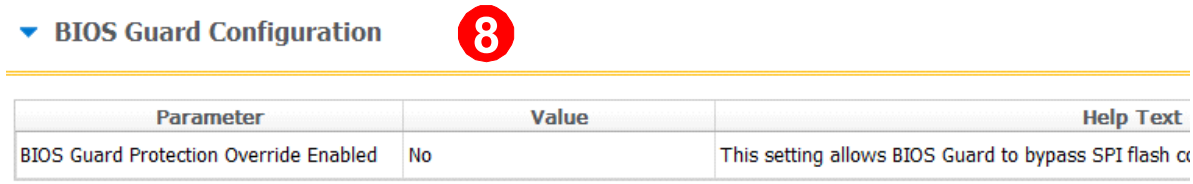


#	Parameter	Platform	Settings
6	**Intel® PTT Configuration**		
	Intel® PTT Supported **Values: Yes/No** - This setting permanently disables Intel® PTT in the firmware image.	TGL-H	Yes
	Intel® PTT initial power-up state **Values: Enabled/Disabled** - This setting determines if Intel® PTT is enabled on platform power-up.	TGL-H	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.	TGL-H	Yes
Click on Platform Protection in the left tabs menu> TPM Over SPI Bus Configuration is expanded by default:			

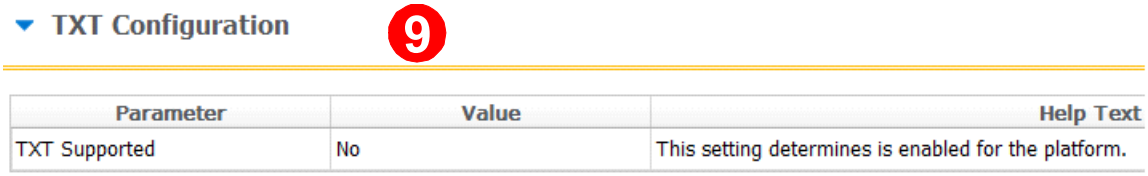


#	Parameter	Platform	Settings
7	**TPM Over SPI Bus Configuration**		
	TPM Clock Frequency **Values: 14MHz, 25MHz, 48MHz** - This setting determines the clock frequency setting to be used for the TPM over SPI bus.	TGL-H	14MHz
	TPM Over SPI Bus Enabled **Values: Yes/No** - This setting determines if TPM over SPI bus is enabled on the platform.	TGL-H	No
Click on Platform Protection in the left tabs menu> BIOS Guard Configuration is expanded by default:			

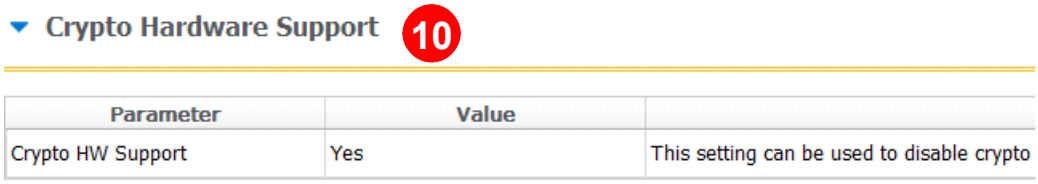
Table 2-7. - Platform Protection (Sheet 5 of 6)



#	Parameter	Platform	Settings
8	**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).	TGL-H	No
Click on Platform Protection in the left tabs menu> TXT Configuration is expanded by default:			

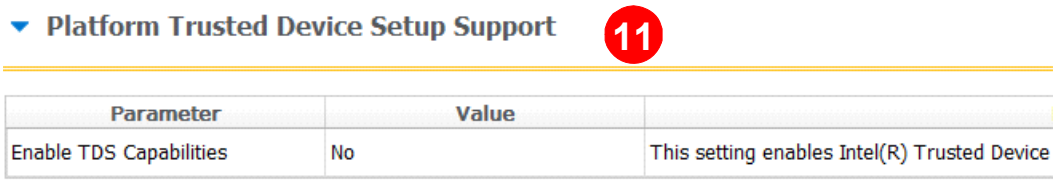


#	Parameter	Platform	Settings
9	**TXT Configuration**		
	TXT Supported This setting determines if enabled for the platform.	TGL-H	No
Click on Platform Protection in the left tabs menu> Crypto Hardware Support is expanded by default:			



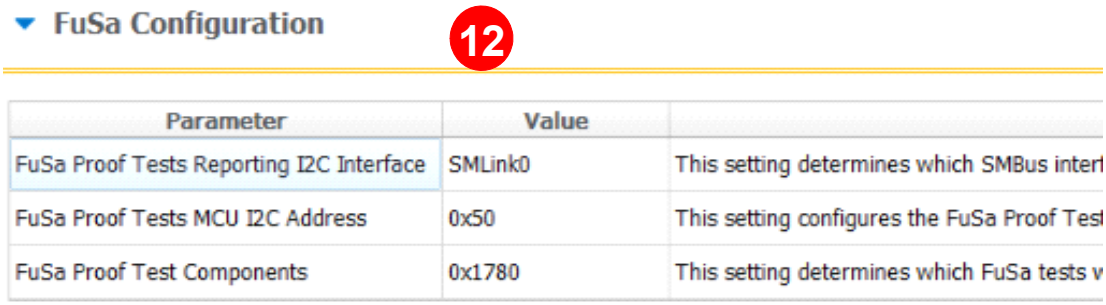
#	Parameter	Platform	Settings
10	**Crypto HW Support**		
	Crypto HW Support **Values: Yes / No** - This setting can be used to disable Intel® CSME cryptographic functionality. ***Caution:*** Configuring this setting to "No" will disables all Intel® CSME cryptographic related features.	TGL-H	Yes
Click on Platform Protection in the left tabs menu> Platform Trusted Device Setup Support is expanded by default:			

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



#	Parameter	Platform	Settings
11	**Platform Trusted Device Setup Support**		
	Enable TDS Capabilities **Values: Yes / No** - This setting enables Intel® Trusted Device Setup on the platform.	TGL-H	No

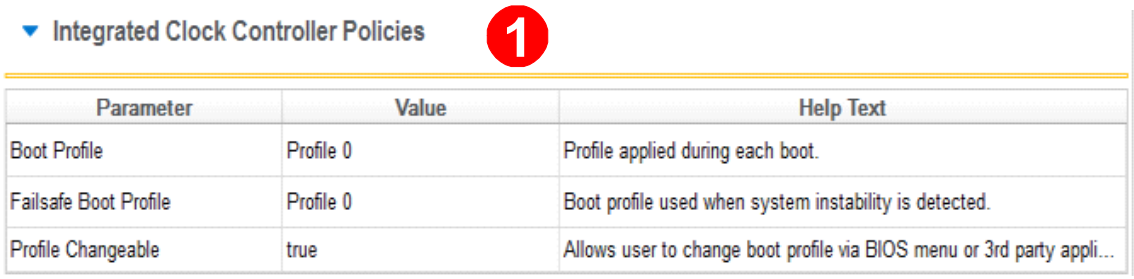
Click on Platform Protection in the left tabs menu> FuSa Configuration is expanded by default:



#	Parameter	Platform	Settings
12	**FuSa Configuration** ***Note:*** The GBST sub-partition is used to enabling FuSa safety standards and is not applicable for client platforms.		
	FuSa Proof Tests Reporting I2C Interface **Values:**	TGL-H	SMLink0
	FuSa Proof Tests MCU I2C Address **Values:**	TGL-H	0x50
	FuSa Proof Tests Components **Values:**	TGL-H	0x1780

Table 2-8. - Integrated Clock Controller (Sheet 1 of 9)

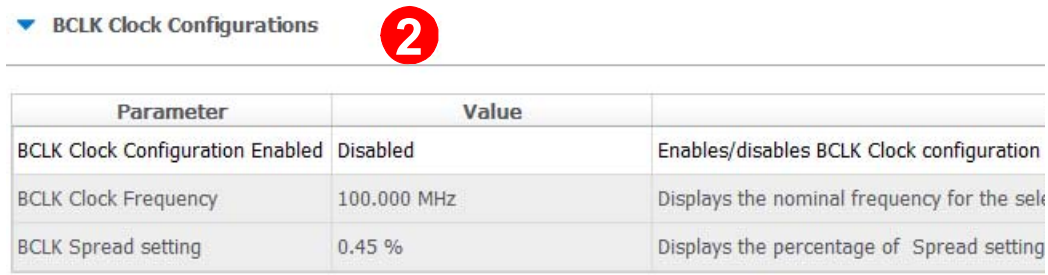
Click on Integrated Clock Controller in the left tabs menu> Integrated Clock Controller Policies are expanded by default:



#	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. Double click on value column of this parameter to choose from available options.	TGL-H	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. Double click on value column of this parameter to choose from available options.	TGL-H	Profile 0
	Profile Changeable Possible configuration: True/False. This parameter controls if BIOS or 3rd party application can select boot profile or not. When set to true, it allows user to change boot profile via BIOS or 3rd party application. When set to false, Runtime change to boot profile is not allowed and boot profile selected by **"Integrated Clock Controller |Integrated Clock Controller Policies - Boot Profile "** parameter will be used to boot platform. Double click on value column of this parameter to choose from available options.	TGL-H	True

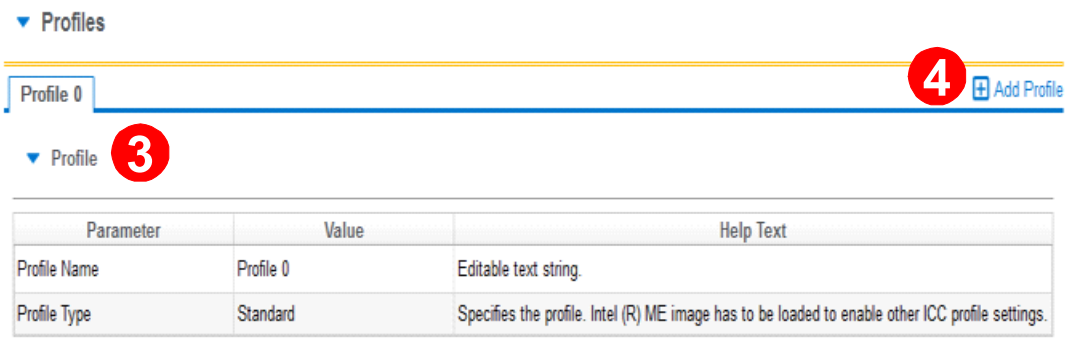
Click on Integrated Clock Controller in the left tabs menu> Profiles >Profile> Bclk Clock Configuration is expanded by default:

Table 2-8. - Integrated Clock Controller (Sheet 2 of 9)



#	Parameter	Platform	Settings
2	**BCLK Clock Configuration**		
	BCLK Clock Configuration Enabled **Values: Enabled / Disabled** This setting enables / disables BCLK Clock configuration values for Adaptive / Overclocking profiles	TGL-H	Disabled
	BCLK Clock Frequency This parameter allows user to select the nominal frequency for the selected clock. Range is limited based on the Clock Range Definition record and HW SKU.	TGL-H	N/A
	BCLK Spread Setting This parameter allows user to select the percentage of Spread setting for the selected clock. Range is limited based on the Clock Range Definition record and HW SKU.	TGL-H	N/A

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

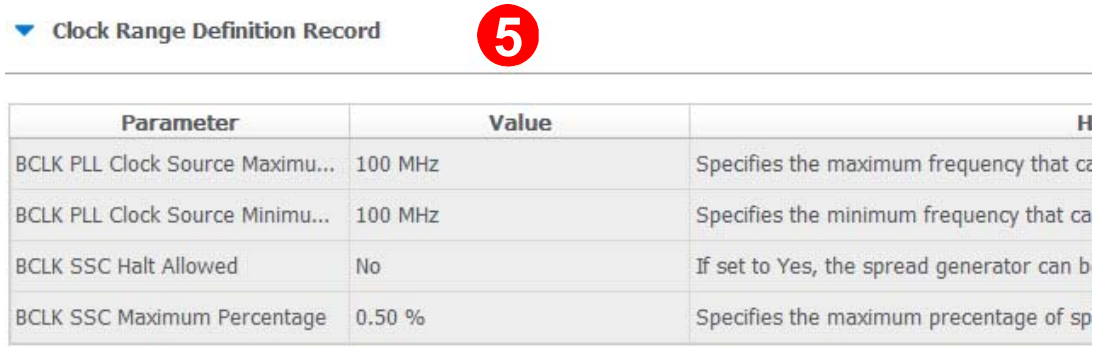


#	Parameter	Platform	Settings

Table 2-8. - Integrated Clock Controller (Sheet 3 of 9)

3	**Profiles - Profile 0** **Note:** Intel® ME image has to be loaded to enable other ICC profile settings. **For UP3/UP4,** Intel® FIT provides 2 pre-defined ICC profiles to choose from. •**Standard**: This profile provides default settings for standard configuration, no adaptive clocking is allowed. Platform clocks output internal and external are driven from USB3PCIE clock. Default clock frequency is 100 MHz with 0.47%DownSpread. BCLK clock source should be turned off in this case to save power. •**Adaptive**: This profile provides Wimax/3G friendly configuration. This profile will configure the platform based on the Adaptive profile allowing adaptive clocking adjustment for BCLK clock source to reduce EMI interference. It supports default clock frequency of 98.875 MHz with 0.48% Downspread. •**Overclocking Ext:** This profile provides overclocking friendly configuration. This profile provides overclocking > 100 MHz and supports all OC frequency ranges or BCLK overclocking. **For** TGL-H**,** Intel® FIT provides 5 pre-defined ICC profiles to choose from. •**Standard** •**Adaptive** •**OverClockingExt** **Note**: User can select pre-defined profiles via **"Integrated Clock Controller | Profiles - Profile Type "** parameter User can add up to maximum 16 profiles.To add new profile, please use **"Integrated Clock Controller | Profiles - + Add Profile Button"**	TGL-H	Standard
	Profile Name This parameter allows user to customize profile name for easy identification. By default it uses pre-defined profile name like Profile 0.	TGL-H	Profile 0
	Profile Type Available ICC profiles for TGL-H are Standard, Adaptive and OverClockingExt. This parameter indicates which pre- defined profile selected for each profile#. Double click on value column of this parameter to choose from available options.	TGL-H	Standard
4	**+ Add Profile Button** This button is used to add new ICC profile. User can add up to maximum 16 profiles. New profile will be added under **"Integrated Clock Controller | Profiles"** tab**.**	TGL-H	
Click on Integrated Clock Controller in the left tabs menu> Profiles >Profile> Clock Range Definition Record is expanded by default:			

Table 2-8. - Integrated Clock Controller (Sheet 4 of 9)



#	Parameter	Platform	Settings
5	**Clock Range Definition Record**		
	BCLK PLL Clock Source Maximum Frequency - This parameter allows user to specify the maximum frequency that can be applied to BCLK clock source when overclocking the platform. Value is limited by divider/frequency limits determined by HW SKU, and cannot be less than 100 MHz. **Standard Setting Profile Type -** Option is grayed out. **Adaptive Setting Profile Type -** Option is able to be edited. **OverClockingExt Setting Profile Type -** Option is able to be edited.	TGL-H	
	BCLK PLL Clock Source Minimum Frequency - This parameter allows user to specify the minimum frequency that can be applied to BCLK clock source when underclocking the platform. Value is limited by divider/frequency limits determined by HW SKU, and cannot be greater than 100 MHz. **Standard Setting Profile Type -** Option is grayed out. **Adaptive Setting Profile Type -** Option is able to be edited. **OverClockingExt Setting Profile Type -** Option is able to be edited.	TGL-H	
	BCLK SSC Halt Allowed - This parameter allows user to select if the spread generator can be disabled at runtime or not.if set to **"True"**, the spread generator can be enabled and disabled at runtime. **Standard Setting Profile Type -** Option is grayed out. **Adaptive Setting Profile Type -** Option is able to be edited. **OverClockingExt Setting Profile Type -** Option is able to be edited.	TGL-H	
	BCLK SSC Percentage - This parameter Specifies the maximum percentage of spread adjustment that can be applied to the clock. Value is specified in 1/100th of percent(50=0.5%) **Standard Setting Profile Type -** Option is grayed out. **Adaptive Setting Profile Type -** Option is able to be edited. **OverClockingExt Setting Profile Type -** Option is able to be edited.	TGL-H	

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

Table 2-8. - Integrated Clock Controller (Sheet 5 of 9)

Clock Output Configuration 6

Parameter	Value	
SRC0	Disabled	Enable/Disable the CLKOUT_SRC0
SRC1	Disabled	Enable/Disable the CLKOUT_SRC1
SRC2	Disabled	Enable/Disable the CLKOUT_SRC2
SRC3	Disabled	Enable/Disable the CLKOUT_SRC3
SRC4	Disabled	Enable/Disable the CLKOUT_SRC4
SRC5	Disabled	Enable/Disable the CLKOUT_SRC5
SRC6	Disabled	Enable/Disable the CLKOUT_SRC6
SRC7	Disabled	Enable/Disable the CLKOUT_SRC7
SRC8	Disabled	Enable/Disable the CLKOUT_SRC8
SRC9	Disabled	Enable/Disable the CLKOUT_SRC9
SRC10	Disabled	Enable/Disable the CLKOUT_SRC1
SRC11	Disabled	Enable/Disable the CLKOUT_SRC1
SRC12	Disabled	Enable/Disable the CLKOUT_SRC1
SRC13	Disabled	Enable/Disable the CLKOUT_SRC1
SRC14	Disabled	Enable/Disable the CLKOUT_SRC1
SRC15	Disabled	Enable/Disable the CLKOUT_SRC1

#	Parameter	Platform	Settings
6	**Clock Output Configuration**		
	SRC0[6:15] **Values: Enabled / Disabled** These parameters come under the Power Management section and they control Enabling /Disabling of specific Output Clocks at boot time. These settings should match with platform hardware design. For RVP, recommend keeping defaults for bring up with Intel® CSME FW. These parameters are specifically used to Enable/Disable the respective CLKOUT_XXX differential output buffers	TGL-H	Enabled

Table 2-8. - Integrated Clock Controller (Sheet 6 of 9)

	SRC1 **Values: Enabled / Disabled** Enables or Disables the CLKOUT_SRC1 differential output buffer.	TGL-H	Enabled
	SRC2 **Values: Enabled / Disabled** Enables or Disables the CLKOUT_SRC2 differential output buffer.	TGL-H	Enabled
	SRC3 **Values: Enabled / Disabled** Enables or Disables the CLKOUT_SRC3 differential output buffer.	TGL-H	Enabled
	SRC4 **Values: Enabled / Disabled** Enables or Disables the CLKOUT_SRC4 differential output buffer.	TGL-H	Enabled
	SRC5 **Values: Enabled / Disabled** Enables or Disables the CLKOUT_SRC5 differential output buffer.	TGL-H	Enabled
	SRC6 **Values: Enabled / Disabled** Enables or Disables the CLKOUT_SRC6 differential output buffer.	TGL-H	Enabled
	SRC7 **Values: Enabled / Disabled** Enables or Disables the CLKOUT_SRC7 differential output buffer.	TGL-H	Enabled
	SRC8 **Values: Enabled / Disabled** Enables or Disables the CLKOUT_SRC8 differential output buffer.	TGL-H	Enabled
	SRC9 **Values: Enabled / Disabled** Enables or Disables the CLKOUT_SRC9 differential output buffer.	TGL-H	Enabled
	SRC10 **Values: Enabled / Disabled** Enables or Disables the CLKOUT_SRC10 differential output buffer.	TGL-H	Enabled
	SRC11 **Values: Enabled / Disabled** Enables or Disables the CLKOUT_SRC11 differential output buffer.	TGL-H	Enabled
	SRC12 **Values: Enabled / Disabled** Enables or Disables the CLKOUT_SRC12 differential output buffer.	TGL-H	Enabled
	SRC13 **Values: Enabled / Disabled** Enables or Disables the CLKOUT_SRC13 differential output buffer.	TGL-H	Enabled
	SRC14 **Values: Enabled / Disabled** Enables or Disables the CLKOUT_SRC14 differential output buffer.	TGL-H	Enabled
	SRC15 **Values: Enabled / Disabled** Enables or Disables the CLKOUT_SRC15 differential output buffer.	TGL-H	Enabled
Click on Integrated Clock Controller in the left tabs menu> Profiles >Profile> Power Management Configuration is expanded by default:			

Table 2-8. - Integrated Clock Controller (Sheet 7 of 9)

Power Management Configuration

Parameter	Value	
SRC0 CLKREQ# Mapping	GPP_B5	Assign the CLKREQ# signal associat
SRC1 CLKREQ# Mapping	GPP_B6	Assign the CLKREQ# signal associat
SRC2 CLKREQ# Mapping	GPP_B7	Assign the CLKREQ# signal associat
SRC3 CLKREQ# Mapping	GPP_B8	Assign the CLKREQ# signal associat
SRC4 CLKREQ# Mapping	GPP_B9	Assign the CLKREQ# signal associat
SRC5 CLKREQ# Mapping	GPP_B10	Assign the CLKREQ# signal associat
SRC6 CLKREQ# Mapping	GPP_H0	Assign the CLKREQ# signal associat
SRC7 CLKREQ# Mapping	GPP_H1	Assign the CLKREQ# signal associat
SRC8 CLKREQ# Mapping	GPP_H2	Assign the CLKREQ# signal associat
SRC9 CLKREQ# Mapping	GPP_H3	Assign the CLKREQ# signal associat
SRC10 CLKREQ# Mapping	GPP_H4	Assign the CLKREQ# signal associat
SRC11 CLKREQ# Mapping	GPP_H5	Assign the CLKREQ# signal associat
SRC12 CLKREQ# Mapping	GPP_H6	Assign the CLKREQ# signal associat
SRC13 CLKREQ# Mapping	GPP_H7	Assign the CLKREQ# signal associat
SRC14 CLKREQ# Mapping	GPP_H8	Assign the CLKREQ# signal associat
SRC15 CLKREQ# Mapping	GPP_H9	Assign the CLKREQ# signal associat

#	Parameter	Platform	Settings
7	**Profile Power Management Configuration** Configuring CLKREQ# and assigning GPIO depends on how CLKOUT_SRCx configuration via FIT is done (Enabled or Disabled) and if CLKREQ is required or not. **Please refer to Appendix B.3 (How to configure CLKREQ# parameters)** for the detail of CLKREQ configuration for SRC Output clocks. Please configure CLKREQ parameters accordingly.		

Table 2-8. - Integrated Clock Controller (Sheet 8 of 9)

	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. **SRC[15:6] CLKREQ# Mapping - TGL-H 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.	TGL-H	GPP_B5
	SRC1 CLKREQ# Mapping Assign the CLKREQ# signal associated with CLKOUT_SRC1.	TGL-H	GPP_B6
	SRC2 CLKREQ# Mapping Assign the CLKREQ# signal associated with CLKOUT_SRC2.	TGL-H	GPP_B7
	SRC3 CLKREQ# Mapping Assign the CLKREQ# signal associated with CLKOUT_SRC3.	TGL-H	GPP_B8
	SRC4 CLKREQ# Mapping Assign the CLKREQ# signal associated with CLKOUT_SRC4.	TGL-H	GPP_B9
	SRC5 CLKREQ# Mapping Assign the CLKREQ# signal associated with CLKOUT_SRC5.	TGL-H	GPP_B10
	SRC6 CLKREQ# Mapping Assign the CLKREQ# signal associated with CLKOUT_SRC6.	TGL-H	GPP_H0
	SRC7 CLKREQ# Mapping Assign the CLKREQ# signal associated with CLKOUT_SRC7.	TGL-H	GPP_H1
	SRC8 CLKREQ# Mapping Assign the CLKREQ# signal associated with CLKOUT_SRC8.	TGL-H	GPP_H2
	SRC9 CLKREQ# Mapping Assign the CLKREQ# signal associated with CLKOUT_SRC9.	TGL-H	GPP_H3
	SRC10 CLKREQ# Mapping Assign the CLKREQ# signal associated with CLKOUT_SRC10.	TGL-H	GPP_H4
	SRC11 CLKREQ# Mapping Assign the CLKREQ# signal associated with CLKOUT_SRC11.	TGL-H	GPP_H5
	SRC12 CLKREQ# Mapping Assign the CLKREQ# signal associated with CLKOUT_SRC12.	TGL-H	GPP_H6
	SRC13 CLKREQ# Mapping Assign the CLKREQ# signal associated with CLKOUT_SRC13.	TGL-H	GPP_H7
	SRC14 CLKREQ# Mapping Assign the CLKREQ# signal associated with CLKOUT_SRC14.	TGL-H	GPP_H8
	SRC15 CLKREQ# Mapping Assign the CLKREQ# signal associated with CLKOUT_SRC15.	TGL-H	GPP_H9

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

#	Parameter	Platform	Settings
8	**PCIe RefClock Configuration**		

Table 2-8. - Integrated Clock Controller (Sheet 9 of 9)

	SSCEN **Values: Enabled / Disabled**	TGL-H	Enabled

Table 2-9. - Networking & Connectivity (Sheet 1 of 4)

Click on Networking & Connectivity in the left tabs menu> Discrete vPro NIC is expanded by default:

Platform vPro 2.5G Wired LAN (i.e. I225) 1

Parameter	Value	Help Te
Platform vPro 2.5G Wired LAN Enabled	No	YES = Discrete NIC enabled in platform NC
Platform vPro 2.5G Wired LAN SMBUS slave address	0x0	Platform discrete NIC slave address Note:

#	Parameter	Platform	Settings
1	**Platform vPro 2.5G Wired LAN**		
	Platform vPro 2.5G Wired LAN Enabled **Values: Yes / No** This setting enables / disables Discrete Intel® vPro Network adapter support on the platform.	TGL-H	No
	Platform vPro 2.5G Wired LAN slave SMBus Address **Values: Hex** This setting configures the SMBus address for the Discrete Intel®vPro Network adapter.	TGL-H	0x49

Click on Networking & Connectivity in the left tabs menu> Docking Station is expanded by default:

Intel vPro (TM) for Thunderbolt (TM) 3/ USB-C Dock station 2

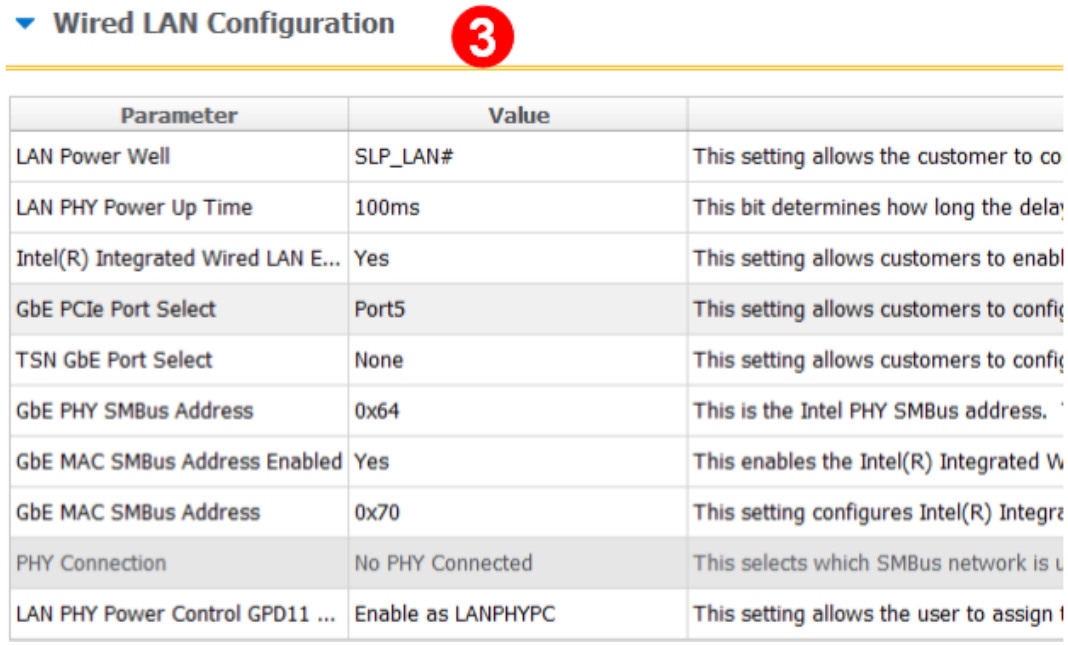
Parameter	Value	Help T
vPro Dock Enabled	No	YES = Enables communication with, vPro supportir
vPro 2.5G Wired LAN on dock slave SMBUS Address	0x0	Dock NIC slave address Note: Input needs to be in
Type-C Port1 Re-Timer I2C Address	0x20	This setting configures the Intel(R) SMBus I2C Add
Type-C Port2 Re-Timer I2C Address	0x21	This setting configures the Intel(R) SMBus I2C Add
Type-C Port3 Re-Timer I2C Address	0x22	This setting configures the Intel(R) SMBus I2C Add
Type-C Port4 Re-Timer I2C Address	0x23	This setting configures the Intel(R) SMBus I2C Add

#	Parameter	Platform	Settings
2	**Intel vPro(TM) for Thinderbolt 3(TM) / USB-C Dock Station**		
	vPro Dock Enabled This setting enables Intel® vPro communication over supported NIC in a Thunderbolt™ Dock.	TGL-H	No
	vPro 2.5G Wired LAN on dock slave SMBus Address This setting configures the NIC SMBus slave address.	TGL-H	0x0
	Type-C Port1 Re-Timer I2C Address This setting configures Intel® SMBus I2C Address.	TGL-H	0x20
	Type-C Port2 Re-Timer I2C Address This setting configures Intel® SMBus I2C Address.	TGL-H	0x21

Table 2-9. - Networking & Connectivity (Sheet 2 of 4)

	Type-C Port3 Re-Timer I2C Address This setting configures Intel® SMBus I2C Address.	TGL-H	0x22
	Type-C Port4 Re-Timer I2C Address This setting configures Intel® SMBus I2C Address.	TGL-H	0x23

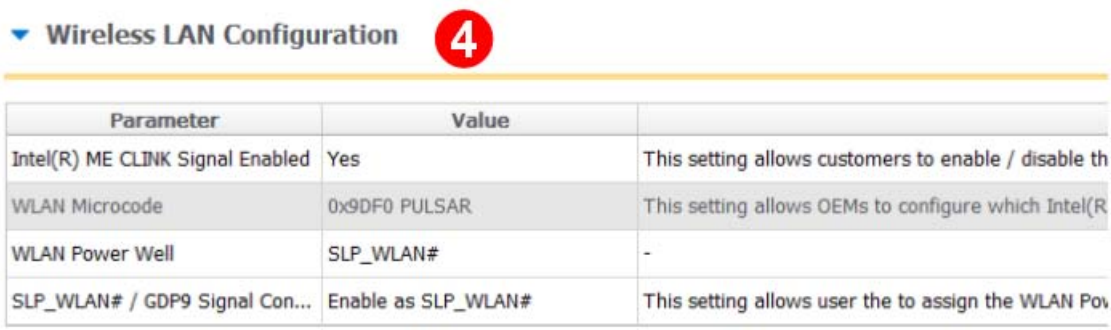
Click on Networking & Connectivity in the left tabs menu> Wired LAN Configuration is expanded by default:



#	Parameter	Platform	Settings
3	**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#.	TGL-H	SLP_LAN#
	LAN PHY Power Up Time **Values: 50ms, 100ms**	TGL-H	100ms
	Intel® Integrated Wired LAN Enable **Values: Enabled / Disabled -** This setting enables or disables the Intel® Integrated LAN.	TGL-H	Enabled
	GbE PCIe Port Select **Values: None, PORT5, PORT9, PORT12, PORT13** - This setting allows customers to configure the PCIe Port that will Intel® Integrated LAN will operate on.	TGL-H	Port 5
	TSN GbE PCIe Port Select **Values: None, TSN PORT6, TSN PORT 7** - This setting allows customers to configure the PCIe port that TSN will operate on. ***Note:*** The Intel® Integrated LAN and TSN GbE are mutually exclusive.	TGL-H	None
	GbE PHY SMBus Address This setting configures Intel® Integrated Wired LAN SMBus address to accept SMBus cycles from the MAC. **Note:** Recommended setting is 64h.	TGL-H	0x64

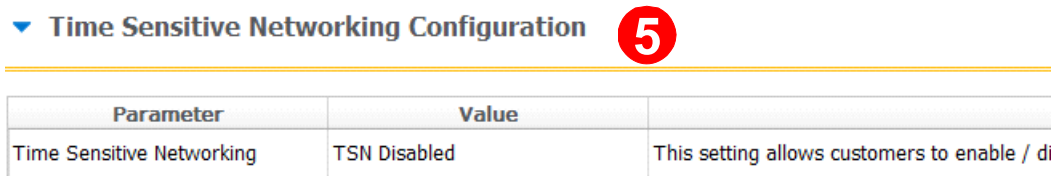
Table 2-9. - Networking & Connectivity (Sheet 3 of 4)

	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.	TGL-H	Yes
	GbE MAC SMBus Address	TGL-H	0x70
	PHY Connection **Values: No PHY connected, PHY on SMLink0**	TGL-H	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".	TGL-H	LANPHYPC
Click on Networking & Connectivity in the left tabs menu> Wireless LAN Configuration is expanded by default:			



#	Parameter	Platform	Settings
4	**Wireless LAN Configuration**		
	CLINK Enabled **Values: Yes/No** This setting allows customers to enable / disable the Wireless LAN CLINK signal through Intel® CSME firmware. ***Note:*** For using Intel® vPro Wireless solutions this should be set to "Yes".	TGL-H	
	WLAN Microcode This setting allow OEMs to configure which Intel® Wireless LAN card microcode to load into the firmware image.	TGL-H	0xA0F0
	WLAN Power Well **Values: Disabled, Sus Well, ME Well, SLP_M#||SPDA, SLP_WLAN#** This setting allows OEMs to configure the power well that will be used by Intel® Wireless LAN. WLAN Sleep via SLP_WLAN# (default) ***Note:*** Recommended setting is SLP_WLAN#.	TGL-H	SLP_WLAN#
	SLP_WLAN# / GPD9 Signal Configuration **Values: SLP_WLAN#, GPD9** - This setting allows the customer to assign the WLAN Power Control signal to WLAN or as GDP9. **Note:** If using Intel® Wireless LAN this setting should be set to "Enable as SLP_WLAN#".	TGL-H	Enable as SLP_WLAN#
Click on Networking & Connectivity in the left tabs menu> Time Sensitive Networking Configuration is expanded by default:			

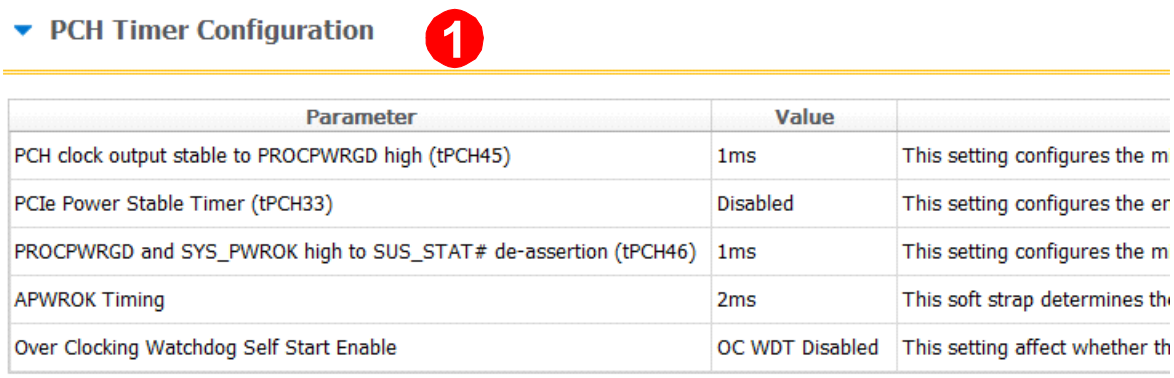
Table 2-9. - Networking & Connectivity (Sheet 4 of 4)



#	Parameter	Platform	Settings
5	**Time Sensitive Networking Configuration**		
	Time Sensitive Networking **Values: TSN Enable / TSN Disabled** ***Note:*** Time Sensitive Networking and Wired LAN are mutually exclusive only one of these features can enabled on the platform.	TGL-H	Disabled

Table 2-10. - Internal PCH Buses (Sheet 1 of 5)

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



#	Parameter	Platform	Settings
1	**PCH Timer Configuration**		
	PCH clock output stable to PROCPWRGD high (tPCH45) **Values: 100ms, 50ms, 5ms, 1ms** - This setting configures the minimum timing from XCK_PLL locked to CPUPWRGD high. For further details see Tiger Lake LP Platform Controller Hub EDS.	TGL-H	1ms
	PCIe Power Stable Timer (tPCH33) **Values: Enabled / Disabled** - This setting configures the enables / disables the t36 timer. When enabled PCH will count 99ms from PWROK assertion before PLTRST# is de-asserted. ***Note:*** The recommended setting is "Disabled".	TGL-H	Disabled
	PROCPWRGD and SYS_PWROK high to SUS_STAT# de-assertion (tPCH46) **Values: 1ms, 2ms, 5ms** - This setting configures the minimum timing from CPUPWRGD assertion to SUS_STAT#. For further details see Tiger Lake LP Platform Controller Hub EDS.	TGL-H	1ms
	APWROK Timing **Values: 2ms, 4ms, 8ms, 15ms** - This soft strap determines the time between the SLP_A# pin de-asserting and the APWROK timer expiration. For further details see Tiger Lake LP Platform Controller Hub EDS.	TGL-H	2ms
	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	TGL-H	OC WDT Disabled

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

Table 2-10. - Internal PCH Buses (Sheet 2 of 5)

SMBus / SMLink Configuration 2

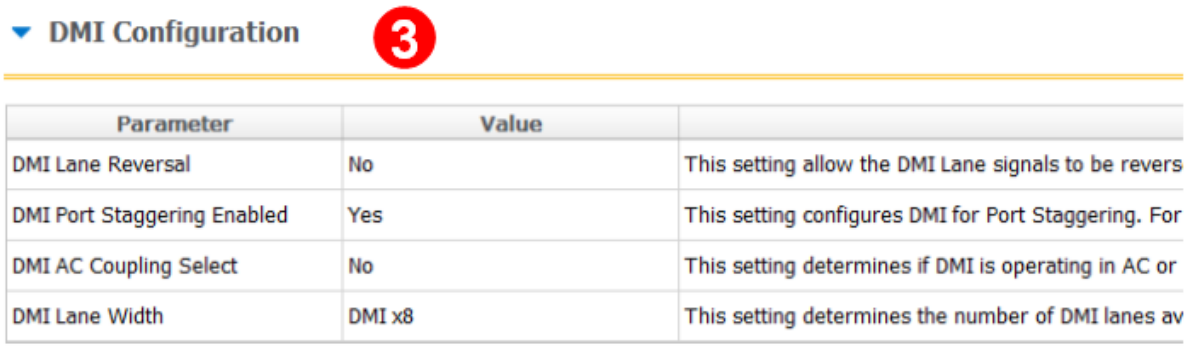
Parameter	Value	
Intel(R) SMLink0 MCTP Address Enabled	No	This setting enables / disables the Intel(R
Intel(R) SMBus ASD Address	0x0	This setting configures the Intel(R) SMBus
Intel(R) SMBus ASD Address Enabled	No	This setting enables / disables the Intel(R
Intel(R) SMBus Subsystem Vendor and Device ID for ASF	0x0	This setting configures the Intel(R) SMBus
Intel(R) SMBus I2C Address	0x0	This setting configures the Intel(R) SMBus
Intel(R) SMBus I2C Address Enabled	No	This setting enables / disables the Intel(R
SMBus / SMLink TCO Slave Connection	Intel(R) SMBus	This setting configures the TCO Slave cor
SMLink0 Enabled	Yes	This setting enables / disables SMLink0 in
SMLink0 Frequency	1 MHz	This setting determines the frequency at
SMLink1 I2C Target Address	0x0	This setting configures SMLink1 I2C Targe
SMLink1 I2C Target Address Enabled	No	This setting configures SMLink1 I2C Targe
SMLink1 GP Target Address	0x0	This setting configures SMLink1 GP Targe
SMLink1 GP Target Address Enabled	No	This setting enables / disables SMLink1 G
SMLink1 Enabled	No	This setting enables / disables SMLink1 in
SMLink1 Frequency	100 KHz	This setting determines the frequency at
Intel(R) SMBus ASD Mode Configuration	Enable as GPP_C2	This setting determines the native mode

#	Parameter	Platform	Settings
2	**SMBus / SMLink Configuration**		
	Intel® SMLink0 MCTP Address Enabled **Value: Yes/No** This setting configures the Intel® SMLink0b MCTP Address. ***Note:*** This setting is only used for testing.	TGL-H	No
	Intel® SMBus ASD Address - This setting configures the Intel® SMBus Alert Sending device Address. For details see Tiger Lake LP SPI Programming guide for further details.	TGL-H	0x00000000
	Intel® SMBus ASD Address Enable **Values: Yes/No** - This setting enables / disables the Intel® SMBus Alert Sending device. For details see Tiger Lake LP SPI Programming guide for further details.	TGL-H	No
	Intel® SMBus Subsystem Vendor & device ID for ASF - This setting configures the Intel® SMBus Subsystem Vendor & device ID for ASF. For details see Tiger Lake LP SPI Programming guide further details.	TGL-H	0x00000000
	Intel® SMBus I2C Address - This setting configures the Intel® SMBus I2C Address. **Note:** This setting is only used for testing purposes. The recommended setting is "0000000".	TGL-H	0x00000000

Table 2-10. - Internal PCH Buses (Sheet 3 of 5)

	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".	TGL-H	No
	SMBus / SMLink TCO Slave Connection **Values: Intel® SMBus, SMLink0** - This setting configures the TCO Slave connection to ether the Intel® SMBus or SMLink0. For further details see Tiger Lake LP Platform Controller Hub EDS.	TGL-H	Intel® SMBus
	SMLink0 Enabled **Values: Yes/No** - This setting enables / disables SMLink0 interface. For further details see Tiger Lake LP Platform Controller Hub EDS.	TGL-H	Yes
	SMLink0 Frequency **Values: 100KHz, 400KHz, 1 MHz** - This setting determines the frequency at which the SMLink0 will operate. **Note:** The recommended setting is "1MHz".	TGL-H	1 MHz
	SMLink1 I2C Target Address - This setting configures SMLink1 I2C Target Address. For further details see Tiger Lake LP Platform Controller Hub EDS.	TGL-H	0x00000000
	SMLink1 I2C Target Address Enabled **Values: Yes/No** - This setting configures SMLink1 I2C Target Address. For further details see Tiger Lake LP Platform Controller Hub EDS.	TGL-H	No
	SMLink1 GP Target Address - This setting configures SMLink1 GP Target Address. For further details see Tiger Lake LP Platform Controller Hub EDS.	TGL-H	0x00000000
	SMLink1 GP Target Address Enabled **Values: Yes/No** - This setting enables / disables SMLink1 GP Target Address interface. For further details see Tiger Lake LP Platform Controller Hub EDS. **Note:** This setting must be set to "Yes" if using PCH / MCP Thermal reporting.	TGL-H	Yes
	SMLink1 Enabled **Values: Yes/No** - This setting enables / disables SMLink1 interface. For further details see Tiger Lake LP Platform Controller Hub EDS. **Note:** This setting must be set to "Yes" if using PCH / MCP Thermal reporting.	TGL-H	Yes
	SMLink1 Frequency **Values: 100KHz, 400KHz, 1 MHz** - This setting determines the frequency at which the SMLink1 will operate. **Note:** The recommended setting is "100KHz".	TGL-H	100 KHz
	Intel® SMBus ASD Mode Configuration This setting determines the native mode of operation for the Intel® SMBus ASD signal.	TGL-H	Enable as GPP_C2

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

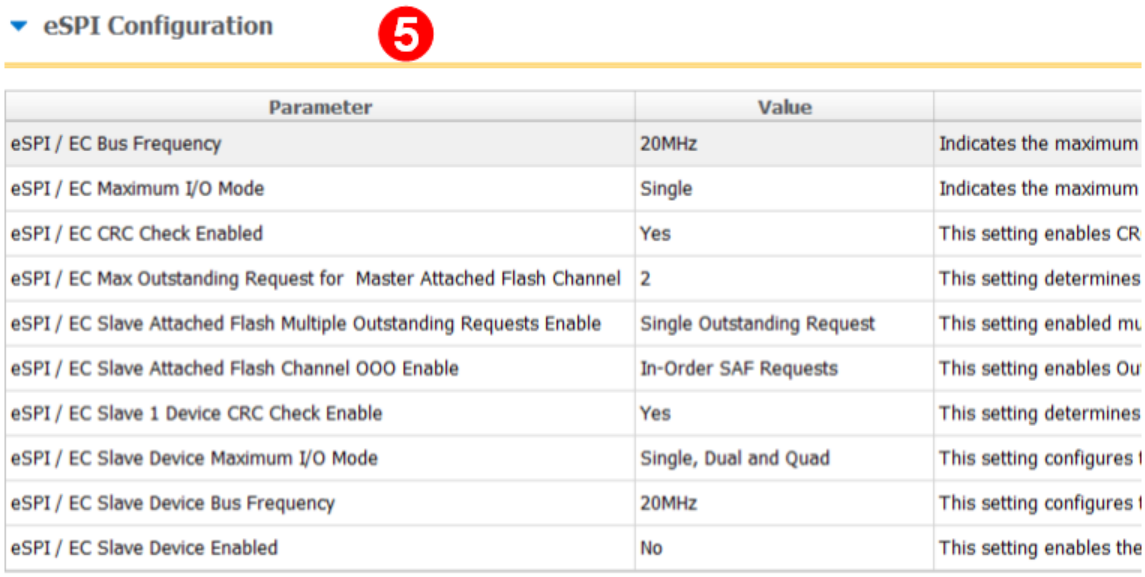


#	Parameter	Platform	Settings
3	**DMI Configuration**		
	DMI Lane Reversal **Values: Yes/No** - This setting allows the DMI Lane signals to be reversed. For further details see Tiger Lake LP Platform Controller Hub EDS.	TGL-H	No

Table 2-10. - Internal PCH Buses (Sheet 4 of 5)

	DMI Port Staggering **Values: Yes/No** - This setting configures DMI for Port Staggering. For further details see Tiger Lake LP Platform Controller Hub EDS.	TGL-H	Yes
	DMI AC Coupling **Values: Yes/No -** This determines if DMI is operating in AC or DC coupled mode	TGL-H	No
	DMI Lane Width **Values: Disabled, x1, x2, x4** - This setting determines the number of DMI lanes available	TGL-H	DMI x8

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



Parameter	Value	
eSPI / EC Bus Frequency	20MHz	Indicates the maximum
eSPI / EC Maximum I/O Mode	Single	Indicates the maximum
eSPI / EC CRC Check Enabled	Yes	This setting enables CR
eSPI / EC Max Outstanding Request for Master Attached Flash Channel	2	This setting determines
eSPI / EC Slave Attached Flash Multiple Outstanding Requests Enable	Single Outstanding Request	This setting enabled mu
eSPI / EC Slave Attached Flash Channel OOO Enable	In-Order SAF Requests	This setting enables Ou
eSPI / EC Slave 1 Device CRC Check Enable	Yes	This setting determines
eSPI / EC Slave Device Maximum I/O Mode	Single, Dual and Quad	This setting configures t
eSPI / EC Slave Device Bus Frequency	20MHz	This setting configures t
eSPI / EC Slave Device Enabled	No	This setting enables the

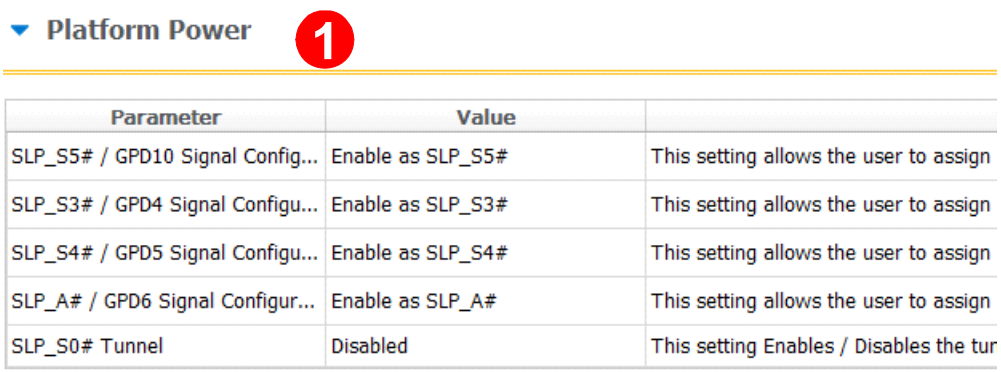
#	Parameter	Platform	Settings
5	**eSPI Configuration**		
	eSPI / EC Bus Frequency **Value: 20MHz, 25MHz, 33MHz, 50MHz** Indicates the maximum frequency of the eSPI bus that is supported by the eSPI Master and platform configuration (trace length, number of Slaves, etc.). The actual frequency of the eSPI bus will be the minimum of this field and the Slave's maximum frequency advertised in its General Capabilities register.	TGL-H	20MHz
	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.	TGL-H	Single, Dual and Quad
	eSPI / EC CRC Check Enabled **Values: Yes/No** This setting enables CRC checking on eSPI Slave 0 channel.	TGL-H	No
	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.	TGL-H	2

Table 2-10. - Internal PCH Buses (Sheet 5 of 5)

	eSPI / EC Slave Attached Flash Multiple Outstanding Requests Enable **Values: Single Outstanding Request/Multiple Outstanding Requests** This setting enabled multiple outstanding requests for the eSPI / EC Slave Attached Flash device.	TGL-H	Single Outstand-ing Request
	eSPI / EC Slave Attached Flash Channel OOO Enable **Values: In-Order SAF Requests/Out-of-Order SAF Requests** This setting enables Out or Order requests on the eSPI / EC Slave Attached Flash device.	TGL-H	In-Order SAF Requests
	eSPI / EC Slave 1 Device CRC Check Enabled **Values: Yes/No** This setting determines if CRC checking is enabled on the eSPI / EC Slave 1 Device channel.	TGL-H	Yes
	eSPI / EC Slave 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.	TGL-H	Single, Dual and Quad
	eSPI / EC Slave Device Bus Frequency **Values: 20MHz, 25MHz, 33MHz, 50MHz** This setting configures the maximum operating frequency of the Slave device.	TGL-H	20MHz
	eSPI / EC Slave Device Enabled **Values: Yes/No** This setting enables the Slave device on the eSPI interface.	TGL-H	No

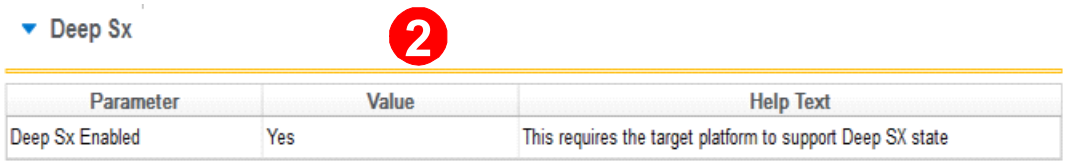
Table 2-11. - Power (Sheet 1 of 2)

Click on Power in the left tabs menu> Platform Power is expanded by default:



#	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. For further details see Tiger Lake LP Platform Controller Hub EDS.	TGL-H	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. For further details see Tiger Lake LP Platform Controller Hub EDS.	TGL-H	SLP_S4#
	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. For further details see Tiger Lake LP Platform Controller Hub EDS.	TGL-H	SLP_S5#
	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. For further details see Tiger Lake LP Platform Controller Hub EDS.	TGL-H	SLP_A#
	SLP_S0# Tunnel This setting Enables / Disables the tunneling of the SLP_S0# pin over ESPI to the EC when in ESPI mode.	TGL-H	Disabled

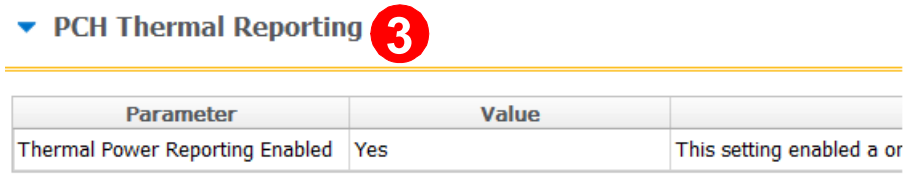
Click on Power in the left tabs menu> Deep Sx is expanded by default:



#	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 Tiger Lake LP Platform Controller Hub EDS. **Note:** Support for Deep Sx is board design dependent.	TGL-H	Yes

Click on Power in the left tabs menu> PCH Thermal Reporting is expanded by default:

Table 2-11. - Power (Sheet 2 of 2)



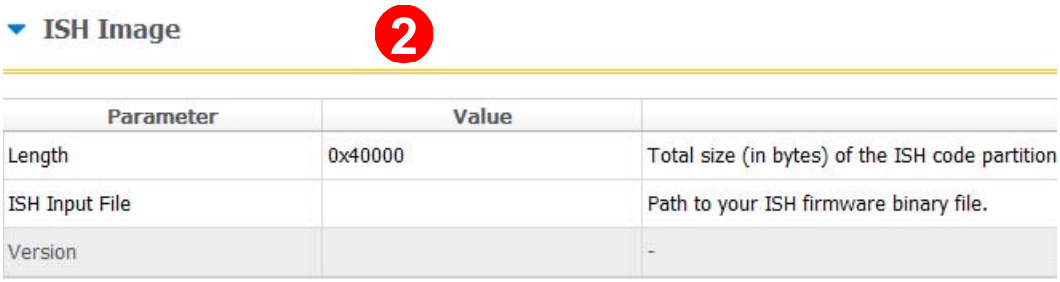
#	Parameter	Platform	Settings
3	**PCH Thermal Reporting**		
	Thermal Power Reporting Enabled This setting enabled a once-per-second timer interrupt is enabled which triggers firmware to report power and temperature information as enabled by configuration registers. Note: When this setting is disabled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

Table 2-12. - Integrated Sensor Hub (Sheet 1 of 2)

Click on Integrated Sensor Hub in the left tabs menu> Integrated Sensor Hub is expanded by default:

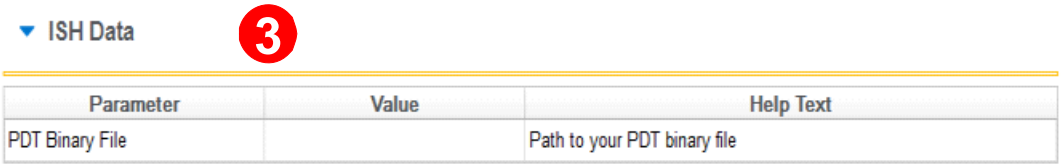
#	Parameter	Platform	Settings
1	**Integrated Sensor Hub**		
	Integrated Sensor Hub Supported **Values: Yes / No** This setting allows customers to disable ISH on the platform.	TGL-H	No
	Integrated Sensor Hub Power Up State **Values: Enabled / Disabled** Field is enabled for editing if "Integrated Sensor Hub Supported" field above is set to "Yes". This setting allows customers to determine the power up state for ISH.	TGL-H	Disabled

Click on Integrated Sensor Hub in the left tabs menu> ISH Image is expanded by default:



#	Parameter	Platform	Settings
2	**ISH Image**		
	Length - Total size (in bytes) of the ISH code partition including reserved space. It is recommended to be at least 256kb.		
	Input File	TGL-H	ISH Binary (Optional)
	Version - This displays the version of ISH		

Click on Integrated Sensor Hub in the left tabs menu> ISH Data is expanded by default:



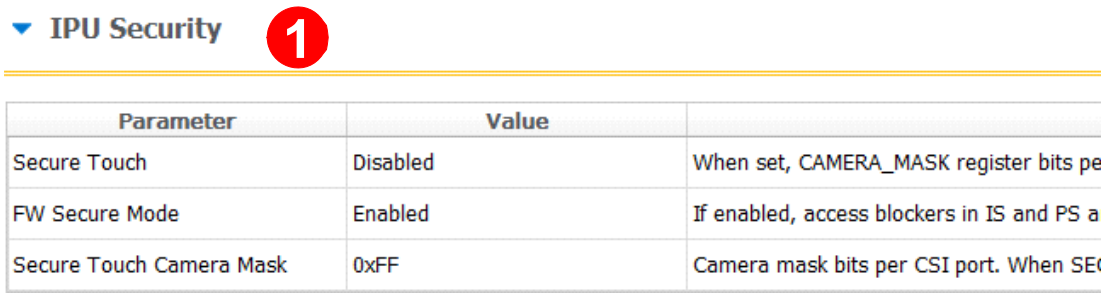
#	Parameter	Platform	Settings

Table 2-12. - Integrated Sensor Hub (Sheet 2 of 2)

3	**Integrated Sensor Hub - ISH Data**		
	PDT Binary File	TGL-H	Path for PDT Binary file

Table 2-13. - Camera

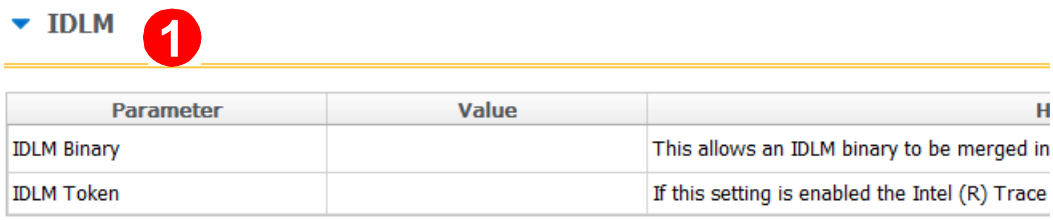
Click on Camera in the left tabs menu> IPU Security is expanded by default:



#	Parameter	Platform	Settings
1	**IPU Security**		
	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.	TGL-H	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.	TGL-H	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.	TGL-H	0xFF

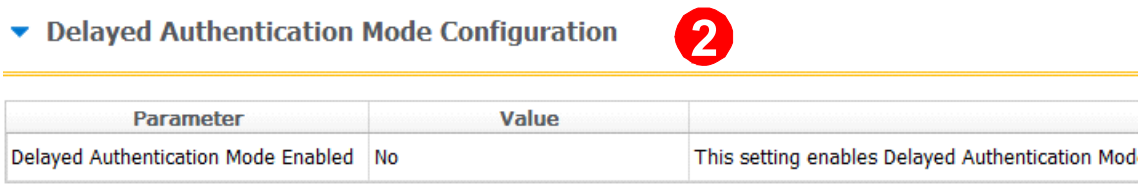
Table 2-14. - Debug (Sheet 1 of 6)

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



#	Parameter	Platform	Settings
1	**IDLM**		
	IDLM Binary This allows an IDLM binary to be merged into output image built by Intel® FIT.	TGL-H	IDLM Binary (Optional)

Click on Debug in the left tabs menu> Delayed Authentication Mode Configuration is expanded by default:



#	Parameter	Platform	Settings
2	**Delayed Authentication Mode Configuration**		
	Delayed Authentication Mode Enabled **Values: Yes / No** - This setting enable / disables Delayed Authentication Mode on the platform.	TGL-H	No

Click on Debug in the left tabs menu> Intel® Trace Hub Technology is expanded by default:

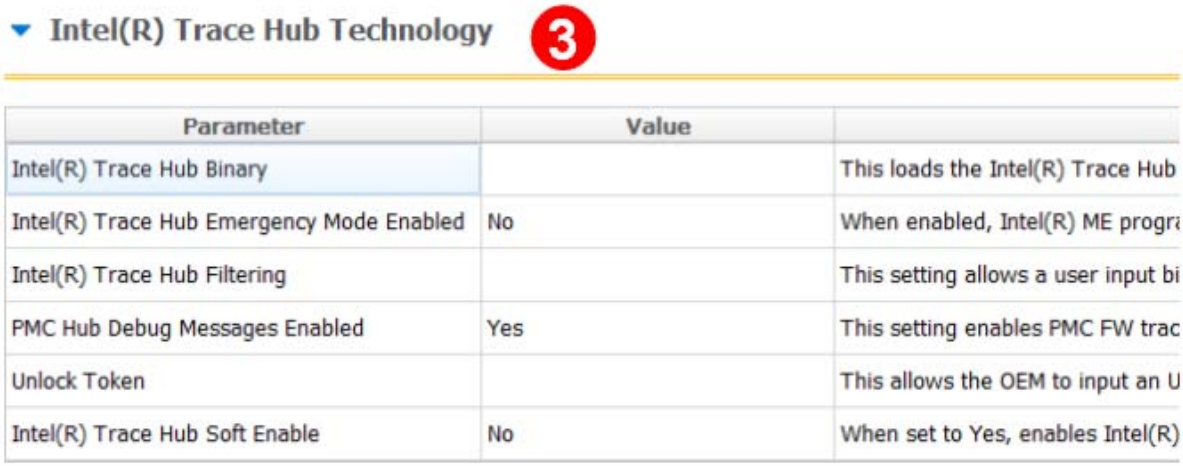
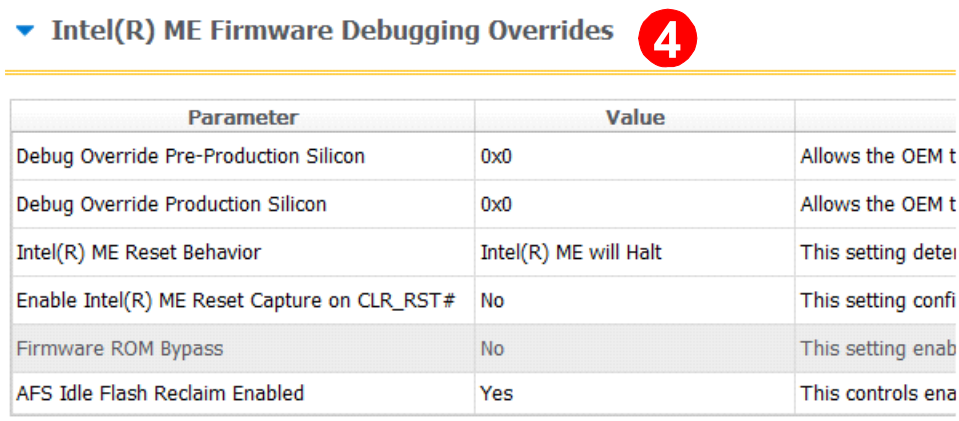


Table 2-14. - Debug (Sheet 2 of 6)

#	Parameter	Platform	Settings
3	**Intel® Trace Hub Technology**		
	Intel® Trace Hub Binary - This loads the Intel® Trace Hub binary that will be merged into the output image generated by the Intel® FIT tool.	TGL-H	Trace Hub Binary
	Intel® Trace Hub Emergency Mode Enabled **Values: Yes / No** - This setting enable / disables Intel® Trace Hub in the firmware base image.	TGL-H	No
	Intel® Trace Hub Filtering This setting allows a user input binary for filtering of output messages for Intel® Trace Hub	TGL-H	Trace Hub Filter Binary (Optional)
	PMC Debug Messages Enabled **Values: Yes / No** - This setting enables/disables the PMC debug messages.	TGL-H	Yes
	Unlock Token This allows the OEM to input an Unlock Token binary file for closed chassis debug.	TGL-H	Unlock Token Binary (Optional)

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

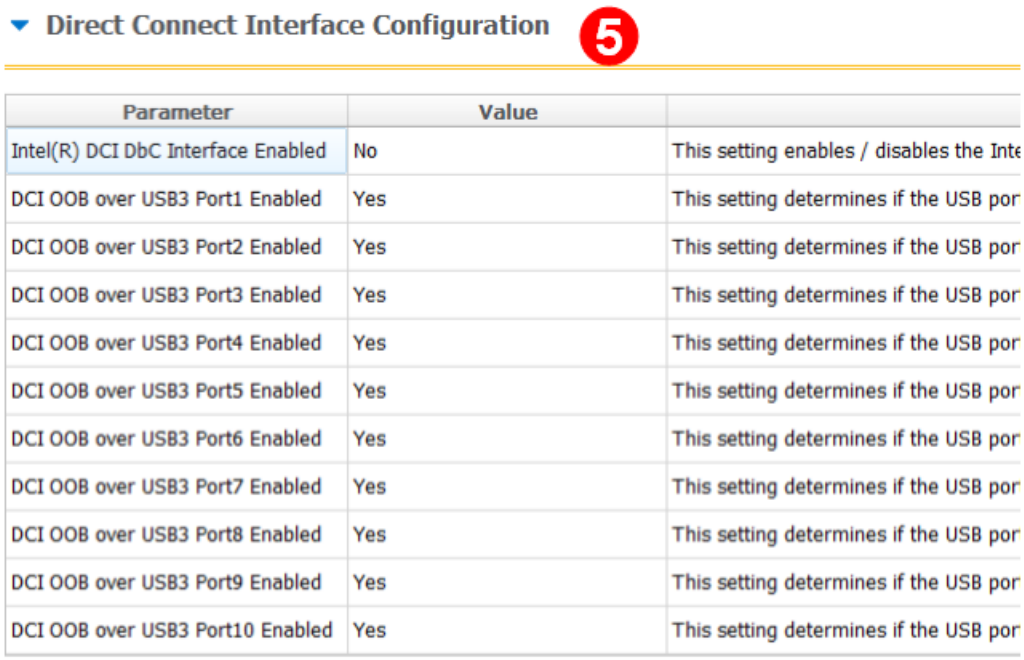


#	Parameter	Platform	Settings
4	**Intel® ME Firmware Debugging Overrides**		
	Debug Override Pre-Production Silicon - Allows the OEM to control FW features to assist with pre-production platform debugging. This control has no effect if used on production silicon. **Bit 0:** Disable DRAM_INIT_DONE (default 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.	TGL-H	0x00000000

Table 2-14. - Debug (Sheet 3 of 6)

	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.	TGL-H	0x00000000
	Intel® ME Reset Behavior **Values: Intel® ME will Halt / Intel® 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. Note: This may block normal Firmware functional flows.	TGL-H	Intel® ME will Halt
	Enable Intel® ME Reset Capture on CLR_RST# **Values: Yes/No** This setting configures Intel® ME behavior when it resets during CL_RST#1. Note: The recommended default for this setting is 'No'	TGL-H	No
	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.	TGL-H	No
	ASF Idle Flash Reclaim Enabled **Values: Yes / No** This controls enabling / disable the Intel® AFS Idle flash reclaim capabilities. ***Note:*** This setting should be used for debug purposes only.	TGL-H	Yes

Click on Debug in the left tabs menu> Direct Connection Interface Configuration is expanded by default:



#	Parameter	Platform	Settings
5	**Direct Connection Interface Configuration** ***Note:*** When any of the DCI BSSB USB3 Port interfaces are enabled the associated USB3 port selection control will be greyed out under the USB3 Port Configuration settings section under the Flex I/O tab		

Table 2-14. - Debug (Sheet 4 of 6)

	Direct Connect Interface (DCI) Enabled **Values: Yes/No** - This setting enables / disables the DCI interface used for Intel® Trace Hub debugging.	TGL-H	No No
	DCI BSSB over USB3 Port 1 Enabled This setting determines if the USB port 1 has BSSB (Boundary Scan Side Band) enabled. ***Note:*** For S0ix and reset flows BSSB should be enabled. ***Note:*** When this setting is enabled the corresponding USB3 Combo Port in the Flex I/O Tab will be Grayed out.	TGL-H	Yes
	DCI BSSB over USB3 Port 2 Enabled This setting determines if the USB port 2 has BSSB (Boundary Scan Side Band) enabled. ***Note:*** For S0ix and reset flows BSSB should be enabled. ***Note:*** When this setting is enabled the corresponding USB3 Combo Port in the Flex I/O Tab will be Grayed out.	TGL-H	Yes
	DCI BSSB over USB3 Port 3 Enabled This setting determines if the USB port 3 has BSSB (Boundary Scan Side Band) enabled. ***Note:*** For S0ix and reset flows BSSB should be enabled. ***Note:*** When this setting is enabled the corresponding USB3 Combo Port in the Flex I/O Tab will be Grayed out.	TGL-H	Yes
	DCI BSSB over USB3 Port 4 Enabled This setting determines if the USB port 4 has BSSB (Boundary Scan Side Band) enabled. ***Note:*** For S0ix and reset flows BSSB should be enabled. ***Note:*** When this setting is enabled the corresponding USB3 Combo Port in the Flex I/O Tab will be Grayed out.	TGL-H	Yes
	DCI BSSB over USB3 Port 5 Enabled This setting determines if the USB port 5 has BSSB (Boundary Scan Side Band) enabled. ***Note:*** For S0ix and reset flows BSSB should be enabled. ***Note:*** When this setting is enabled the corresponding USB3 Combo Port in the Flex I/O Tab will be Grayed out.	TGL-H	Yes
	DCI BSSB over USB3 Port 6 Enabled This setting determines if the USB port 6 has BSSB (Boundary Scan Side Band) enabled. ***Note:*** For S0ix and reset flows BSSB should be enabled. ***Note:*** When this setting is enabled the corresponding USB3 Combo Port in the Flex I/O Tab will be Grayed out.	TGL-H	Yes
	DCI BSSB over USB3 Port 7 Enabled This setting determines if the USB port 7 has BSSB (Boundary Scan Side Band) enabled. ***Note:*** For S0ix and reset flows BSSB should be enabled. ***Note:*** When this setting is enabled the corresponding USB3 Combo Port in the Flex I/O Tab will be Grayed out.	TGL-H	No
	DCI BSSB over USB3 Port 8 Enabled This setting determines if the USB port 8 has BSSB (Boundary Scan Side Band) enabled. ***Note:*** For S0ix and reset flows BSSB should be enabled. ***Note:*** When this setting is enabled the corresponding USB3 Combo Port in the Flex I/O Tab will be Grayed out.	TGL-H	No

Table 2-14. - Debug (Sheet 5 of 6)

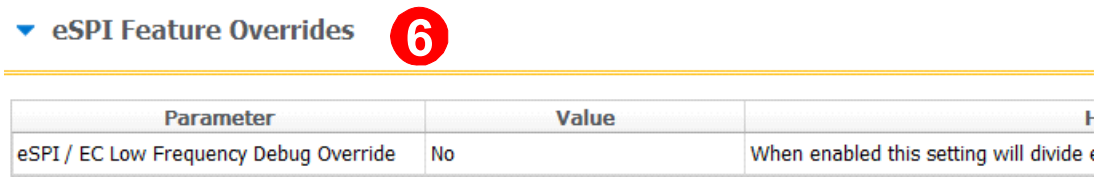
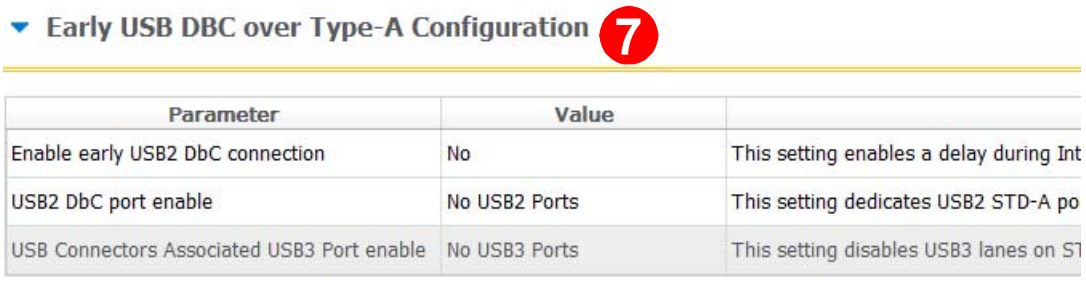
	DCI BSSB over USB3 Port 9 Enabled This setting determines if the USB port 9 has BSSB (Boundary Scan Side Band) enabled. ***Note:*** For S0ix and reset flows BSSB should be enabled. ***Note:*** When this setting is enabled the corresponding USB3 Combo Port in the Flex I/O Tab will be Grayed out.	TGL-H	No
	DCI BSSB over USB3 Port 10 Enabled This setting determines if the USB port 10 has BSSB (Boundary Scan Side Band) enabled. ***Note:*** For S0ix and reset flows BSSB should be enabled. ***Note:*** When this setting is enabled the corresponding USB3 Combo Port in the Flex I/O Tab will be Grayed out.	TGL-H	No
Click on Debug in the left tabs menu> eSPI Feature Overrides is expanded by default:			
			
#	**Parameter**	**Platform**	**Settings**
6	**eSPI Feature Overrides**		
	eSPI / EC Low Frequency Debug Override When enabled this setting will divide eSPI clock frequency by 8. ***Note:*** This setting should only be used for debugging purposes. Leaving this set to "Yes" will impact eSPI performance on the platform.	TGL-H	No
Click on Debug in the left tabs menu> Early USB DBC Type-A Configuration is expanded by default:			
			
#	**Parameter**	**Platform**	**Settings**
7	**Early USB DBC Type-A Configuration**		
	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	TGL-H	No
	USB2 DbC port enable This setting determines which USB2 ports are enabled for Early DbC debugging.	TGL-H	No USB2 Ports

Table 2-14. - Debug (Sheet 6 of 6)

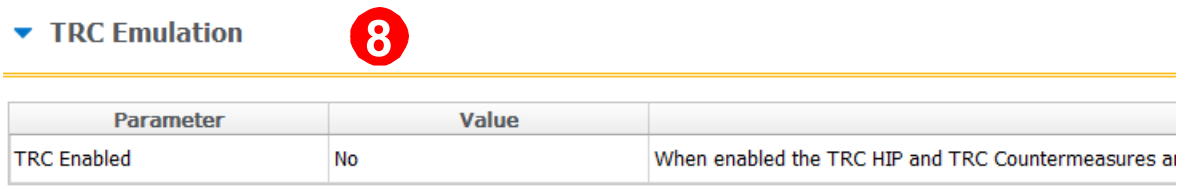
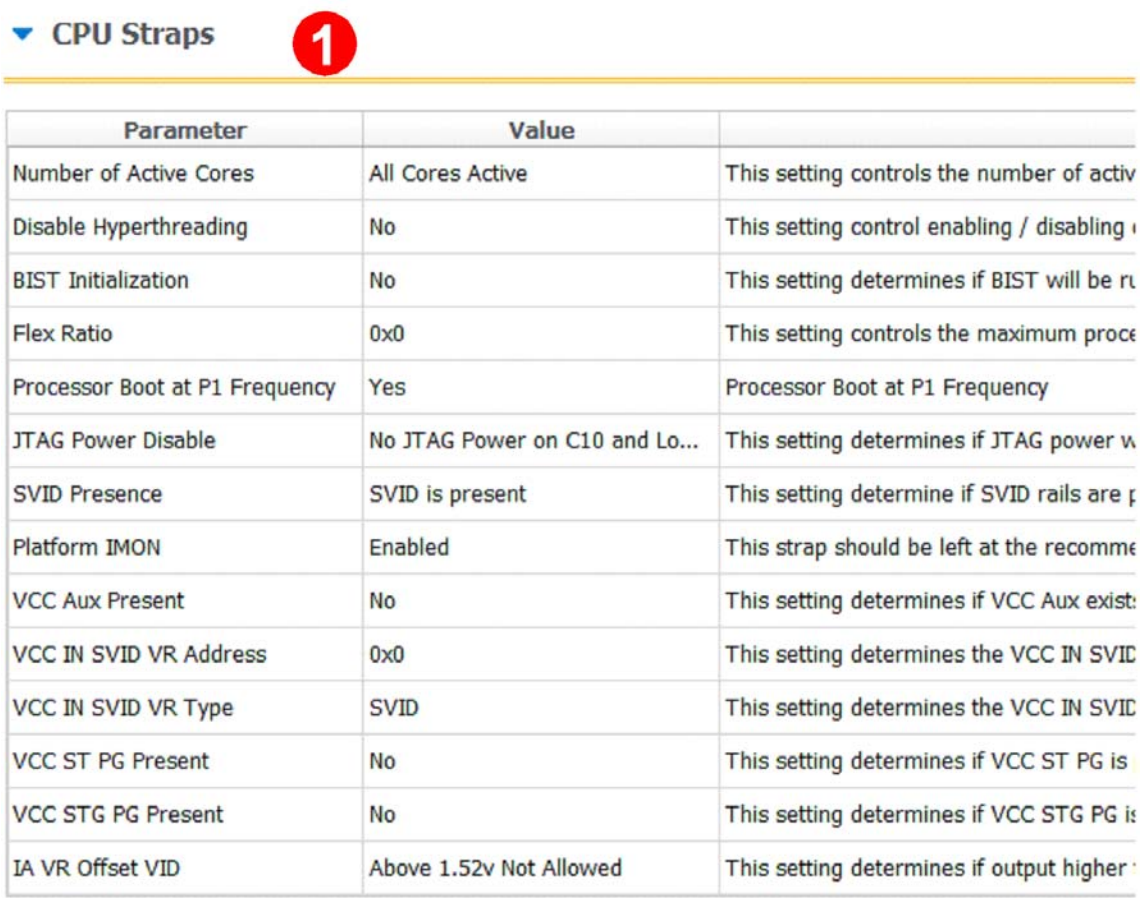
	USB Connectors associated USB3 Port enable This setting determines which USB3 ports goes to the target USB2 ports connector for Early DbC debugging.	TGL-H	No USB3 Ports
Click on Debug in the left tabs menu> Early TRC Emulation is expanded by default:			
			
#	**Parameter**	**Platform**	**Settings**
8	**TRC Emulation**		
	TRC Enabled (FPF) **Values: Yes / No** When enabled the TRC HIP and TRC Countermeasures are enabled. When manufacture is completed, this value is burned into an FPF. ***Note:*** This setting should be set to "Yes" for production platforms.	TGL-H	No

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

Click on CPU Straps in the left tabs menu> CPU Straps are expanded by default:



CPU Straps 1

Parameter	Value	
Number of Active Cores	All Cores Active	This setting controls the number of activ
Disable Hyperthreading	No	This setting control enabling / disabling
BIST Initialization	No	This setting determines if BIST will be ru
Flex Ratio	0x0	This setting controls the maximum proce
Processor Boot at P1 Frequency	Yes	Processor Boot at P1 Frequency
JTAG Power Disable	No JTAG Power on C10 and Lo...	This setting determines if JTAG power w
SVID Presence	SVID is present	This setting determine if SVID rails are p
Platform IMON	Enabled	This strap should be left at the recomme
VCC Aux Present	No	This setting determines if VCC Aux exist
VCC IN SVID VR Address	0x0	This setting determines the VCC IN SVID
VCC IN SVID VR Type	SVID	This setting determines the VCC IN SVID
VCC ST PG Present	No	This setting determines if VCC ST PG is
VCC STG PG Present	No	This setting determines if VCC STG PG is
IA VR Offset VID	Above 1.52v Not Allowed	This setting determines if output higher

#	Parameter	Platform	Settings
1	**CPU Straps - CPU Straps**		
	Number of Active Cores **Values: All, 1, 2, 3, 4, 5, 6, 7, 8, 9** This setting controls the number of active processor cores. ***Note:*** This strap is intended for debugging purposes only. See BIOS Spec for more details on enabling or disabling processor cores.	TGL-H	All Cores Active
	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.	TGL-H	No
	BIST Initialization **Values: Yes / No** This setting determines if BIST will be run at platform reset after BIOS requested actions. ***Note:*** This strap is intended for debugging purposes only.	TGL-H	No

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

	Flex Ratio This setting controls the maximum processor non-turbo ratio. ***Note:*** This strap is intended for debugging purposes only. See BIOS Spec for more details on maximum processor non-turbo ratio configuration.	TGL-H	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.	TGL-H	Yes
	JTAG Power Disable **Values: Yes - JTAG Power on C10 and Lower/No - No Power on C10 and Lower** This setting determines if JTAG power will be maintained on C10 or lower power states. ***Note:*** This strap is intended for debugging purposes only.	TGL-H	No JTAG Power on C10 and Lower
	SVID Presence **Value: SVID Present/SVID Not Present** This setting determines if SVID rails are present on the platform. See Processor EDS for details.	TGL-H	SVID Present
	Platform IMON **Value: Enabled/Disabled** ***Note:*** This strap should be left at the recommended default setting.	TGL-H	Enabled
	VCC Aux Present **Value: Yes/No** This setting determines if VCC Aux exists as a separate VR.	TGL-H	Yes
	VCCIN SVID Address This setting determines the VCCIN SVID Address. See Processor EDS for details. **Note:** This strap should be left at the recommended default setting.	TGL-H	0x0
	VCC SVID VR Type **Values: SVID/Fixed VR** This setting determines the VCC IN SVID VR Type. See Processor EDS for details.	TGL-H	SVID
	VCC ST PG Present **Values: Yes/No** This setting determines if VCC ST PG is present on the platform.	TGL-H	No
	VCC STG PG Present **Values: Yes/No** This setting determines if VCC STG PG is present on the platform.	TGL-H	No
	IA VR Offset VID **Values: Above 1.52v Not Allowed/Above 1.52v Allowed** This setting determines if output higher than 1.52v is allowed for 8 or higher core count processors.	TGL-H	Above 1.52v Not Allowed

Table 2-16. - Flex I/O Straps (Sheet 1 of 21)

Click on Flex I/O in the left tabs menu> Intel® RST for PCIe Configuration is expanded by default:

Intel(R) RST for PCIe Configuration 1

Parameter	Value	
PCIe Controller 3 Port 4 SRIS Enabled	No	This is used to configure SRIS Port 4 for
PCIe Controller 3 Port 3 SRIS Enabled	No	This is used to configure SRIS Port 1 for
PCIe Controller 3 Port 2 SRIS Enabled	No	This is used to configure SRIS Port 2 for
PCIe Controller 3 Port 1 SRIS Enabled	No	This is used to configure SRIS Port 1 for
PCIe Controller 5 Port 4 SRIS Enabled	No	This is used to configure SRIS Port 4 for
PCIe Controller 5 Port 3 SRIS Enabled	No	This is used to configure SRIS Port 3 for
PCIe Controller 5 Port 2 SRIS Enabled	No	This is used to configure SRIS Port 2 for
PCIe Controller 5 Port 1 SRIS Enabled	No	This is used to configure SRIS Port 1 for
PCIe Controller 6 Port 4 SRIS Enabled	No	This is used to configure SRIS Port 4 for
PCIe Controller 6 Port 3 SRIS Enabled	No	This is used to configure SRIS Port 3 for
PCIe Controller 6 Port 2 SRIS Enabled	No	This is used to configure SRIS Port 2 for
PCIe Controller 6 Port 1 SRIS Enabled	No	This is used to configure SRIS Port 1 for
Intel(R) RST for PCIe-C3 Select x2 or x4	x2	This is used to configure NAND Cycle ro
Intel(R) RST for PCIe-C2 Select x2 or x4	x2	This is used to configure NAND Cycle ro
Intel(R) RST for PCIe-C1 Select x2 or x4	x2	This is used to configure NAND Cycle ro
Intel® RST for PCIe Controller 1	1x4	This is used to configure PCIe Controller
Intel® RST for PCIe Controller 2	1x4	This is used to configure PCIe Controller
Intel® RST for PCIe Controller 3	2x2	This is used to configure PCIe Controller

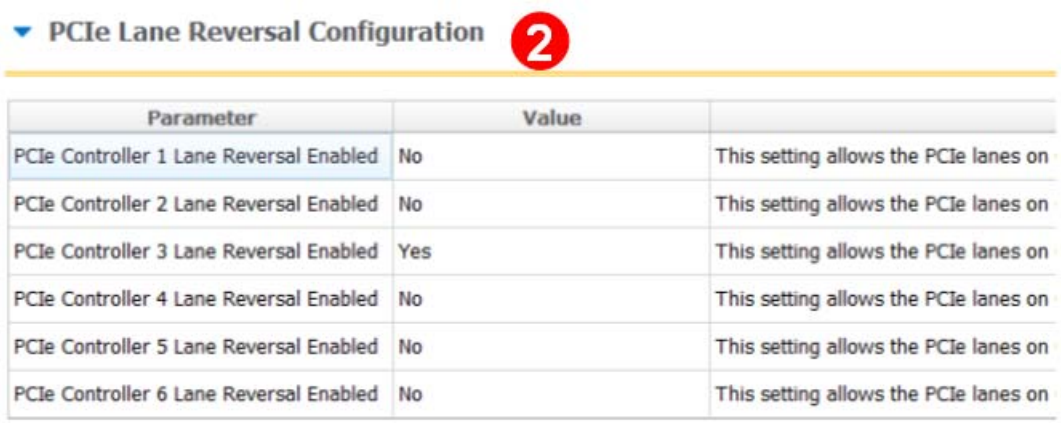
#	Parameter	Platform	Settings
1	**Intel® RST for PCIe Configuration**		
	PCIe Controller 3 Port 1 SRIS Enabled **Values: Yes/ No** - This is used to configure SRIS Port 1 for Intel® RST for PCIe on PCIe Controller 3. **Note:** Configuration of this setting is only required if the NVM device will be connected external SATA Express cable.	TGL-H	No
	PCIe Controller 3 Port 2 SRIS Enabled **Values: Yes/ No** - This is used to configure SRIS Port 2 for Intel® RST for PCIe on PCIe Controller 3. **Note:** Configuration of this setting is only required if the NVM device will be connected external SATA Express cable.	TGL-H	No

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

	PCIe Controller 3 Port 3 SRIS Enabled **Values: Yes/ No** - This is used to configure SRIS Port 3 for Intel® RST for PCIe on PCIe Controller 3. **Note:** Configuration of this setting is only required if the NVM device will be connected external SATA Express cable.	TGL-H	No
	PCIe Controller 3 Port 4 SRIS Enabled **Values: Yes/ No** - This is used to configure SRIS Port 4 for Intel® RST for PCIe on PCIe Controller 3. **Note:** Configuration of this setting is only required if the NVM device will be connected external SATA Express cable.	TGL-H	No
	PCIe Controller 5 Port 1 SRIS Enabled **Values: Yes/ No** - This is used to configure SRIS Port 1 for Intel® RST for PCIe on PCIe Controller 5. **Note:** Configuration of this setting is only required if the NVM device will be connected external SATA Express cable.	TGL-H	No
	PCIe Controller 5 Port 2 SRIS Enabled **Values: Yes/ No** - This is used to configure SRIS Port 2 for Intel® RST for PCIe on PCIe Controller 5. **Note:** Configuration of this setting is only required if the NVM device will be connected external SATA Express cable.	TGL-H	No
	PCIe Controller 5 Port 3 SRIS Enabled **Values: Yes/ No** - This is used to configure SRIS Port 3 for Intel® RST for PCIe on PCIe Controller 5. **Note:** Configuration of this setting is only required if the NVM device will be connected external SATA Express cable.	TGL-H	No
	PCIe Controller 5 Port 4 SRIS Enabled **Values: Yes/ No** - This is used to configure SRIS Port 4 for Intel® RST for PCIe on PCIe Controller 5. **Note:** Configuration of this setting is only required if the NVM device will be connected external SATA Express cable.	TGL-H	No
	PCIe Controller 6 Port 1 SRIS Enabled **Values: Yes/ No** - This is used to configure SRIS Port 1 for Intel® RST for PCIe on PCIe Controller 6. **Note:** Configuration of this setting is only required if the NVM device will be connected external SATA Express cable.	TGL-H	No
	PCIe Controller 6Port 2 SRIS Enabled **Values: Yes/ No** - This is used to configure SRIS Port 2 for Intel® RST for PCIe on PCIe Controller 6. **Note:** Configuration of this setting is only required if the NVM device will be connected external SATA Express cable.	TGL-H	No
	PCIe Controller 6 Port 3 SRIS Enabled **Values: Yes/ No** - This is used to configure SRIS Port 3 for Intel® RST for PCIe on PCIe Controller 6. **Note:** Configuration of this setting is only required if the NVM device will be connected external SATA Express cable.	TGL-H	No
	PCIe Controller 6 Port 4 SRIS Enabled **Values: Yes/ No** - This is used to configure SRIS Port 4 for Intel® RST for PCIe on PCIe Controller 6. **Note:** Configuration of this setting is only required if the NVM device will be connected external SATA Express cable.	TGL-H	No
	Intel® RST for PCIe-C1 Select x2 or x4 **Values: x2, x4** - This is used to configure NAND Cycle routers for the Intel® RST for PCIe interface as either x2 or x4 lane operation on PCIe Controller 1.	TGL-H	x2
	Intel® RST for PCIe-C2 Select x2 or x4 **Values: x2, x4** - This is used to configure NAND Cycle routers for the Intel® RST for PCIe interface as either x2 or x4 lane operation on PCIe Controller 2.	TGL-H	x2
	Intel® RST for PCIe-C3 Select x2 or x4 **Values: x2, x4** - This is used to configure NAND Cycle routers for the Intel® RST for PCIe interface as either x2 or x4 lane operation on PCIe Controller 3.	TGL-H	x2

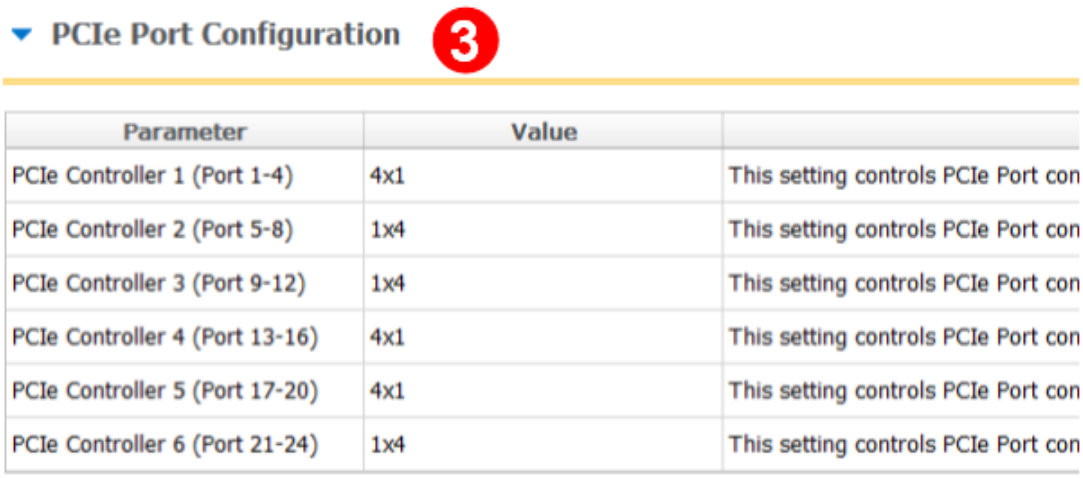
Table 2-16. - Flex I/O Straps (Sheet 3 of 21)

	Intel® RST for PCIe Controller 1 **Values: 1x4, 2x2** - This is used to configure PCIe Controller 1 for Intel® RST for PCIe interface as either x2 or x4 lane operation on PCIe Controller 3.	TGL-H	1x4
	Intel® RST for PCIe Controller 2 **Values: 1x4, 2x2** - This is used to configure PCIe Controller 2 for Intel® RST for PCIe interface as either x2 or x4 lane operation on PCIe Controller 2.	TGL-H	1x4
	Intel® RST for PCIe Controller 3 **Values: 1x4, 2x2** - This is used to configure PCIe Controller 3 for Intel® RST for PCIe interface as either x2 or x4 lane operation on PCIe Controller 3.	TGL-H	1x4
Click on Flex I/O in the left tabs menu> PCIe Lane Reversal Configuration is expanded by default:			



#	Parameter	Platform	Settings
2	**PCIe Lane Reversal Configuration**		
	PCIe Controller 1 Lane Reversal Enabled **Values: Yes/ No** - This setting allows the PCIe lanes on Controller 1 to be reversed. **Note:** Refer to EDS for PCIe supported port configurations.	TGL-H	No
	PCIe Controller 2 Lane Reversal Enabled **Values: Yes/ No** - This setting allows the PCIe lanes on Controller 2 to be reversed. **Note:** Refer to EDS for PCIe supported port configurations.	TGL-H	No
	PCIe Controller 3 Lane Reversal Enabled **Values: Yes/ No** - This setting allows the PCIe lanes on Controller 3 to be reversed. **Note:** Refer to EDS for PCIe supported port configurations.	TGL-H	Yes
	PCIe Controller 4 Lane Reversal Enabled **Values: Yes/ No** - This setting allows the PCIe lanes on Controller 4 to be reversed. **Note:** Refer to EDS for PCIe supported port configurations.	TGL-H	No
	PCIe Controller 5 Lane Reversal Enabled **Values: Yes/ No** - This setting allows the PCIe lanes on Controller 5 to be reversed. **Note:** Refer to EDS for PCIe supported port configurations.	TGL-H	No
	PCIe Controller 6 Lane Reversal Enabled **Values: Yes/ No** - This setting allows the PCIe lanes on Controller 6 to be reversed. **Note:** Refer to EDS for PCIe supported port configurations.	TGL-H	No
Click on Flex I/O in the left tabs menu> PCIe Port Configuration is expanded by default:			

Table 2-16. - Flex I/O Straps (Sheet 4 of 21)



PCIe Port Configuration 3

Parameter	Value	
PCIe Controller 1 (Port 1-4)	4x1	This setting controls PCIe Port con
PCIe Controller 2 (Port 5-8)	1x4	This setting controls PCIe Port con
PCIe Controller 3 (Port 9-12)	1x4	This setting controls PCIe Port con
PCIe Controller 4 (Port 13-16)	4x1	This setting controls PCIe Port con
PCIe Controller 5 (Port 17-20)	4x1	This setting controls PCIe Port con
PCIe Controller 6 (Port 21-24)	1x4	This setting controls PCIe Port con

#	Parameter	Platform	Settings
3	**PCIe Port Configuration**		
	PCIe Controller 1 (Port 1-4) **Values: 4x1, (1x2, 2x1), 2x2, 1x4** - This setting controls PCIe Port configurations for PCIe Controller 1. For further details see Tiger Lake LP Platform Controller Hub EDS.	TGL-H	1x4
	PCIe Controller 2 (Port 5-8) **Values: 4x1, (1x2, 2x1), 2x2, 1x4** - This setting controls PCIe Port configurations for PCIe Controller 2. For further details see Tiger Lake LP Platform Controller Hub EDS.	TGL-H	4x1
	PCIe Controller 3 (Port 9-12) **Values: 4x1, (1x2, 2x1), 2x2, 1x4** - This setting controls PCIe Port configurations for PCIe Controller 3. For further details see Tiger Lake LP Platform Controller Hub EDS.	TGL-H	1x4
	PCIe Controller 4 (Port 13-16) **Values: 4x1, (1x2, 2x1), 2x2, 1x4** - This setting controls PCIe Port configurations for PCIe Controller 4. For further details see Tiger Lake LP Platform Controller Hub EDS.	TGL-H	4x1
	PCIe Controller 5 (Port 17-20) **Values: 4x1, (1x2, 2x1), 2x2, 1x4** - This setting controls PCIe Port configurations for PCIe Controller 5. For further details see Tiger Lake LP Platform Controller Hub EDS.	TGL-H	1x4
	PCIe Controller 6 (Port 21-24) **Values: 4x1, (1x2, 2x1), 2x2, 1x4** - This setting controls PCIe Port configurations for PCIe Controller 6. For further details see Tiger Lake LP Platform Controller Hub EDS.	TGL-H	1x4
Click on Flex I/O in the left tabs menu> SATA / PCIe Combo Port Configuration is expanded by default:			

Table 2-16. - Flex I/O Straps (Sheet 5 of 21)

SATA / PCIe Combo Port Configuration 4

Parameter	Value	
SATA / PCIe Combo Port 0	PCIe	This setting configur
SATA / PCIe Combo Port 1	GPIO Polarity PCIe	This setting configur
SATA / PCIe Combo Port 2	PCIe	This setting configur
SATA / PCIe Combo Port 3	PCIe	This setting configur
SATA / PCIe Combo Port 4	SATA	This setting configur
SATA / PCIe Combo Port 5	SATA	This setting configur
SATA / PCIe Combo Port 6	SATA	This setting configur
SATA / PCIe Combo Port 7	SATA	This setting configur
SATA / PCIe Combo Port 8	SATA	This setting configur
SATA / PCIe Combo Port 9	SATA	This setting configur
SATA / PCIe Combo Port 0 and 2 Mode Select	PCIe CLKREQ#	The corresponding C
SATA / PCIe Combo Port 1 and 3 Mode Select	PCIe CLKREQ#	The corresponding C
SATA / PCIe Combo Port 4 Mode Select	PCIe CLKREQ#	The corresponding C
SATA / PCIe Combo Port 5 Mode Select	PCIe CLKREQ#	The corresponding C
SATA / PCIe Combo Port 6 Mode Select	PCIe CLKREQ#	The corresponding C
SATA / PCIe Combo Port 7 Mode Select	PCIe CLKREQ#	The corresponding C
SATA / PCIe Combo Port 8 Mode Select	PCIe CLKREQ#	The corresponding C
SATA / PCIe Combo Port 9 Mode Select	PCIe CLKREQ#	The corresponding C

#	Parameter	Platform	Settings
4	**SATA / PCIe Combo Port Configuration**		
	SATA / PCIe Combo Port 0 **Values: SATA, PCIe (or GbE), GPIO** - This setting configures the PCIe port to operate as either: PCIe Port 11 or SATA Port 0 For further details on Flex I/O see Comet Lake H Platform Controller Hub EDS.	TGL-H	PCIe

Table 2-16. - Flex I/O Straps (Sheet 6 of 21)

	SATA / PCIe Combo Port 1 **Values: SATA, PCIe, GPIO Polarity PCIe, GPIO Polarity SATA** - This setting configures the PCIe port to operate as either: PCIe Port 12 or SATA Port 1a For further details on Flex I/O see Comet Lake H Platform Controller Hub EDS. ***Note:*** This port is shared with GbE Port select if PCIe Port 12 has been selected for Intel® Integrated LAN this port setting will be grayed out.	TGL-H	GPIO Polarity PCIe
	SATA / PCIe Combo Port 2 **Values: SATA, PCIe, GPIO Polarity PCIe, GPIO Polarity SATA** - This setting configures the PCIe port to operate as either: PCIe Port 13 or SATA Port 0b For further details on Flex I/O see Comet Lake H Platform Controller Hub EDS. ***Note:*** This port is shared with GbE Port select if PCIe Port 13 has been selected for Intel® Integrated LAN this port setting will be grayed out.	TGL-H	PCIe
	SATA / PCIe Combo Port 3 **Values: SATA, PCIe, GPIO Polarity PCIe, GPIO Polarity SATA -** This setting configures the PCIe port to operate as either: PCIe Port 14 or SATA Port 1b For further details on Flex I/O see Comet Lake H Platform Controller Hub EDS.	TGL-H	PCIe
	SATA / PCIe Combo Port 4 **Values: SATA, PCIe, GPIO Polarity PCIe, GPIO Polarity SATA -** This setting configures the PCIe port to operate as either: PCIe Port 15 or SATA Port 2 For further details on Flex I/O see Comet Lake H Platform Controller Hub EDS.	TGL-H	SATA
	SATA / PCIe Combo Port 5 **Values: SATA, PCIe, GPIO Polarity PCIe, GPIO Polarity SATA -** This setting configures the PCIe port to operate as either: PCIe Port 16 or SATA Port 3 For further details on Flex I/O see Comet Lake H Platform Controller Hub EDS.	TGL-H	SATA
	SATA / PCIe Combo Port 6 **Values: SATA, PCIe, GPIO Polarity PCIe, GPIO Polarity SATA -** This setting configures the PCIe port to operate as either: PCIe Port 17 or SATA Port 4 For further details on Flex I/O see Comet Lake H Platform Controller Hub EDS.	TGL-H	GPIO Polarity PCIe
	SATA / PCIe Combo Port 7 **Values: SATA, PCIe, GPIO Polarity PCIe, GPIO Polarity SATA -** This setting configures the PCIe port to operate as either: PCIe Port 18 or SATA Port 5 For further details on Flex I/O see Comet Lake H Platform Controller Hub EDS.	TGL-H	PCIe
	SATA / PCIe Combo Port 8 **Values: SATA, PCIe, GPIO Polarity PCIe, GPIO Polarity SATA -** This setting configures the PCIe port to operate as either: PCIe Port 19 or SATA Port 6 For further details on Flex I/O see Comet Lake H Platform Controller Hub EDS. ***Note:*** **Workstation / Server Only**	TGL-H	PCIe
	SATA / PCIe Combo Port 9 **Values: SATA, PCIe, GPIO Polarity PCIe, GPIO Polarity SATA -** This setting configures the PCIe port to operate as either: PCIe Port 20 or SATA Port 7 For further details on Flex I/O see Comet Lake H Platform Controller Hub EDS. ***Note:*** **Workstation / Server Only**	TGL-H	PCIe
	SATA / PCIe Combo Port 0 and 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 0 Mode Select is configured to SATA	TGL-H	PCIe CLKREQ#

Table 2-16. - Flex I/O Straps (Sheet 7 of 21)

	SATA / PCIe Combo Port 1 and 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 1 Mode Select is configured to SATA	TGL-H	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	TGL-H	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	TGL-H	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	TGL-H	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	TGL-H	PCIe CLKREQ#
	SATA / PCIe Combo Port 8 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 8 Mode Select is configured to SATA	TGL-H	PCIe CLKREQ#
	SATA / PCIe Combo Port 9 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 9 Mode Select is configured to SATA	TGL-H	PCIe CLKREQ#
Click on Flex I/O in the left tabs menu> USB3 Port Configuration is expanded by default:			

Table 2-16. - Flex I/O Straps (Sheet 8 of 21)

USB3 Port Configuration 5

Parameter	Value	
USB3 / PCIe Combo Port 0	USB3	This setting configures the PCIe port to operat
USB3 / PCIe Combo Port 1	USB3	This setting configures the PCIe port to operat
USB3 / PCIe Combo Port 2	USB3	This setting configures the PCIe port to operat
USB3 / PCIe Combo Port 3	USB3	This setting configures the PCIe port to operat
USB3 Port 1 Connector Type Select	Type C	This setting configures the physical connector t
USB3 Port 2 Connector Type Select	Type C	This setting configures the physical connector t
USB3 Port 3 Connector Type Select	Type C	This setting configures the physical connector t
USB3 Port 4 Connector Type Select	Type C	This setting configures the physical connector t
USB3 Port 5 Connector Type Select	Type C	This setting configures the physical connector t
USB3 Port 6 Connector Type Select	Type C	This setting configures the physical connector t
USB3 Port 7 Connector Type Select	Type A / Type C	This setting configures the physical connector t
USB3 Port 8 Connector Type Select	Type A / Type C	This setting configures the physical connector t
USB3 Port 9 Connector Type Select	Type A / Type C	This setting configures the physical connector t
USB3 Port 10 Connector Type Select	Type A / Type C	This setting configures the physical connector t
USB Type AB Mode Select	USB Type AB HW Select	This setting determines how the USB Type AB
USB3 Port 1 Speed Capability	USB 3.1 Gen2	This setting determines the USB3 Port 1 speed
USB3 Port 2 Speed Capability	USB 3.1 Gen2	This setting determines the USB3 Port 2 speed
USB3 Port 3 Speed Capability	USB 3.1 Gen2	This setting determines the USB3 Port 3 speed
USB3 Port 4 Speed Capability	USB 3.1 Gen2	This setting determines the USB3 Port 4 speed
USB3 Port 5 Speed Capability	USB 3.1 Gen2	This setting determines the USB3 Port 5 speed
USB3 Port 6 Speed Capability	USB 3.1 Gen2	This setting determines the USB3 Port 6 speed
USB3 Port 7 Speed Capability	USB 3.1 Gen2	This setting determines the USB3 Port 7 speed
USB3 Port 8 Speed Capability	USB 3.1 Gen2	This setting determines the USB3 Port 8 speed
USB3 Port 9 Speed Capability	USB 3.1 Gen2	This setting determines the USB3 Port 9 speed
USB3 Port 10 Speed Capability	USB 3.1 Gen2	This setting determines the USB3 Port 10 spee

#	Parameter	Platform	Settings
5	**USB3 Port Configuration**		

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

	USB3 / PCIe Combo Port 0 **Values: PCIe (or GbE), USB3 -** This setting configures the PCIe port to operate as either: PCIe Port 1 or USB3 Port 7 For further details on Flex I/O see Tiger Lake H Platform Controller Hub EDS. ***Note:*** If DCI BSSB for this USB3 Combo port it will be Grayed out.	TGL-H	PCIe
	USB3 / PCIe Combo Port 1 **Values: PCIe (or GbE), USB3 -** This setting configures the PCIe port to operate as either: PCIe Port 2 or USB3 Port 8 For further details on Flex I/O see Tiger Lake H Platform Controller Hub EDS. ***Note:*** If DCI BSSB for this USB3 Combo port it will be Grayed out.	TGL-H	PCIe
	USB3 / PCIe Combo Port 2 **Values: PCIe (or GbE), USB3** - This setting configures the PCIe port to operate as either: PCIe Port 3 or USB3 Port 9 For further details on Flex I/O see Tiger Lake H Platform Controller Hub EDS. ***Note:*** If DCI BSSB for this USB3 Combo port it will be Grayed out.	TGL-H	PCIe
	USB3 / PCIe Combo Port 3 **Values: PCIe (or GbE), USB3** - This setting configures the PCIe port to operate as either: PCIe 4 or USB3 Port 10 For further details on Flex I/O see Tiger Lake H Platform Controller Hub EDS. ***Note:*** If DCI BSSB for this USB3 Combo port it will be Grayed out.	TGL-H	PCIe
	USB3 Port 1 Connector Type Select This setting configures the physical connector type to be used for USB 3.0 / 3.1 Port 1.	TGL-H	Type A / Type C
	USB3 Port 2 Connector Type Select This setting configures the physical connector type to be used for USB 3.0 / 3.1 Port 2.	TGL-H	Type A / Type C
	USB3 Port 3 Connector Type Select This setting configures the physical connector type to be used for USB 3.0 / 3.1 Port 3.	TGL-H	Type A / Type C
	USB3 Port 4 Connector Type Select This setting configures the physical connector type to be used for USB 3.0 / 3.1 Port 4.	TGL-H	Type A / Type C
	USB3 Port 5 Connector Type Select This setting configures the physical connector type to be used for USB 3.0 / 3.1 Port 4.	TGL-H	Type A / Type C
	USB3 Port 6Connector Type Select This setting configures the physical connector type to be used for USB 3.0 / 3.1 Port 4.	TGL-H	Type A / Type C
	USB3 Port 7 Connector Type Select This setting configures the physical connector type to be used for USB 3.0 / 3.1 Port 4.	TGL-H	Type A / Type C
	USB3 Port 8 Connector Type Select This setting configures the physical connector type to be used for USB 3.0 / 3.1 Port 4.	TGL-H	Type A / Type C
	USB3 Port 9 Connector Type Select This setting configures the physical connector type to be used for USB 3.0 / 3.1 Port 4.	TGL-H	Type A / Type C
	USB3 Port 10 Connector Type Select This setting configures the physical connector type to be used for USB 3.0 / 3.1 Port 4.	TGL-H	Type A / Type C
	USB Type AB Mode Select This setting determines how the USB Type AB connector switching is handled.	TGL-H	USB Type AB SW Select

Table 2-16. - Flex I/O Straps (Sheet 10 of 21)

	USB3 Port 1 Speed Capability This setting determines the USB3 Port 1 speed capabilities. ***Note:*** When a USB 3.2 Gen 2x1 (10 Gb/s) capable port is configured to USB 3.2 Gen 1x1 (5 Gb/s) speed using the soft strap, the port may still send 10 Gb/s compliance patterns if the USB compliance test (TD1.4, and TD1.7) is run on the port.	TGL-H	USB 3.1 Gen2
	USB3 Port 2 Speed Capability This setting determines the USB3 Port 2 speed capabilities. ***Note:*** When a USB 3.2 Gen 2x1 (10 Gb/s) capable port is configured to USB 3.2 Gen 1x1 (5 Gb/s) speed using the soft strap, the port may still send 10 Gb/s compliance patterns if the USB compliance test (TD1.4, and TD1.7) is run on the port.	TGL-H	USB 3.1 Gen2
	USB3 Port 3 Speed Capability This setting determines the USB3 Port 3 speed capabilities. ***Note:*** When a USB 3.2 Gen 2x1 (10 Gb/s) capable port is configured to USB 3.2 Gen 1x1 (5 Gb/s) speed using the soft strap, the port may still send 10 Gb/s compliance patterns if the USB compliance test (TD1.4, and TD1.7) is run on the port.	TGL-H	USB 3.1 Gen2
	USB3 Port 4 Speed Capability This setting determines the USB3 Port 4 speed capabilities. ***Note:*** When a USB 3.2 Gen 2x1 (10 Gb/s) capable port is configured to USB 3.2 Gen 1x1 (5 Gb/s) speed using the soft strap, the port may still send 10 Gb/s compliance patterns if the USB compliance test (TD1.4, and TD1.7) is run on the port.	TGL-H	USB 3.1 Gen2
	USB3 Port 5 Speed Capability This setting determines the USB3 Port 5 speed capabilities. ***Note:*** When a USB 3.2 Gen 2x1 (10 Gb/s) capable port is configured to USB 3.2 Gen 1x1 (5 Gb/s) speed using the soft strap, the port may still send 10 Gb/s compliance patterns if the USB compliance test (TD1.4, and TD1.7) is run on the port.	TGL-H	USB 3.1 Gen2
	USB3 Port 6 Speed Capability This setting determines the USB3 Port 6 speed capabilities. ***Note:*** When a USB 3.2 Gen 2x1 (10 Gb/s) capable port is configured to USB 3.2 Gen 1x1 (5 Gb/s) speed using the soft strap, the port may still send 10 Gb/s compliance patterns if the USB compliance test (TD1.4, and TD1.7) is run on the port.	TGL-H	USB 3.1 Gen2
	USB3 Port 7 Speed Capability This setting determines the USB3 Port 7 speed capabilities. ***Note:*** When a USB 3.2 Gen 2x1 (10 Gb/s) capable port is configured to USB 3.2 Gen 1x1 (5 Gb/s) speed using the soft strap, the port may still send 10 Gb/s compliance patterns if the USB compliance test (TD1.4, and TD1.7) is run on the port.	TGL-H	USB 3.1 Gen2
	USB3 Port 8 Speed Capability This setting determines the USB3 Port 8 speed capabilities. ***Note:*** When a USB 3.2 Gen 2x1 (10 Gb/s) capable port is configured to USB 3.2 Gen 1x1 (5 Gb/s) speed using the soft strap, the port may still send 10 Gb/s compliance patterns if the USB compliance test (TD1.4, and TD1.7) is run on the port.	TGL-H	USB 3.1 Gen2
	USB3 Port 9 Speed Capability This setting determines the USB3 Port 9 speed capabilities. ***Note:*** When a USB 3.2 Gen 2x1 (10 Gb/s) capable port is configured to USB 3.2 Gen 1x1 (5 Gb/s) speed using the soft strap, the port may still send 10 Gb/s compliance patterns if the USB compliance test (TD1.4, and TD1.7) is run on the port.	TGL-H	USB 3.1 Gen2

Table 2-16. - Flex I/O Straps (Sheet 11 of 21)

	USB3 Port 10 Speed Capability This setting determines the USB3 Port 10 speed capabilities. ***Note:*** When a USB 3.2 Gen 2x1 (10 Gb/s) capable port is configured to USB 3.2 Gen 1x1 (5 Gb/s) speed using the soft strap, the port may still send 10 Gb/s compliance patterns if the USB compliance test (TD1.4, and TD1.7) is run on the port.	TGL-H	USB 3.1 Gen2

Click on Flex I/O in the left tabs menu> USB2 Port Configuration is expanded by default:

USB2 Port Configuration 6

Parameter	Value	
USB2 Port 1 Connector Type Select	Type C	This setting configures the phys
USB2 Port 2 Connector Type Select	Type C	This setting configures the phys
USB2 Port 3 Connector Type Select	Type A / Type C	This setting configures the phys
USB2 Port 4 Connector Type Select	Type C	This setting configures the phys
USB2 Port 5 Connector Type Select	Type C	This setting configures the phys
USB2 Port 6 Connector Type Select	Type C	This setting configures the phys
USB2 Port 7 Connector Type Select	Type C	This setting configures the phys
USB2 Port 8 Connector Type Select	Type A / Type C	This setting configures the phys
USB2 Port 9 Connector Type Select	Type A / Type C	This setting configures the phys
USB2 Port 10 Connector Type Select	Express Card / M.2 S2	This setting configures the phys
USB2 Port 11 Connector Type Select	Type A / Type C	This setting configures the phys
USB2 Port 12 Connector Type Select	Type A / Type C	This setting configures the phys
USB2 Port 13 Connector Type Select	Type A / Type C	This setting configures the phys
USB2 Port 14 Connector Type Select	Type A / Type C	This setting configures the phys

#	Parameter	Platform	Settings
6	**Flex I/O - USB2 Port Configuration**		
	USB2 Port 1 Connector Type Select This setting configures the physical connector type to be used for USB2 Port 1.	TGL-H	Type A / Type C
	USB2 Port 2 Connector Type Select This setting configures the physical connector type to be used for USB2 Port 2.	TGL-H	Type A / Type C
	USB2 Port 3 Connector Type Select This setting configures the physical connector type to be used for USB2 Port 3.	TGL-H	Type A / Type C
	USB2 Port 4 Connector Type Select This setting configures the physical connector type to be used for USB2 Port 4.	TGL-H	Type A / Type C

Table 2-16. - Flex I/O Straps (Sheet 12 of 21)

	USB2 Port 5 Connector Type Select This setting configures the physical connector type to be used for USB2 Port 5.	TGL-H	Type A / Type C
	USB2 Port 6 Connector Type Select This setting configures the physical connector type to be used for USB2 Port 6.	TGL-H	Type A / Type C
	USB2 Port 7 Connector Type Select This setting configures the physical connector type to be used for USB2 Port 7.	TGL-H	Type-C
	USB2 Port 8 Connector Type Select This setting configures the physical connector type to be used for USB2 Port 8.	TGL-H	Type-C
	USB2 Port 9 Connector Type Select This setting configures the physical connector type to be used for USB2 Port 9.	TGL-H	Type-C
	USB2 Port 10 Connector Type Select This setting configures the physical connector type to be used for USB2 Port 10.	TGL-H	Type-C
	USB2 Port 11 Connector Type Select This setting configures the physical connector type to be used for USB2 Port 11.	TGL-H	Type A / Type C
	USB2 Port 12 Connector Type Select This setting configures the physical connector type to be used for USB2 Port 12.	TGL-H	Type A / Type C
	USB2 Port 13 Connector Type Select This setting configures the physical connector type to be used for USB2 Port 13.	TGL-H	Type A / Type C
	USB2 Port 14 Connector Type Select This setting configures the physical connector type to be used for USB2 Port 14.	TGL-H	Type A / Type C
Click on Flex I/O in the left tabs menu> Type-C Subsystem Configuration is expanded by default:			

Table 2-16. - Flex I/O Straps (Sheet 13 of 21)

Type-C Subsystem Configuration 6

Parameter	Value	
IO Manageability Engine Binary File		This loads the Type-C Subsystem IO Manageability Engine
IO Manageability Engine Enabled	Yes	This setting enables\ disables the Type-C Subsystem IO M
IO Manageability Engine Length	0x12000	Set the length of IOM sub partition.
IO Manageability Engine version		-
IO Manageability Engine OEM configuration Binary File		This loads the Type-C Subsystem IO Manageability Engine
PHY Binary File		This loads the Type-C Subsystem PHY binary that will be r
PHY Manifest Enabled	Yes	This setting enables\ disables the Type-C Subsystem MG I
PHY Length	0x10000	Set the length of MG PHY sub partition.
PHY version		-
Thunderbolt(TM)/USB4(TM) Binary File		This loads the Type-C Subsystem Thunderbolt(TM)/USB4(
Thunderbolt(TM)/USB4(TM) Binary file Length	0x40000	Set the length of Thunderbolt(TM) sub partition.
Thunderbolt(TM)/USB4(TM) version		-
Tcss - Partial Update Enabled	Disabled	This setting enables partial update for TCSS partitions
Type-C Subsystem Port Enable Mask	0xF	This setting determines the Type-C Subsystem Port Enabl
Type-C Port 1 Configuration	No Restrictions	This setting determines the configuration of Type-C Port 1
Type-C Port 2 Configuration	No Restrictions	This setting determines the configuration of Type-C Port 2
Type-C Port 3 Configuration	No Restrictions	This setting determines the configuration of Type-C Port 3
Type-C Port 4 Configuration	No Restrictions	This setting determines the configuration of Type-C Port 4
Type-C Port 1 Speed Capability	USB 3.1 Gen2	This setting determines the Type-C Port 1 speed capabiliti
Type-C Port 2 Speed Capability	USB 3.1 Gen2	This setting determines the Type-C Port 2 speed capabiliti
Type-C Port 3 Speed Capability	USB 3.1 Gen2	This setting determines the Type-C Port 3 speed capabiliti
Type-C Port 4 Speed Capability	USB 3.1 Gen2	This setting determines the Type-C Port 4 speed capabiliti
Type-C Port 1 Initialization Speed Select	USB3.1 Gen1 LBPM	This setting determines Type-C Port 1 speed during platfo
Type-C Port 2 Initialization Speed Select	USB3.1 Gen1 LBPM	This setting determines Type-C Port 2 speed during platfo
Type-C Port 3 Initialization Speed Select	USB3.1 Gen1 LBPM	This setting determines Type-C Port 3 speed during platfo
Type-C Port 4 Initialization Speed Select	USB3.1 Gen1 LBPM	This setting determines Type-C Port 4 speed during platfo
Type-C Port 1 Connector Type Select	Type C	This setting configures the physical connector type to be u
Type-C Port 2 Connector Type Select	Type C	This setting configures the physical connector type to be u
Type-C Port 3 Connector Type Select	Type C	This setting configures the physical connector type to be u
Type-C Port 4 Connector Type Select	Type C	This setting configures the physical connector type to be u
xDCI Split Die Configuration	xDCI Split Die Enabled	This setting determines if xDCI Split die configuration is en

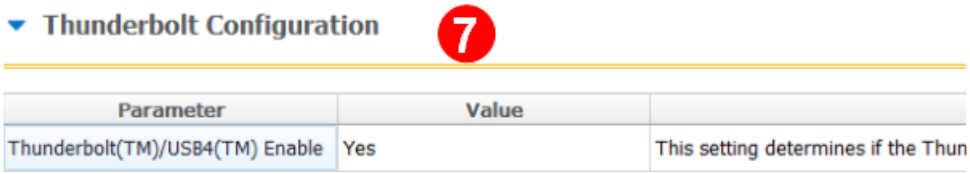
#	Parameter	Platform	Settings

Table 2-16. - Flex I/O Straps (Sheet 14 of 21)

7	**Type-C Subsystem Configuration**		
	IO Manageability Engine Binary File - This loads the IO Manageability binary that will be merged into the output image generated by the Intel® FIT.	TGL-H	IOM Binary
	IO Manageability Engine Enabled **Values: Yes/No** This setting enables / disables the Type-C Subsystem IO Manageability Engine on the platform.	TGL-H	Yes
	IO Manageability Engine Length - This displays the length of the IO Manageability binary. ***Note:*** This value will be automatically populated by Intel® FIT during image build.		
	IO Manageability Engine Version - This displays the version of IO Manageability binary.		
	PHY Binary File - This loads the PHY binary that will be merged into the output image generated by the Intel® FIT.	TGL-H	PHY Binary
	PHY Manifest Enabled **Values: Yes/No** This setting enables / disables the PHY on the platform.	TGL-H	Yes
	PHY Length - This displays the length of the PHY binary. ***Note:*** This value will be automatically populated by Intel® FIT during image build.		
	PHY Version - This displays the version of PHY binary.		
	Thunderbolt(TM)/USB4(TM) Binary File **Values: Yes/No** This setting enables Anti-Roll back for the Type-C Subsystem Thunderbolt(TM)/USB4(TM) binary.	TGL-H	TBT Binary
	Thunderbolt(TM)/USB4(TM) Length - This displays the length of the Thunderbolt(TM)/USB4(TM) binary. ***Note:*** This value will be automatically populated by Intel® FIT during image build.		
	Thunderbolt(TM)/USB4(TM) Version - This displays the version of Thunderbolt(TM)/USB4(TM) binary.		
	Tcss - Partial Update Enabled **Values: Enabled/Disabled** This setting enabled partial firmware update of the TCSS partitions.	TGL-H	Disabled
	Type-C Subsystem Port Enable Mask This setting determines the Type-C Subsystem Port Enable Mask	TGL-H	0xF
	Type-C Subsystem Authentication Enabled **Values: Yes/No** This setting enables / disables firmware authentication for the Type-C Subsystem on power-up.	TGL-H	Yes
	Type-C Port 1 Configuration **Value: No Restrictions/DP Fixed Connection/No Thunderbolt** This setting determines the configuration for Type-C Port 1	TGL-H	No Restrictions
	Type-C Port 2 Configuration **Value: No Restrictions/DP Fixed Connection/No Thunderbolt** This setting determines the configuration for Type-C Port 2	TGL-H	No Restrictions
	Type-C Port 3 Configuration **Value: No Restrictions/DP Fixed Connection/No Thunderbolt** This setting determines the configuration for Type-C Port 3	TGL-H	No Restrictions
	Type-C Port 4 Configuration **Value: No Restrictions/DP Fixed Connection/No Thunderbolt** This setting determines the configuration for Type-C Port 4	TGL-H	No Restrictions

Table 2-16. - Flex I/O Straps (Sheet 15 of 21)

	Type-C Port 1 Speed Capability **Values: USB 3.1 Gen2/USB 3.1 Gen1** This setting determines the Type-C Port 1 speed capability	TGL-H	USB 3.1 Gen2
	Type-C Port 2 Speed Capability **Values: USB 3.1 Gen2/USB 3.1 Gen1** This setting determines the Type-C Port 2 speed capability	TGL-H	USB 3.1 Gen2
	Type-C Port 3 Speed Capability **Values: USB 3.1 Gen2/USB 3.1 Gen1** This setting determines the Type-C Port 3 speed capability	TGL-H	USB 3.1 Gen2
	Type-C Port 4 Speed Capability **Values: USB 3.1 Gen2/USB 3.1 Gen1** This setting determines the Type-C Port 4 speed capability	TGL-H	USB 3.1 Gen2
	Type-C Port 1 Initialization Speed Select **Values: USB3.1 Gen1 LBPM/USB3.1 Gen2 skip LBPM** This setting determines Type-C Port 1 speed during platform power-up.	TGL-H	USB3.1 Gen1 LBPM
	Type-C Port 2 Initialization Speed Select **Values: USB3.1 Gen1 LBPM/USB3.1 Gen2 skip LBPM** This setting determines Type-C Port 2 speed during platform power-up.	TGL-H	USB3.1 Gen1 LBPM
	Type-C Port 3 Initialization Speed Select **Values: USB3.1 Gen1 LBPM/USB3.1 Gen2 skip LBPM** This setting determines Type-C Port 3 speed during platform power-up.	TGL-H	USB3.1 Gen1 LBPM
	Type-C Port 4 Initialization Speed Select **Values: USB3.1 Gen1 LBPM/USB3.1 Gen2 skip LBPM** This setting determines Type-C Port 4 speed during platform power-up.	TGL-H	USB3.1 Gen1 LBPM
	Type-C Port 1 Connector Type Select This setting configures the physical connector type to be used for Type-C Port 1.	TGL-H	Type-C
	Type-C Port 2 Connector Type Select This setting configures the physical connector type to be used for Type-C Port 2.	TGL-H	Type-C
	Type-C Port 3 Connector Type Select This setting configures the physical connector type to be used for Type-C Port 3.	TGL-H	Type-C
	Type-C Port 4 Connector Type Select This setting configures the physical connector type to be used for Type-C Port 4.	TGL-H	Type-C
	xDCI Split Die Configuration **Values: xDCI Split Die Enabled, xDCI Split Die Disabled**	TGL-H	xDCI Split Die Enabled
Click on Flex I/O in the left tabs menu> Thunderbolt Configuration is expanded by default:			



#	Parameter	Platform	Settings
8	**Thunderbolt Configuration**		
	Thunderbolt(TM)/USB4(TM) Enable **Values: Yes/No** This setting determines if the Thunderbolt(tm)/USB4(TM) interface is enabled on the platform.	TGL-H	Yes Yes
Click on Flex I/O in the left tabs menu> Power Delivery PD Controller Configuration is expanded by default:			

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

Power Delivery PD Controller Configuration 8

Parameter	Value	
PMC-PD Controller USB Type-C Mode	PMC / SMBus	This bit defines how the PMC interfaces with the T
Re-timer Power Gating Enabled	No	Indicates whether platform Re-timer power gating
Type-C port 1 Enabled	Yes	Indicates whether the associated Type-C port is er
USB2 Port Number associated for Type-C Port 1	USB2 Port 7	USB2 port number for the associated Type-C port
USB3 Port Number associated for Type-C Port 1	Type-C Port 1	USB3 port number for the associated Type-C port
Type-C Port 1 Re-Timer Present	Yes	Indicates whether a re-timer is present for the ass
Type-C Port 1 Re-timer Configuration Enabled	No	Indicates whether the associated re-timer requires
Type-C Port 1 Re-timer SMBus Address	0x50	SMBus address for the associated re-timer.
Type C Port 1 SMBus Address	0x21	SMBus address for the associated Type-C port.
Type-C port 2 Enabled	Yes	Indicates whether the associated Type-C port is er
USB2 Port Number associated for Type-C Port 2	USB2 Port 8	USB2 port number for the associated Type-C port
USB3 Port Number associated for Type-C Port 2	Type-C Port 2	USB3 port number for the associated Type-C port
Type-C Port 2 Re-Timer Present	Yes	Indicates whether a re-timer is present for the ass
Type-C Port 2 Re-timer Configuration Enabled	No	Indicates whether the associated re-timer requires
Type-C Port 2 Re-timer SMBus Address	0x51	SMBus address for the associated re-timer
Type-C Port 2 SMBus Address	0x25	SMBus address for the associated Type-C port
Type-C port 3 Enabled	Yes	Indicates whether the associated Type-C port is er
USB2 Port Number associated for Type-C Port 3	USB2 Port 9	USB2 port number for the associated Type-C port
USB3 Port Number associated for Type-C Port 3	Type-C Port 3	USB3 port number for the associated Type-C port
Type-C Port 3 Re-Timer Present	Yes	Indicates whether a re-timer is present for the ass
Type-C Port 3 Re-timer Configuration Enabled	No	Indicates whether the associated re-timer requires
Type-C Port 3 Re-timer SMBus Address	0x53	SMBus address for the associated re-timer
Type-C Port 3 SMBus Address	0x20	SMBus address for the associated Type-C port
Type-C port 4 Enabled	Yes	Indicates whether the associated Type-C port is er
USB2 Port Number associated for Type-C Port 4	USB2 Port 10	USB2 port number for the associated Type-C port
USB3 Port Number associated for Type-C Port 4	Type-C Port 4	USB3 port number for the associated Type-C port
Type-C Port 4 Re-Timer Present	Yes	Indicates whether a re-timer is present for the assc
Type-C Port 4 Re-timer Configuration Enabled	No	Indicates whether the associated re-timer requires
Type-C Port 4 Re-timer SMBus Address	0x55	SMBus address for the associated re-timer
Type-C Port 4 SMBus Address	0x24	SMBus address for the associated Type-C port
Type-C Port 1 USB3 Ownership	CPU	This setting determines if the Type-C Port 1 USB3 i
Type-C Port 1 Re-Timer Configuration Type	1 Re-Timer	This setting determines the number of Re-Timers b
Type-C Port 2 USB3 Ownership	CPU	This setting determines if the Type-C Port 2 USB3 i
Type-C Port 2 Re-Timer Configuration Type	1 Re-Timer	This setting determines the number of Re-Timers b
Type-C Port 3 USB3 Ownership	CPU	This setting determines if the Type-C Port 3 USB3 i
Type-C Port 3 Re-Timer Configuration Type	1 Re-Timer	This setting determines the number of Re-Timers b
Type-C Port 4 USB3 Ownership	CPU	This setting determines if the Type-C Port 4 USB3 i
Type-C Port 4 Re-Timer Configuration Type	1 Re-Timer	This setting determines the number of Re-Timers b

Table 2-16. - Flex I/O Straps (Sheet 17 of 21)

9	**Power Delivery PD Controller Configuration**		
	PMC-PD controller USB-C Mode Enabled **Values:** **0: PMC interfaces with an eSPI connected agent via eSPI OOB** **1: PMC interfaces with PD chips/Re-timer via ALERT# pin which triggers SMBus transactions.** This bit defines how the PMC interfaces with the Type-C components on the board. ***Notes:*** 1. This setting is greyed and not configurable for LP based SKUs. for LP SKUs, PMC interfaces with PD chips/Re-timer via ALERT# pin. 2. if user selection is 0 where PMC interfaces with an eSPI connected agent, all of the below parameters are N/A and will be grayed out.	TGL-H	PMC / SMBus PMC / SMBus
	Re-timer Power Gating Enabled **Values: Yes / No** This setting indicates whether platform Re-timer power gating is enabled.	TGL-H	No
	Type-C port 1 Enabled **Values: Yes / No** This setting indicates whether the associated Type-C port1 is enabled. ***Note:*** This setting is only available for configuration when PMC-PD controller USB-C Mode Enabled parameter is set to 1.	TGL-H	Yes
	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:*** 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)	TGL-H	USB2 Port 7
	USB3 Port number associated for Type-C Port 1 **Values: USB3 Port 1,USB3 Port 2,USB3 Port 3,USB3 Port 4** This indicates the USB3 port number for the associated Type-C port1. ***Notes:*** 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)	TGL-H	USB3 Port 1

Table 2-16. - Flex I/O Straps (Sheet 18 of 21)

	Type-C Port 1 Re-timer Present **Values: Yes / No** This indicates whether a re-timer is present for the associated Type-C port.	TGL-H	Yes
	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.	TGL-H	No
	Type-C Port 1 Re-timer SMBus Address **Value: Hex** This indicates the SMBus address for the associated re-timer.	TGL-H	0x50
	Type-C Port 1 SMBus Address **Value: Hex** This indicates the SMBus address for the associated Type-C port. ***Note:*** OEMs are recommended to set unique SMBus address allocation for Type-C port and Re-timer associated.	TGL-H	0x21
	Type-C port 2 Enabled **Values: Yes / No** This setting indicates whether the associated Type-C port is enabled. ***Note:*** This setting is only available for configuration when PMC-PD controller USB-C Mode Enabled parameter is set to 1.	TGL-H	Yes
	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:*** 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)	TGL-H	USB2 Port 8
	USB3 Port number associated for Type-C Port 2 **Values: USB3 Port 1,USB3 Port 2,USB3 Port 3,USB3 Port 4** This indicates the USB3 port number for the associated Type-C port. ***Notes:*** 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)	TGL-H	USB3 Port 2
	Type-C Port 2 Re-timer Present **Values: Yes / No** This indicates whether a re-timer is present for the associated Type-C port.	TGL-H	Yes

Table 2-16. - Flex I/O Straps (Sheet 19 of 21)

	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.	TGL-H	No
	Type-C Port 2 Re-timer SMBus Address **Value: Hex** This indicates the SMBus address for the associated re-timer.	TGL-H	0x51
	Type-C Port 2 SMBus Address **Value: Hex** This indicates the SMBus address for the associated Type-C port. ***Note:*** OEMs are recommended to set unique SMBus address allocation for Type-C port and Re-timer associated.	TGL-H	0x25
	Type-C port 3 Enabled **Values: Yes / No** This setting indicates whether the associated Type-C port is enabled. ***Note:*** This setting is only available for configuration when PMC-PD controller USB-C Mode Enabled parameter is set to 1.	TGL-H	Yes
	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:*** 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 por3 ,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)	TGL-H	USB2 Port 9
	USB3 Port number associated for Type-C Port 3 **Values: USB3 Port 1,USB3 Port 2,USB3 Port 3,USB3 Port 4** This indicates the USB3 port number for the associated Type-C port. ***Notes:*** 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)	TGL-H	USB3 Port 3
	Type-C Port 3 Re-timer Present **Values: Yes / No** This indicates whether a re-timer is present for the associated Type-C port.	TGL-Y TGL-U	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.	TGL-Y TGL-U	No

Table 2-16. - Flex I/O Straps (Sheet 20 of 21)

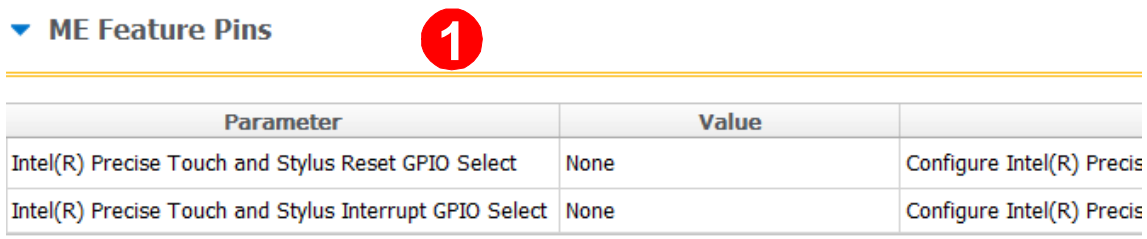
	Type-C Port 3 Re-timer SMBus Address **Value: Hex** This indicates the SMBus address for the associated re-timer.	TGL-H	0x53
	Type-C Port 3 SMBus Address **Value: Hex** This indicates the SMBus address for the associated Type-C port. ***Note:*** OEMs are recommended to set unique SMBus address allocation for Type-C port and Re-timer associated.	TGL-H	0x20
	Type-C port 4 Enabled **Values: Yes / No** This setting indicates whether the associated Type-C port is enabled. ***Note:*** This setting is only available for configuration when PMC-PD controller USB-C Mode Enabled parameter is set to 1.	TGL-H	Yes
	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:*** 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)	TGL-H	USB2 Port 10
	USB3 Port number associated for Type-C Port 4 **Values: USB3 Port 1,USB3 Port 2,USB3 Port 3,USB3 Port 4** This indicates the USB3 port number for the associated Type-C port. ***Notes:*** 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)	TGL-H	USB3 Port 4
	Type-C Port 4 Re-timer Present **Values: Yes / No** This indicates whether a re-timer is present for the associated Type-C port.	TGL-H	Yes
	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.	TGL-H	No
	Type-C Port 4 Re-timer SMBus Address **Value: Hex** This indicates the SMBus address for the associated re-timer.	TGL-H	0x55

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

	Type-C Port 4 SMBus Address **Value: Hex** This indicates the SMBus address for the associated Type-C port. ***Note:*** OEMs are recommended to set unique SMBus address allocation for Type-C port and Re-timer associated.	TGL-H	0x24
	Type-C Port 1 USB3 Ownership **Values: CPU / PCH** This setting determined if the Type-C Port is owned by CPU or PCH	TGL-H	CPU
	Type-C Port 1 Re-Timer Configuration Type Select **Values: 1 Re-Timer, 2 Re-Timers** This setting determines the number of Re-Timers being used for TYpe-C Port 1	TGL-H	1 Re-Timer
	Type-C Port 2 USB3 Ownership **Values: CPU / PCH** This setting determined if the Type-C Port is owned by CPU or PCH	TGL-H	CPU
	Type-C Port 2 Re-Timer Configuration Type Select **Values: 1 Re-Timer, 2 Re-Timers** This setting determines the number of Re-Timers being used for TYpe-C Port 2	TGL-H	1 Re-Timer
	Type-C Port 3 USB3 Ownership **Values: CPU / PCH** This setting determined if the Type-C Port is owned by CPU or PCH	TGL-H	CPU
	Type-C Port 3 Re-Timer Configuration Type Select **Values: 1 Re-Timer, 2 Re-Timers** This setting determines the number of Re-Timers being used for TYpe-C Port 3	TGL-H	1 Re-Timer
	Type-C Port 4 USB3 Ownership **Values: CPU / PCH** This setting determined if the Type-C Port is owned by CPU or PCH	TGL-H	CPU
	Type-C Port 4 Re-Timer Configuration Type Select **Values: 1 Re-Timer, 2 Re-Timers** This setting determines the number of Re-Timers being used for TYpe-C Port 4	TGL-H	1 Re-Timer

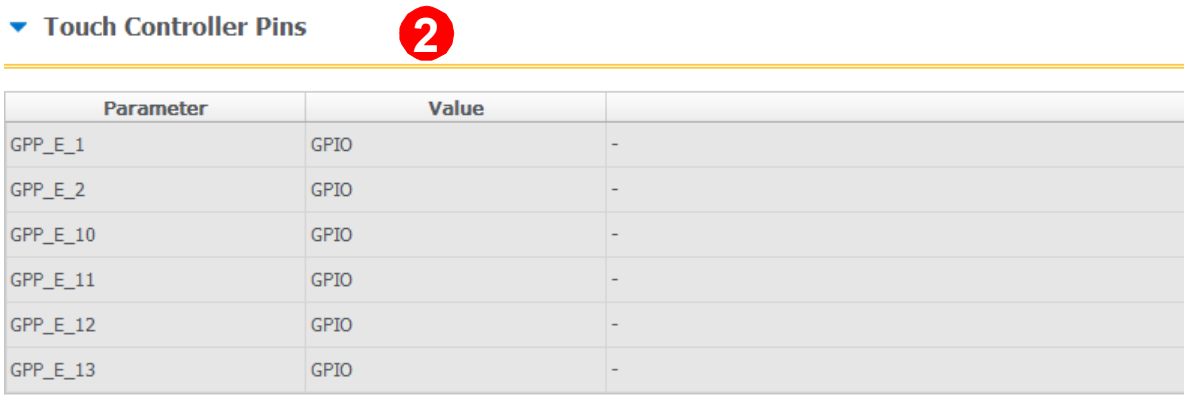
Table 2-17. - GPIO (Sheet 1 of 6)

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



#	Parameter	Platform	Settings
1	**ME Feature Pins**		
	Intel® Precise Touch and Stylus Reset GPIO Select Configure Intel® Precise Touch and Stylus Reset GPIO.	TGL-H	None
	Intel® Precise Touch and Stylus Interrupt GPIO Select Configure Intel® Precise Touch and Stylus Interrupt GPIO.	TGL-H	None

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



#	Parameter	Platform	Settings
2	**Touch Controller Pins**		
	GPP_E_1	TGL-H	GPIO
	GPP_E_2	TGL-H	GPIO
	GPP_E_10	TGL-H	GPIO
	GPP_E_11	TGL-H	GPIO
	GPP_E_12	TGL-H	GPIO
	GPP_E_13	TGL-H	GPIO

Click on GPIO in the left tabs menu> GPIO VCCIO Voltage Control is expanded by default:

Table 2-17. - GPIO (Sheet 2 of 6)

GPIO VCCIO Voltage Control

3

Parameter	Value	
Clockout 48 Mode Configuration	GPP_A16	This setting determines the native mode of operation for the CLK
GPP_A0 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage for the GPP_A0 GPIO pin.
GPP_A1 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage for the GPP_A1 GPIO pin.
GPP_A2 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage for the GPP_A2 GPIO pin.
GPP_A3 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage for the GPP_A3 GPIO pin.
GPP_A4 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage for the GPP_A4 GPIO pin.
GPP_A5 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage for the GPP_A5 GPIO pin.
GPP_A6 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage for the GPP_A6 GPIO pin.
GPP_A7 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage for the GPP_A7 GPIO pin.
GPP_A8 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage for the GPP_A8 GPIO pin.
GPP_A9 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage for the GPP_A9 GPIO pin.
GPP_A10 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage for the GPP_A10 GPIO pir
GPP_A11 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage for the GPP_A11 GPIO pir
GPP_A12 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage for the GPP_A12 GPIO pir
GPP_A13 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage for the GPP_A13 GPIO pir
GPP_A14 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage for the GPP_A14 GPIO pir
GPP_B Group Master Voltage Select	3.3Volts	This setting controls configures the VCCIO voltage all of the GPP_
GPP_C Group Master Voltage Select	3.3Volts	This setting controls configures the VCCIO voltage all of the GPP_
GPP_D Group Master Voltage Select	1.8Volts	This setting controls configures the VCCIO voltage all of the GPP_
GPP_E Group Master Voltage Select	3.3Volts	This setting controls configures the VCCIO voltage all of the GPP_
GPP_F Group Master Voltage Select	3.3Volts	This setting controls configures the VCCIO voltage all of the GPP_

#	Parameter	Platform	Settings
3	**GPIO VCCIO Voltage Control** ***Warning:*** Incorrectly configuring GPIO voltages may result in PCH damage. The voltage settings below are for the specific RVPs noted under the Platform column. Customers should check their schematics to verify that the appropriate voltages are configured.		
	Deep Sx Mode Configuration **Values: GPP_A16 / CLKOUT_48** This setting determines the native mode of operation for the CLKOUT_48 signal	TGL-H	GPP_A16
	GPP_A0 Individual Voltage Select **Values: 3.3Volts / 1.8Volts** This setting configures the VCCIO voltage for the GPP_A0 GPIO pin.	TGL-H	1.8 Volts
	GPP_A1 Individual Voltage Select **Values: 3.3Volts / 1.8Volts** This setting configures the VCCIO voltage for the GPP_A1 GPIO pin.	TGL-H	1.8 Volts

Table 2-17. - GPIO (Sheet 3 of 6)

	GPP_A2 Individual Voltage Select **Values: 3.3Volts / 1.8Volts** This setting configures the VCCIO voltage for the GPP_A2 GPIO pin.	TGL-H	1.8 Volts
	GPP_A3 Individual Voltage Select **Values: 3.3Volts / 1.8Volts** This setting configures the VCCIO voltage for the GPP_A3 GPIO pin.	TGL-H	1.8 Volts
	GPP_A4 Individual Voltage Select **Values: 3.3Volts / 1.8Volts** This setting configures the VCCIO voltage for the GPP_A4 GPIO pin.	TGL-H	1.8 Volts
	GPP_A5 Individual Voltage Select **Values: 3.3Volts / 1.8Volts** This setting configures the VCCIO voltage for the GPP_A5 GPIO pin.	TGL-H	1.8 Volts
	GPP_A6 Individual Voltage Select **Values: 3.3Volts / 1.8Volts** This setting configures the VCCIO voltage for the GPP_A6 GPIO pin.	TGL-H	1.8 Volts
	GPP_A7 Individual Voltage Select **Values: 3.3Volts / 1.8Volts** This setting configures the VCCIO voltage for the GPP_A7 GPIO pin.	TGL-H	1.8 Volts
	GPP_A8 Individual Voltage Select **Values: 3.3Volts / 1.8Volts** This setting configures the VCCIO voltage for the GPP_A8 GPIO pin.	TGL-H	1.8 Volts
	GPP_A9 Individual Voltage Select **Values: 3.3Volts / 1.8Volts** This setting configures the VCCIO voltage for the GPP_A9 GPIO pin.	TGL-H	1.8 Volts
	GPP_A10 Individual Voltage Select **Values: 3.3Volts / 1.8Volts** This setting configures the VCCIO voltage for the GPP_A10 GPIO pin.	TGL-H	1.8 Volts
	GPP_A11 Individual Voltage Select **Values: 3.3Volts / 1.8Volts** This setting configures the VCCIO voltage for the GPP_A11 GPIO pin.	TGL-H	1.8 Volts
	GPP_A12 Individual Voltage Select **Values: 3.3Volts / 1.8Volts** This setting configures the VCCIO voltage for the GPP_A12 GPIO pin.	TGL-H	1.8 Volts
	GPP_A13 Individual Voltage Select **Values: 3.3Volts / 1.8Volts** This setting configures the VCCIO voltage for the GPP_A13 GPIO pin.	TGL-H	1.8 Volts
	GPP_A14 Individual Voltage Select **Values: 3.3Volts / 1.8Volts** This setting configures the VCCIO voltage for the GPP_A14 GPIO pin.	TGL-H	1.8 Volts
	GPP_B Group Master Voltage Select **Values: 3.3Volts / 1.8Volts** This setting configures the VCCIO voltage for the GPP_B GPIO group.	TGL-H	3.3 Volts
	GPP_C Group Master Voltage Select **Values: 3.3Volts / 1.8Volts** This setting configures the VCCIO voltage for the GPP_C GPIO group.	TGL-H	3.3 Volts
	GPP_B Group Master Voltage Select **Values: 3.3Volts / 1.8Volts** This setting configures the VCCIO voltage for the GPP_D GPIO group.	TGL-H	1.8 Volts
	GPP_B Group Master Voltage Select **Values: 3.3Volts / 1.8Volts** This setting configures the VCCIO voltage for the GPP_E GPIO group.	TGL-H	3.3 Volts
	GPP_F Group Master Voltage Select **Values: 3.3Volts / 1.8Volts** This setting configures the VCCIO voltage for the GPP_F GPIO group.	TGL-H	3.3 Volts

Table 2-17. - GPIO (Sheet 4 of 6)

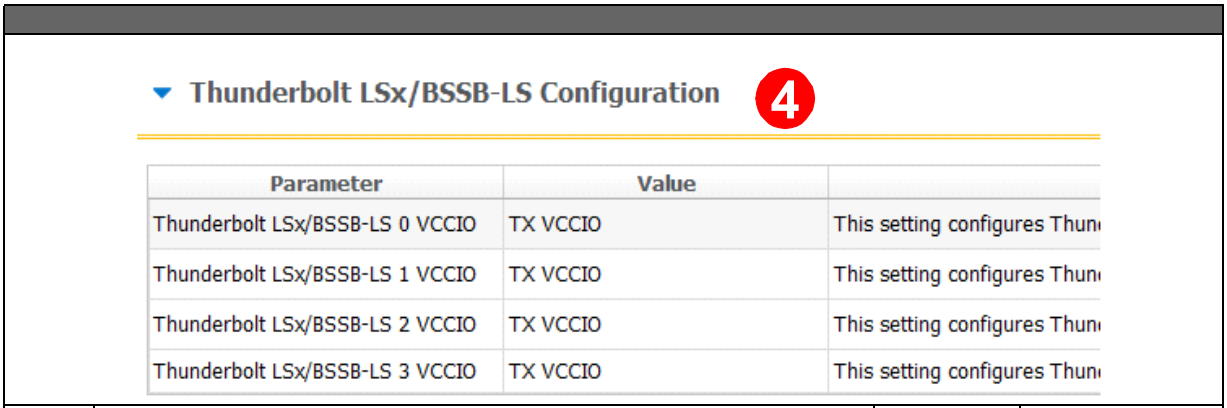
GPP_G0 Individual Voltage Select	3.3Volts	This setting controls the VCCIO voltage for the GPP_G0 GPIO pin
GPP_G1 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage for the GPP_G1 GPIO pin
GPP_G2 Individual Voltage Select	3.3Volts	This setting controls the VCCIO voltage for the GPP_G2 GPIO pin
GPP_G3 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage for the GPP_G3 GPIO pin
GPP_G4 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage for the GPP_G4 GPIO pin
GPP_G5 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage for the GPP_G5 GPIO pin
GPP_G6 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage for the GPP_G6 GPIO pin
GPP_G7 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage for the GPP_G7 GPIO pin
GPP_G8 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage for the GPP_G8 GPIO pin
GPP_G9 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage for the GPP_G9 GPIO pin
GPP_G10 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage for the GPP_G10 GPIO pi
GPP_G11 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage for the GPP_G11 GPIO pi
GPP_G12 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage for the GPP_G12 GPIO pi
GPP_G13 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage for the GPP_G13 GPIO pi
GPP_G14 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage for the GPP_G14 GPIO pi
GPP_G15 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage for the GPP_G15 GPIO pi
GPP_H Group Master Voltage Select	3.3Volts	This setting controls configures the VCCIO voltage all of the GPP
GPP_I Group Master Voltage Select	3.3Volts	This setting controls configures the VCCIO voltage all of the GPP
GPP_K Group Master Voltage Select	3.3Volts	This setting controls configures the VCCIO voltage all of the GPP
Intel(R) HD Audio Voltage Select	1.8Volts	This setting controls configures the VCCIO voltage for all of the I

#	Parameter	Platform	Settings
	GPP_G0 Individual Voltage Select **Values: 3.3Volts / 1.8Volts** This setting configures the VCCIO voltage for the GPP_G0 GPIO pin.	TGL-H	3.3 Volts
	GPP_G1 Individual Voltage Select **Values: 3.3Volts / 1.8Volts** This setting configures the VCCIO voltage for the GPP_G1 GPIO pin.	TGL-H	1.8 Volts
	GPP_G2 Individual Voltage Select **Values: 3.3Volts / 1.8Volts** This setting configures the VCCIO voltage for the GPP_G2 GPIO pin.	TGL-H	3.3 Volts
	GPP_G3 Individual Voltage Select **Values: 3.3Volts / 1.8Volts** This setting configures the VCCIO voltage for the GPP_G3 GPIO pin.	TGL-H	1.8 Volts
	GPP_G4 Individual Voltage Select **Values: 3.3Volts / 1.8Volts** This setting configures the VCCIO voltage for the GPP_G4 GPIO pin.	TGL-H	1.8 Volts
	GPP_G5 Individual Voltage Select **Values: 3.3Volts / 1.8Volts** This setting configures the VCCIO voltage for the GPP_G5 GPIO pin.	TGL-H	1.8 Volts

Table 2-17. - GPIO (Sheet 5 of 6)

	GPP_G6 Individual Voltage Select **Values: 3.3Volts / 1.8Volts** This setting configures the VCCIO voltage for the GPP_G6 GPIO pin.	TGL-H	1.8 Volts
	GPP_G7 Individual Voltage Select **Values: 3.3Volts / 1.8Volts** This setting configures the VCCIO voltage for the GPP_G7 GPIO pin.	TGL-H	1.8 Volts
	GPP_G8 Individual Voltage Select **Values: 3.3Volts / 1.8Volts** This setting configures the VCCIO voltage for the GPP_G8 GPIO pin.	TGL-H	1.8 Volts
	GPP_G9 Individual Voltage Select **Values: 3.3Volts / 1.8Volts** This setting configures the VCCIO voltage for the GPP_G9 GPIO pin.	TGL-H	1.8 Volts
	GPP_G10 Individual Voltage Select **Values: 3.3Volts / 1.8Volts** This setting configures the VCCIO voltage for the GPP_G10 GPIO pin.	TGL-H	1.8 Volts
	GPP_G11 Individual Voltage Select **Values: 3.3Volts / 1.8Volts** This setting configures the VCCIO voltage for the GPP_G11 GPIO pin.	TGL-H	1.8 Volts
	GPP_G12 Individual Voltage Select **Values: 3.3Volts / 1.8Volts** This setting configures the VCCIO voltage for the GPP_G12 GPIO pin.	TGL-H	1.8 Volts
	GPP_G13 Individual Voltage Select **Values: 3.3Volts / 1.8Volts** This setting configures the VCCIO voltage for the GPP_G13 GPIO pin.	TGL-H	1.8 Volts
	GPP_G14 Individual Voltage Select **Values: 3.3Volts / 1.8Volts** This setting configures the VCCIO voltage for the GPP_G14 GPIO pin.	TGL-H	1.8 Volts
	GPP_G15 Individual Voltage Select **Values: 3.3Volts / 1.8Volts** This setting configures the VCCIO voltage for the GPP_G15 GPIO pin.	TGL-H	1.8 Volts
	GPP_H Group Master Voltage Select **Values: 3.3Volts / 1.8Volts** This setting configures the VCCIO voltage for the GPP_H GPIO group.	TGL-H	3.3 Volts
	GPP_I Group Master Voltage Select **Values: 3.3Volts / 1.8Volts** This setting configures the VCCIO voltage for the GPP_I GPIO group.	TGL-H	3.3 Volts
	GPP_K Group Master Voltage Select **Values: 3.3Volts / 1.8Volts** This setting configures the VCCIO voltage for the GPP_K GPIO group.	TGL-H	3.3 Volts
	Intel® HD Audio Voltage Select **Values: 3.3Volts / 1.8Volts** This setting configures the VCCIO voltage for all of the Intel® HD Audio GPIO pins.	TGL-H	1.8 Volts

Table 2-17. - GPIO (Sheet 6 of 6)



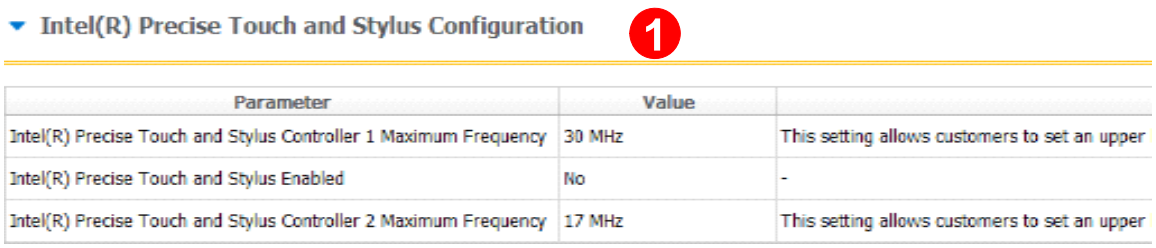
Thunderbolt LSx/BSSB-LS Configuration 4

Parameter	Value	
Thunderbolt LSx/BSSB-LS 0 VCCIO	TX VCCIO	This setting configures Thun
Thunderbolt LSx/BSSB-LS 1 VCCIO	TX VCCIO	This setting configures Thun
Thunderbolt LSx/BSSB-LS 2 VCCIO	TX VCCIO	This setting configures Thun
Thunderbolt LSx/BSSB-LS 3 VCCIO	TX VCCIO	This setting configures Thun

#	Parameter	Platform	Settings
4	**Thunderbolt LSx/BSSB-LS Configuration**		
	Thunderbolt LSx/BSSB-LS 0 VCCIO **Values: TX VCCIO / Legacy VCCIO** This setting configured Thunderbolt LSx/BSSB-LS 0 VCCIO.	TGL-H	TX VCCIO
	Thunderbolt LSx/BSSB-LS 1 VCCIO **Values: TX VCCIO / Legacy VCCIO** This setting configured Thunderbolt LSx/BSSB-LS 0 VCCIO.	TGL-H	TX VCCIO
	Thunderbolt LSx/BSSB-LS 2 VCCIO **Values: TX VCCIO / Legacy VCCIO** This setting configured Thunderbolt LSx/BSSB-LS 0 VCCIO.	TGL-H	TX VCCIO
	Thunderbolt LSx/BSSB-LS 3 VCCIO **Values: TX VCCIO / Legacy VCCIO** This setting configured Thunderbolt LSx/BSSB-LS 0 VCCIO.	TGL-H	TX VCCIO

Table 2-18. - Intel® Precise Touch and Stylus

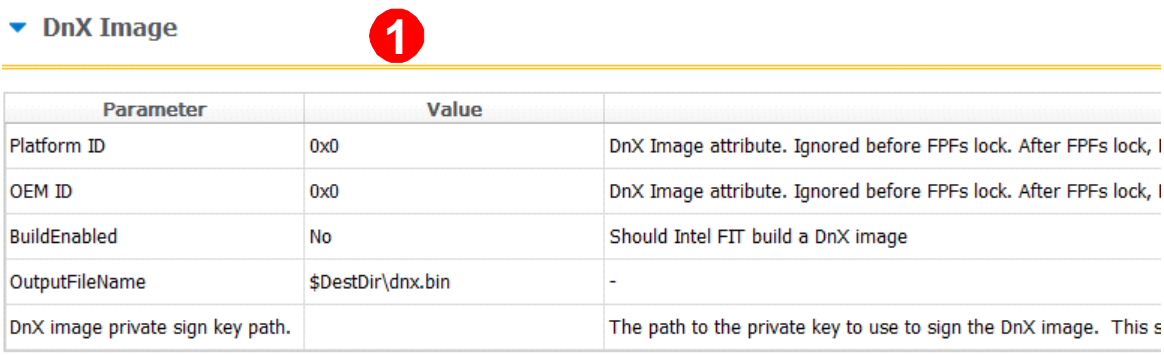
Click on Intel® Precise Touch and Stylus in the left tabs menu> Intel® Precise Touch and Stylus Configuration is expanded by default:



#	Parameter	Platform	Settings
1	**Intel® Precise Touch and Stylus Configuration**		
	Intel® Precise Touch and Stylus Controller 1 Maximum Frequency **Values: 17MHz, 30MHz, 48MHz** This setting allows customers to set an upper limit on the frequency for the Intel® Precise Touch and Stylus Controller 1 interface.	TGL-H	30MHz
	Intel® Precise Touch and Stylus Enabled **Values: Yes / No** This setting enables / disables the Intel® Precise Touch and Stylus interface.	TGL-H	No
	Intel® Precise Touch and Stylus Controller 2 Maximum Frequency **Values: 17MHz, 30MHz, 48MHz** This setting allows customers to set an upper limit on the frequency for the Intel® Precise Touch and Stylus Controller 2 interface.	TGL-H	17MHz

Table 2-19. - Download and Execute

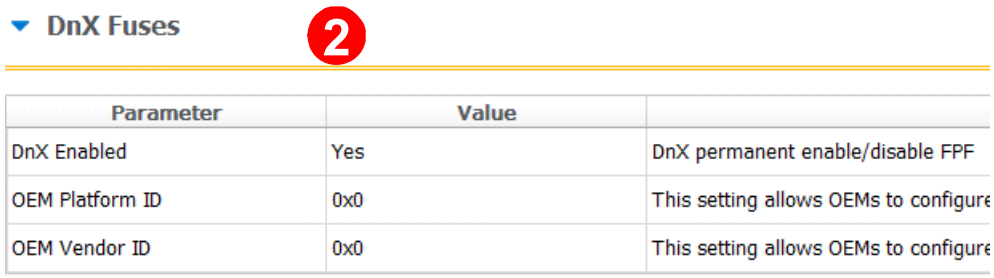
Click on Download and Execute in the left tabs menu> DnX Image is expanded by default:



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

Click on Download and Execute in the left tabs menu> DnX Fuses is expanded by default:

Table 2-19. - Download and Execute



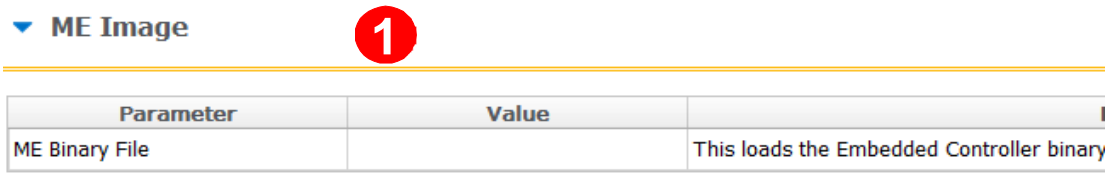
DnX Fuses

Parameter	Value	
DnX Enabled	Yes	DnX permanent enable/disable FPF
OEM Platform ID	0x0	This setting allows OEMs to configure
OEM Vendor ID	0x0	This setting allows OEMs to configure

2	**DnX Fuses**		
	DnX Enabled **Value: Yes / No** This setting enables / disables DnX. ***Caution:*** Setting this option to No will permanently DnX on the platform hardware.	TGL-H	Yes
	Platform ID **Value: Hex** This configures the Platform ID that DnX uses to verify the image is correct for the platform. Before FPFs are fused, this field is ignored and DnX will accept any image. After FPS lock, only images with this Platform ID will be accepted by DnX. ***Caution:*** Ensure that the Platform ID value is correctly populated prior to close of manufacturing on the platform.	TGL-H	0
	OEM ID **Value: Hex** This configures the OEM ID that DnX uses to verify the image is correct for the platform. Before FPFs fused, this field is ignored and DnX will accept any image. After FPF lock, only images with this OEM ID will be accepted by DnX. ***Caution:*** Ensure that the OEM ID value is correctly populated prior to close of manufacturing on the platform.	TGL-H	0

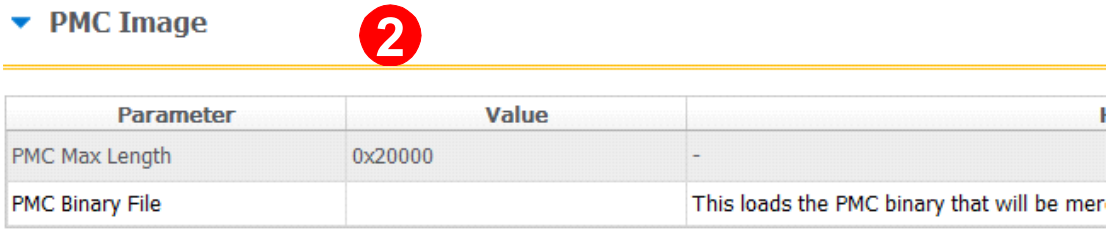
Table 2-20. - FW Update Image Build

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



#	Parameter	Platform	Settings
	The FW Update Image Build tab allows users to build firmware update image binaries based on one or several of the following elements combined together: **Intel® ME, PMC, OEM KM, IOM, MG, TBT, ISH, iUnit, PCHC and GBST**		
1	**ME Image**		
	ME Binary Image **Values: Binary File** This loads the Embedded Controller binary that will be merged into the FWUpdate image generated by the Intel® FIT tool.	TGL-H	ME Binary

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



#	Parameter	Platform	Settings
2	**PMC Image**		
	PMC Max Length		
	PMC Binary Image **Values: Binary File** This loads the PMC binary that will be merged into the FWUpdate image generated by the Intel® FIT tool.	TGL-H	PMC Binary

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

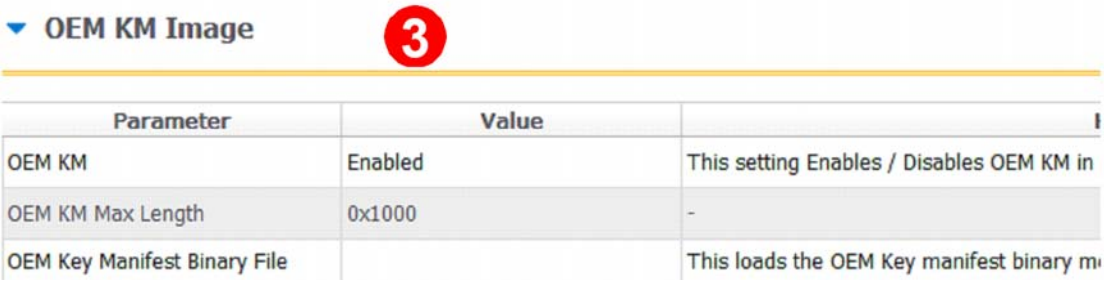
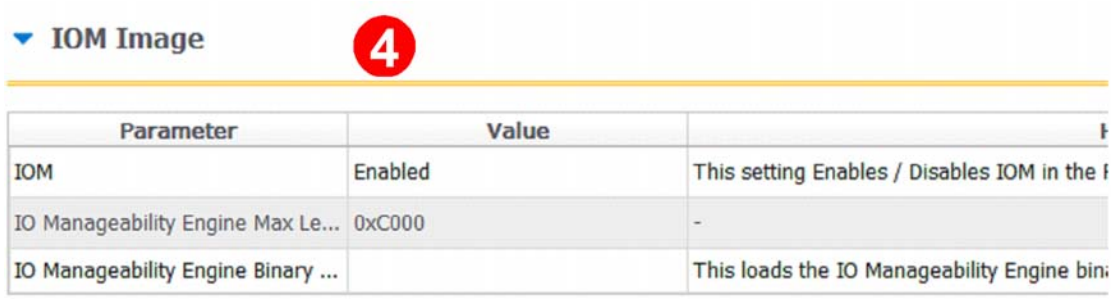


Table 2-20. - FW Update Image Build

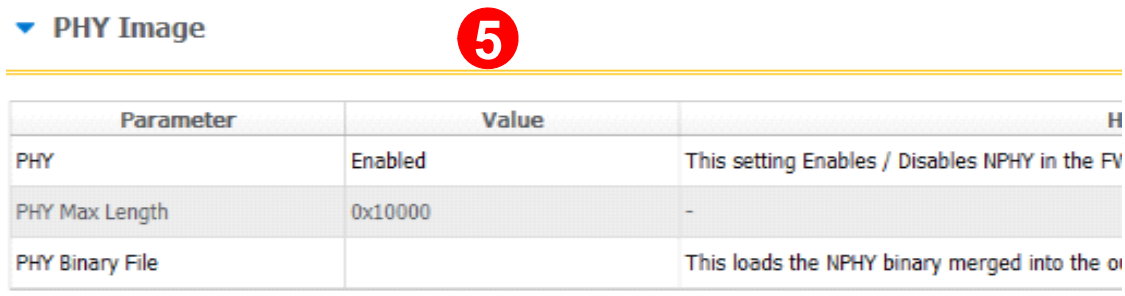
#	Parameter	Platform	Settings
3	**OEM KM Image**		
	OEM KM **Values: Enabled / Disabled** This setting Enables / Disables OEM KM in the FWUpdate image.	TGL-H	Enabled
	OEM KM Max Length		
	OEM Key Manifest Binary File **Values: Binary File** This loads the OEM Key manifest binary merged into the output image generated by the Intel® FIT tool.	TGL-H	OEM KM Binary

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



#	Parameter	Platform	Settings
4	**IOM Image**		
	IOM **Values: Enabled / Disabled** This setting Enables / Disables IOM in the FWUpdate image.	TGL-H	Enabled
	IO Manageability Engine Max Length		
	IO Manageability Engine Binary File **Values: Binary File** This loads the IO Manageability binary merged into the output image generated by the Intel® FIT tool.	TGL-H	IOM Binary

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

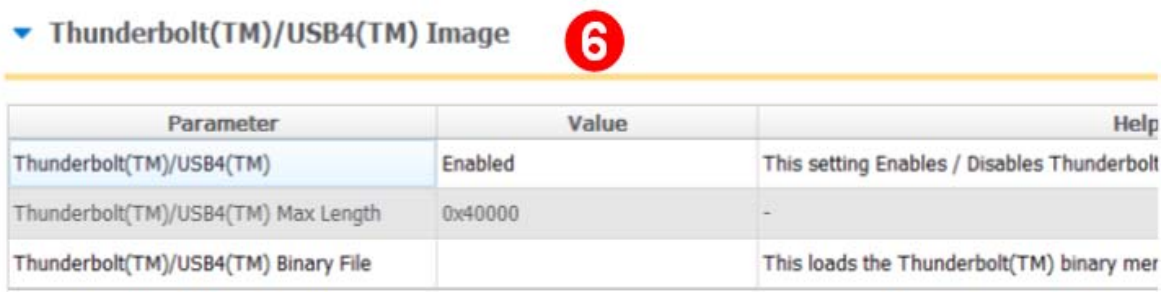


#	Parameter	Platform	Settings

Table 2-20. - FW Update Image Build

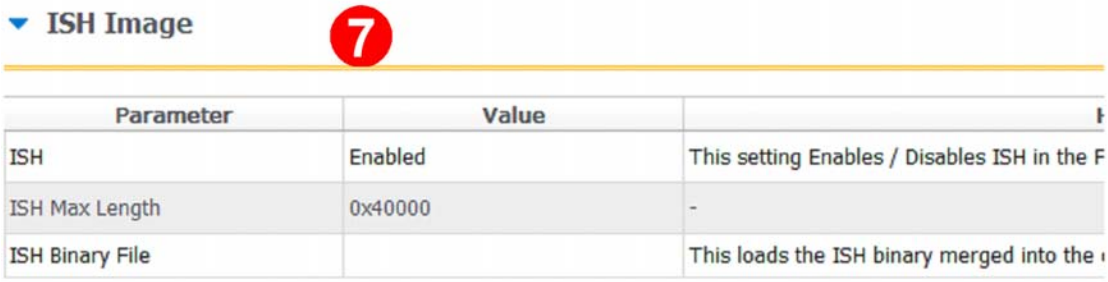
5	**PHY Image**		
	PHY **Values: Enabled / Disabled** This setting Enables / Disables NPHY in the FWUpdate image.	TGL-H	Enabled
	PHY Max Length		
	PHY Binary File **Values: Binary File** This loads the NPHY binary merged into the output image generated by the Intel® FIT tool.	TGL-H	NPHY Binary

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



#	Parameter	Platform	Settings
6	**TBT Image**		
	Thunderbolt(TM) / USB4(TM) **Values: Enabled / Disabled** This setting Enables / Disables Thunderbolt(TM)/USB4(TM) in the FWUpdate image.	TGL-H	Enabled
	Thunderbolt(TM) / USB4(TM) Max Length		
	Thunderbolt(TM) / USB4(TM) Binary File **Values: Binary File** This loads the Thunderbolt(TM)/USB4(TM) binary merged into the output image generated by the Intel® FIT tool.	TGL-H	TBT Binary

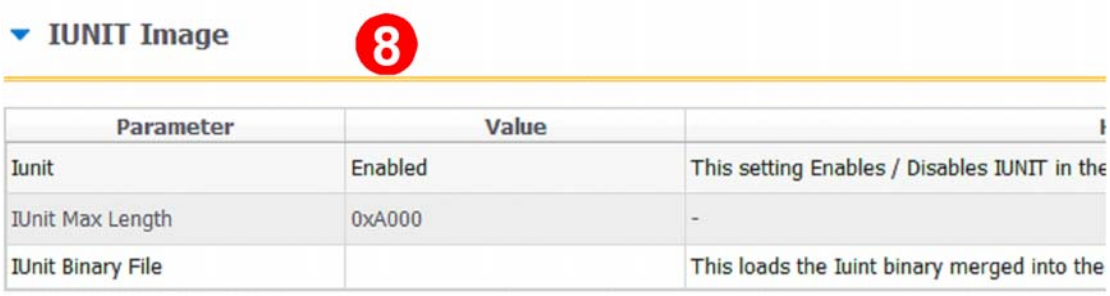
Click on FW Update Image Build in the left tabs menu> ISH Image is expanded by default:



#	Parameter	Platform	Settings
7	**ISH Image**		

Table 2-20. - FW Update Image Build

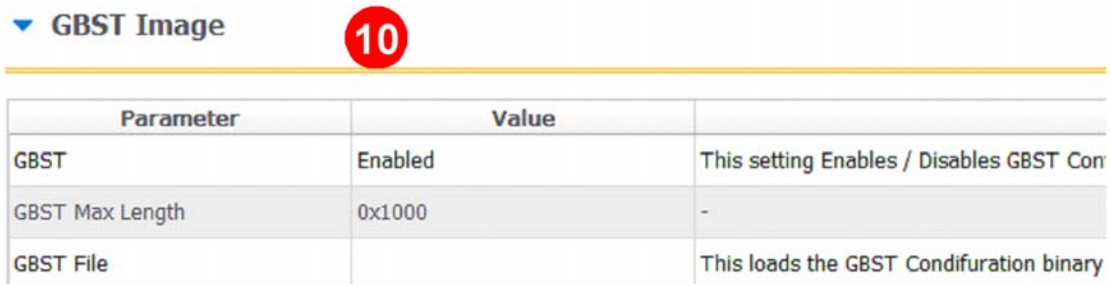
	ISH **Values: Enabled / Disabled** This setting Enables / Disables ISH in the FWUpdate image.	TGL-H	Enabled
	ISH Max Length		
	ISH Binary File **Values: Binary File** This loads the ISH binary merged into the output image generated by the Intel® FIT tool.	TGL-H	ISH Binary
Click on FW Update Image Build in the left tabs menu> IUNIT Image is expanded by default:			



#	Parameter	Platform	Settings
8	**IUNIT Image**		
	IUnit **Values: Enabled / Disabled** This setting Enables / Disables IUNIT in the FWUpdate image.	TGL-H	Enabled
	IUnit Max Length		
	IUnit Binary File **Values: Binary File** This loads the IUnit binary merged into the output image generated by the Intel® FIT tool.	TGL-H	IUnit Binary
Click on FW Update Image Build in the left tabs menu> PCHC Image is expanded by default:			

#	Parameter	Platform	Settings
9	**PCHC Image**		
	PCH Configuration Max Length		
	Values: Binary File This loads the PCHC binary merged into the output image generated by the Intel® FIT tool.	TGL-H	PCHC Binary
Click on FW Update Image Build in the left tabs menu> GBST Image is expanded by default:			

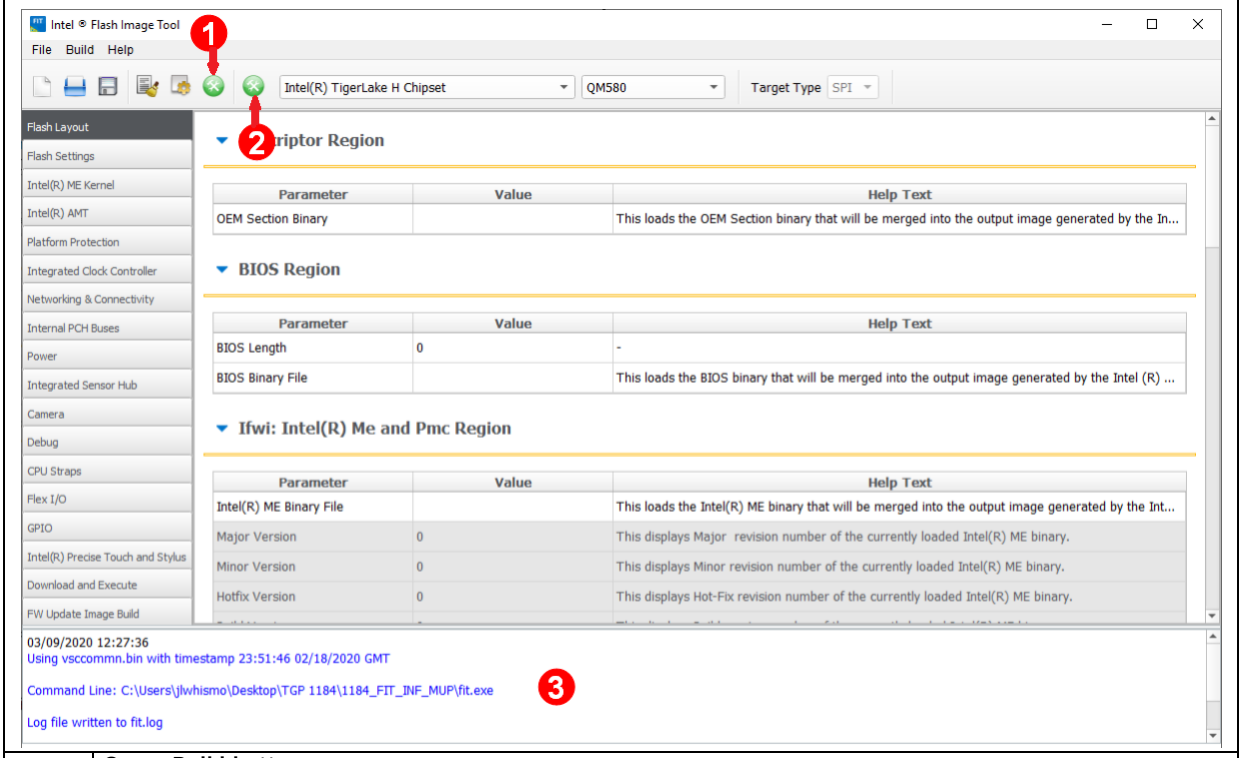
Table 2-20. - FW Update Image Build



#	Parameter	Platform	Settings
10	**GBST Image**		
	GBST Configuration Enable **Values: Enabled / Disabled** This setting Enables / Disables GBST in the FWUpdate image.	TGL-H	Disabled
	GBST Configuration Max Length		
	Values: Binary File This loads the GBST binary merged into 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.	TGL-H	GBST Binary (Optional)

Table 2-21. - Intel® FIT - Build Image

#	Parameter	CRB	Values



1	**Green Build button** Can also select CTRL+B, or Build> Build Image from the menu bar along the top of the screen
2	**Console shows status of build and path where saved**
3	**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® ME 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: 15.0.0.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

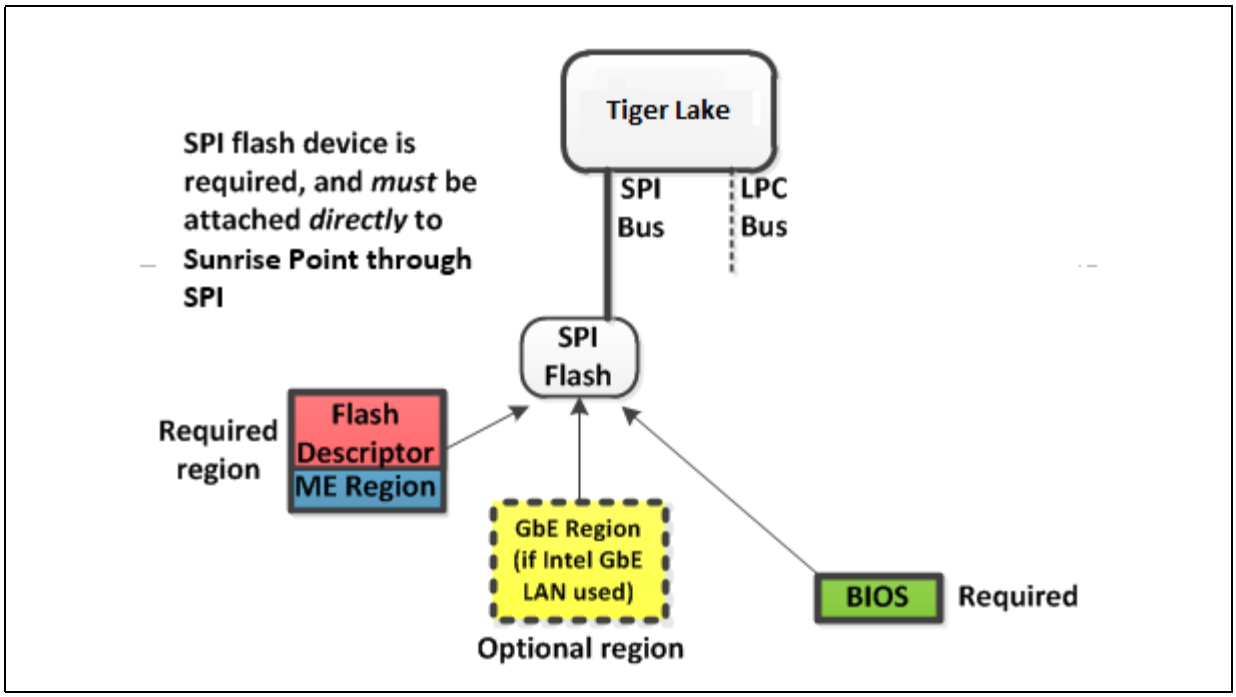
Problem / Issue	Solution / Workaround
System does not boot to DOS	By default, the system will boot to EFI Shell. To boot to DOS, 1. Enter BIOS menu, then go to the 'Boot' screen 2. Change 'Boot Option #1' to be your USB key (ensure USB key is formatted to be DOS bootable) 3. Press 'F4' to save settings and reboot
Hear 3 beeps when platform powers on	Possible device is disconnected or device not found, check • 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: • 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 - Mobile Family clocks, see Intel® *Tiger Lake PCH-H / LP Clocks* and *Intel® Converged Security and Management Engine — Platform Compliancy Guide for ME Hardware*.

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



§ §

B Appendix — Intel® ICCS SKU Support Matrix

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

Note: Please refer to Tiger Lake-H/LP Platform Controller Hub (PCH) External Design Specification (EDS) for details about Tiger Lake-H/LP Chipset Clock architecture

In below tables,

Min = Clock Div Max (minimum allowed frequency)

Max = Clock Div Min (maximum allowed frequency)

B.1 Intel® ICCS SKU Matrix - TGP-H

Note: ICC SKU is divided into 2 categories: Basic and Enhanced. Mark "x" indicates category supported by PCH SKU.

Table B-1. Intel® ICCS SKU Matrix - TGP-H

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

B.2 How to configure CLKREQ# parameters

Below table provides guideline on how to configure CLKREQ# parameters for SRC[0:15] output clocks depending on dynamic control of the clock via CLKREQ is required or not.

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.

Note: In below table, Mask Control CLKREQ cannot be configured via FIT Tool. It's configured to default once by FW during cold boot and bios can set/clear bits anytime.

C Appendix — Boot Guard Configuration

C.1 Boot Guard Profiles

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

Table C-1. Profile Description

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

C.2 Enforcement Policies

Table C-2. Enforcement Policy Description

Error Enforcement Policy (ENF)	Enforcement Mode Name	Description
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.

C.3 OEM Profile Parameters

Table C-3. Profile Parameters Description

Parameter	Description	Settings
Force Boot Guard ACM Enabled (F)	Force Boot Guard Boot determines if the platform starts the Force Boot Guard Boot timer. If it successfully starts it indicates success. When the Force Boot Guard timer stops, it starts the Protect Bios Environment timer, if indicated by the boot policy restrictions. Anchor ACM then jumps to the Initial Boot Block(IBB) with the Force Boot Guard Boot time stopped and the Protect BIOS enable timer running.	**false** - Allow the CPU to jump to the legacy reset vector if the Boot Guard Module cannot be successfully loaded. (default) **true -** Force the Boot Guard ACM to execute.
Verified Boot Enabled (V)	Boot Guard cryptographically verifies the platform Initial Boot Block (IBB) using the boot policy key. On successful verification, Boot Guard executes Initial Boot Block (IBB) using the boot policy key. If the verification fails, Anchor signals or enters Remediation.	**false** - Platform does not perform verified boot (default) **true** - Platform performs verified boot
Measured Boot Enabled (M)	Boot Guard measures the Initial Boot Block (IBB) into the TPM. Boot Guard perform no verification that the IBB is correct or from the platform manufacturer. The Slylake 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, • Allowing platform to continue to boot • Immediate Shutdown • Shutdown with Timeout intervals When the ENF logic is invoked, PTT or TPM also disconnects.	See Section C-2 for details.

D Appendix — Intel® Platform Trust Technology

D.1 Intel® Platform Trust Technology

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

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

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

E 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 Tiger Lake Mobile, Tiger 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 E-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.