Ice Lake-N Intel® Converged Security and Management Engine Firmware 13.0

Slim Firmware Bring Up Guide

September 2019

Revision 1.1

The Ice Lake Platform and Ice Lake PCH products may contain design defects or errors known as errata which may cause the product to deviate from published specifications. Current characterized errata are available on request.

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

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

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

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

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

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

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.

Contents

Figures

Tables

Revision History

Document Number	Revision Number	Description	Revision Date
	0.8	Initial Release	October 2018
	0.81	Added PCH Configuration settings Added Gen2 / Gen4 settings to Integrated Clock Controller tab	December 2018
	0.82	Updated PD Type-C Port 1 SMBus values	February 2019
	0.83	Corrected USB3 / PCIe Combo port designations	February 2019
	0.84	Updated PD Controller 2 Re-timer SMBus address and SmBus address for ICL-YN	March 2019
	0.85	Additional changes for PD Controllers	March 2019
	1.0	Updated to Rev 1.0	July 2019
	1.1	Changed MG PHY to NPHY for Type-C Firmware Anti-Rollback Configuration	September 2019

§ §

1 Introduction

This document covers the Intel® Converged Security and Management Engine Firmware (Intel® CSME) 13.0 - Consumer Firmware bring up procedure. Intel® CSME is tied to essential platform functionality — this dependency cannot be avoided for engineering reasons.

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

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

1.1 Related Documentation

VIP: Kit# xxxxxx - Intel® Ethernet Network Connections (20.1 OEM Gen) - LAN Software Production Candidate 20.1

CDI # xxxxxx Intel® Ethernet Connection i2xx [TBD]

1.2 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.

1.3 Prerequisites

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

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

This document makes only the following limited assumptions regarding hardware:

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

1.4 Acronyms and Definitions

1.4.1 General

Acronym or Term	Definition
BIOS	Basic Input Output System
DIMM	Dual In-line Memory Module
DMI	Direct Media Interface
EC	Embedded Controller
FPF	Field Programmable Fuses
FW	Firmware
GbE	Gigabit Ethernet
HECI	Host Embedded Controller Interface (aka Intel® MEI)
Intel® ICCS	Intel® Integrated Clock Controller Service
Intel® CSME	Intel® Converged Security and Management Engine (Intel®CSME)
Intel® MEI	Intel® Management Engine Interface (Intel® MEI) (renamed from HECI)
Intel® PTT	Intel® Platform Trusted Technology (Intel® PPT)
Intel® MSS	Intel® Management and Security Status Application
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
SMBus	System Management Bus
SPI Flash	Serial Peripheral Interface Flash
TPM	Trusted Platform Module
VSCC	Vendor Specific Configuration

1.4.2 Intel® Converged Security and Management Engine

Acronym or Term	Definition
3PDS	3rd Party Data Storage
Agent	Software that runs on a client PC with OS running
End User	The person who uses the computer (either Desktop or Mobile). In corporate, the user usually does not have administrator privileges.
Host or Host CPU	The processor that is running the operating system. This is different than the management processor running the Intel® Converged Security and Management Engine Firmware.
Host Service/Application	An application that is running on the host CPU
INF	An information file (.inf) used by Microsoft* operating systems that supports the Plug & Play feature. When installing a driver, this file provides the OS the necessary information about driver filenames, driver components, and supported hardware.
Intel® Management Engine Interface (Intel® MEI)	Interface between the 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 Service: A SW application which runs on the host machine and provide a secured communication between the ISV agent and the Intel® Management Engine Firmware.
Intel® ME	Intel® Management Engine: The embedded processor residing in the chipset MCP
MECI	ME-VE Communication Interface
NVM	Non-Volatile Memory: A type of memory that will retain its contents even if power is removed. In the Intel® AMT current implementation, this is achieved using a FLASH memory device.
OOB Interface	Out Of Band interface: This is WSMAN interface over secure or non-secure TCP protocol.
OS not Functional	The Host OS is considered non-functional in Sx power state and any one of the following cases when system is in S0 power state: • OS is hung • After PCI reset • OS watch dog expires • OS is not present
System States	Operating System power states such as S0. See detailed definitions in System States and Power Management section.

1.4.3 System States and Power Management

Acronym or Term	Definition
G3	A system state of Mechanical Off where all power is disconnected from the system. G3 power state does not necessarily indicate that RTC power is removed.
CM0	Intel® Management Engine firmware power state where all hardware power planes are activated. The host power state is S0.
CM3	Intel® 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® CSME Well Powered; (Intel® ME core not consuming power) DRAM available.
CM3-PG	An Intel® CSME Firmware power state where no power is applied to the 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® 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.

1.5 Reference Documents

Document	Doc Number / Location*
Ice Lake Intel® Converged Security and Management Engine (Intel® CSME) and Embedded Controller Interaction Product Specification Revision 0.5	549024 / CDI
Intel® Management Engine BIOS Writers Guide	TBD / *
Intel® Converged Security and Management Engine (Intel® CSME) 13 SKU Firmware Consumer *Compliance Guide for Ice Lake PCH-H/LP Chipset Family - Ice Lake Platform Compliancy and Testing Guide - Revision 1.1*	TBD / CDI

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

1.6 Format and Notation

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

Table 1-1. Number Format Notation

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

Table 1-2. Data Format Notation

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

1.7 Kit Contents

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

Table 1-3. Kit Contents (Sheet 1 of 7)

File or [Directory]	Content Description
[root]	Root directory
ConsumerICL-LP Consumer Bring Up Guide.pdf	This document
Icelake-LP Client SPI Programming Guide.pdf	How to program SPI device parameters and descriptor region details. Also contains a complete SPI Flash softstrap reference.
[Image Components]	
[3rd party Licenses in FW]	Third Party Licenses used in firmware
Apache Harmony Apache Version 2.0, January 2004 w header.txt	
Apache-Xerces-Java-XML-Parser.txt	
ConvertUTF unicode license.txt	
CxImage license complete.txt	
HTTP Client C MIT license.txt	
llvm.org University of Illinois_NCSA.txt	
Minix 3.pdf	
MIT Kerberos for Windows.pdf	
newlib_licenses.txt	
wpa supplicant license.txt	
zlib license.txt	
[CSME]	Intel® CSME firmware image (**Non Production FW Rom Bypass**) - supports **unfused** Icelake 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.
[Silicon]	
[LP]	
CSME_FW_Consumer_ICP-LP_B0_PCH.bin CSME_FW_Consumer_ICP-H_A0_PCH.bin	Intel® CSME firmware image (**Non Production FW**) - supports **unfused** Ice Lake 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.
[Documentation]	
ICL_Intel_IOM_ FW_Release_Notes_02.009.0.00.pdf	
ICL_Intel_MG_Phy_FW_RN_7.0.2.6.pdf	
TBT Release Notes for Burnside Bridge A-Step Rev12.0.pdf	
TBT Release Notes for YFL B Rev 28.pdf	

Table 1-3. Kit Contents (Sheet 2 of 7)

File or [Directory]	Content Description
[IOM]	IOM binary
iomp_02.009.00.bin	
[NPHY]	NPHY Binary
nphyfwpkg_7.0.2.6.bin	
[Retimer]	Retimer Binaries
BBR_CDR_A1_ICL_PORTS_0_1_rev12_sign.bin	
BBR_CDR_A1_ICL_PORTS_2_3_rev12_sign.bin	
[TBTYFL]	Thunderbolt$^{(TM)}$ binary
TBT_YFL_B0_REV28_signed.bin	
[Installers]	
Intel®_ME SW Installation Guide.pdf	Intel® CSME Software installation Guide.
[3rd party Licenses SW]	Third Party Licenses used in software
ACE-TAO-CIAO.pdf	
Apache-Xerces-C++-XML-Parser.txt	
libxml2.txt	
Microsoft Windows Classic Samples.txt	
openwsman.pdf	
Windows driver samples.txt	
WixLicenseNote.txt	
[ME_SW_MSI]	
IntelMEFWVer.dll	DLL file
MUP	XML file
SetupME	Intel® CSME software installer
[MEI-Only Installer MSI]	
IntelMEFWVer.dll	DLL file
MEISetup	MEI software installer
MUP	XML file
[WindowsDriverPackages]	Windows* driver packages
[ICLS]	Intel® Capability Licensing Service drivers
iclsClient.cat	
iclsClient..inf	
[iCLS]	
[conf]	
cacert.pem	
epid_paramcert.dat	
epid2_paramacert.dat	
EPIDGroupCertLegacy.cer	
EPIDGroupdCertX509.cer	
iclsProxy.conf	

Table 1-3. Kit Contents (Sheet 3 of 7)

File or [Directory]	Content Description
[Documents]	Documents for Intel® Capability Licensing Service
development_tools.txt	
License.txt	
Readme.txt	
redist.txt	
Third Party Licenses.txt	
[x64]	x64 drivers
iclsClient.dll	
iclsClientInternal.dll	
iclsProxy.dll	
iclsProxyInternal.dll	
IntelPTTEKRecertification.exe	
libcrypto-1_1-x64.dll	
libssl-1_1-x64.dll	
SocketHeciServer.exe	
TPMProvisioningService.exe	
[x86]	x86 drivers
x86_iclsClient.dll	
x86_iclsClientInternal.dll	
x86_iclsProxy.dll	
x86_iclsProxyInternal.dll	
x86_IntelPTTEKRecertification.exe	
x86_libcrypto-1_1-x64.dll	
x86_libssl-1_1-x64.dll	
x86_SocketHeciServer.exe	
x86_TPMProvisioningService.exe	
[vs2015]	
[x64]	x64 Visual Studio* runtime DLLs
msvcp140.dll	
vcruntime140.dll	
[x86]	x86 Visual Studio* runtime DLLs
x86_msvcp140.dll	
x86_vcruntime140.dll	
[JHI]	

Table 1-3. Kit Contents (Sheet 4 of 7)

File or [Directory]	Content Description
[win10]	Intel® Dynamic Application Loader drivers
bhPlugin.dll	
bhPluginV2.dll	
dal.cat	
DAL.inf	
JHI.dll	
jhi_service.exe	
JHI64.dll	
SpoolerApplet.dalp	
TEEManagement.dll	
TEEManagement64.dll	
TEETransport.dll	
[MEI]	Intel® MEI drivers files
heci.cat	
heci.inf	
[x64]	x64 driver
TeeDriverW8x64.sys	
[x86]	x86 driver
TeeDriverW8.sys	
OemExtension]	OEM Extension driver
OemExtension.cat	
OemExtension.inf	
[Tools]	
[3rd party Licenses in Tools]	Third part Licenses in Tools
Android Autogenerated Files Apache 2.0.pdf	
C Make License.pdf	
EFI tool kit intel BSD 2 clause license.txt	
Expat XMLparser MIT license.txt	
Jquery MIT license.txt	
JsonCpp MIT license.txt	
MSDN Example code.pdf	
pugixml license.txt	
[ICC_Tools]	
Intel® ME Firmware ICC Tools User Guide.pdf	ICC Tools User Guide
[CCT]	
cct	Exe file
cct	Ini file
cctDll.dll	
cctDllx64.dll	
cctWin	Exe file

Table 1-3. Kit Contents (Sheet 5 of 7)

File or [Directory]	Content Description
[EFI]	
cct.efi	CCT for EFI
[System Tools]	
System Tools User Guide.pdf	System Tools User Guide
[FIT]	
[system32]	
fit.exe	Intel® Flash Image Tool (Intel® FIT)
vsccommn.bin	Binary containing the supported SPI parts
VSCCommn_bin Content.pdf	Documentation listing the SPI parts supported by vscccommn.bin
[FPT]	
[EFI64]	
fparts.txt	List of supported SPI Flash devices with specific Flash parameters
fpt.efi	FPT for EFI
[Windows]	
fparts.txt	List of supported SPI Flash devices with specific Flash parameters
fptw.exe	FPT for Windows*
Idrvdll.dll	
Pmxdll.dll	
[Windows64]	
fparts.txt	List of supported SPI Flash devices with specific Flash parameters
fptw64.exe	Intel® FPT for Windows* (64-bit) OS
Idrvdll32e.dll	
Pmxdll32e.dll	
[FWUpdate]	
[EFI64]	
FWUpdLcl.efi	FW Update Tool (EFI version)
fwudef.h	
FwUpdateEfiLib.lib	
fwupdatelib.h	
fwupdatelibdeprecated.h	
[Win]	
FWUpdLcl.exe	FW Update Tool (Windows* version 32bit)
Idrvdll.dll	
Pmxdll.dll	
errorlist.c	

Table 1-3. Kit Contents (Sheet 6 of 7)

File or [Directory]	Content Description
errorlist.h	
fwudef.h	
fwupdatelib.h	
FWUpdateLib.lib	
fwupdatelibdeprecated.h	
FWUpdateSample.c	
[Win64]	
FWUpdLcl64.exe	FW Update Tool (Windows* version 64bit)
Idrvdll32e.dll	
Pmxdll32e.dll	
errorlist.c	
errorlist.h	
fwudef.h	
fwupdatelib.h	
FWUpdateLib.lib	
fwupdatelibdeprecated.h	
FWUpdateSample.c	
[FWUpdate_RS	FW Update Tool API code
[Efi64]	
fwUpdLcl.efi	
errorlist.c	
errorlist.h	
fwudef.h	
fwupdatelib.h	
FWUpdateLib.lib	
fwupdatelibdeprecated.h	
FWUpdateSample.c	
[MEInfo]	
[EFI64]	
MEInfo.efi	Intel® ME Information Tool (EFI version)
[Windows]	
MEInfoWin.exe	Intel® ME Information Tool (Windows* version 32bit)
Idrvdll.dll	
Pmxdll.dll	
[Windows64]	
MEInfoWin64.exe	Intel® ME Information Tool (Windows* version 64bit)
Idrvdll32e.dll	
Pmxdll32e.dll	

Table 1-3. Kit Contents (Sheet 7 of 7)

File or [Directory]	Content Description
[MEManuf]	
[EFI64]	
MEManuf.efi	Intel® ME Manufacturing Tool (EFI version)
[Windows]	
Idrvdll.dll	
MEManufWin.exe	Intel® ME Manufacturing Tool (Windows* version 32bit)
Pmxdll.dll	
[Windows64]	
Idrvdll32e.dll	
MEManufWin64.exe	Intel® ME Manufacturing Tool (Windows* version 64bit)
Pmxdll32e.dll	
(empty)	
[Manifest Extension Utility]	
[Win]	
Signing and Manifesting Guide.pdf	
[Windows32]	
meu.exe	Intel® Manifest Extension Utility (MEU) executable file that allows input of FW binary and outputs and independent updatable partition that is compressed and signed.

1.8 External Hardware Requirements for Bring Up

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

Windows* OS System	Flash Burner	DOS Bootable USB Key
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.

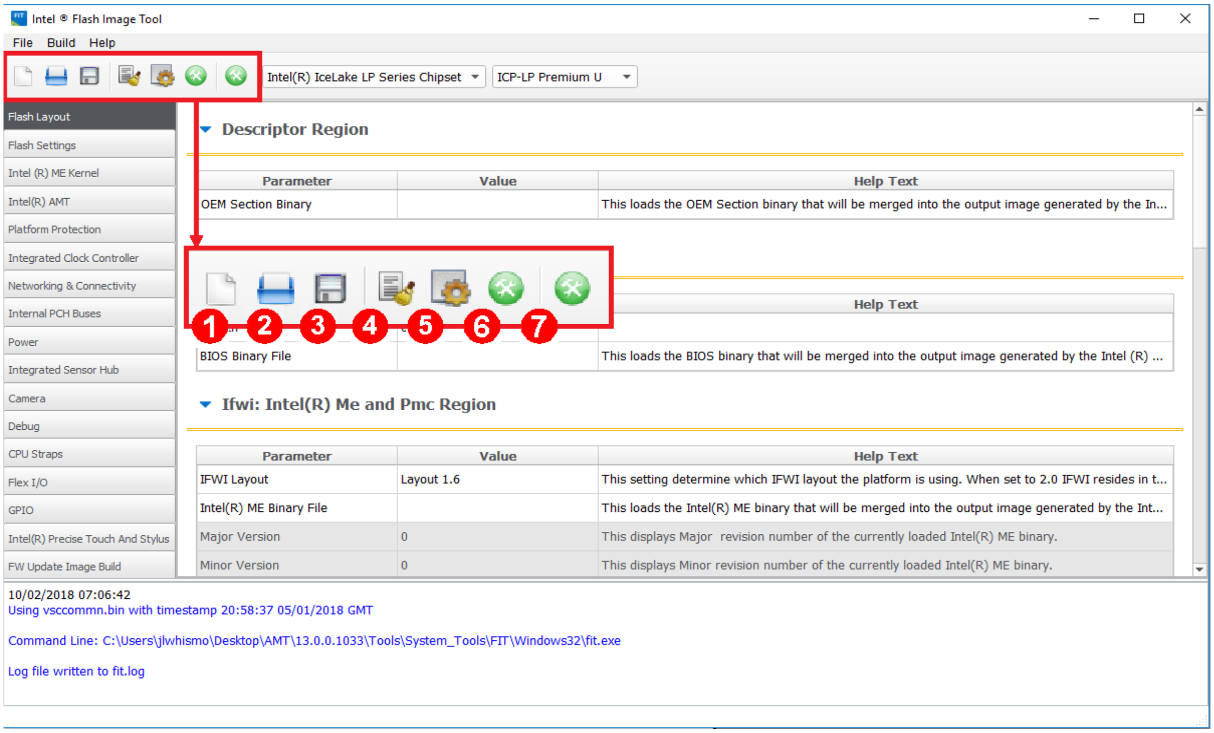
Note: The Flash Image Tool may be updated throughout the release cycles. As a general rule, please ensure you use the tools, images and other content from the same kit and refrain from using different version tools.

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 1.7). Double-click **FIT.exe**.
2. **NOTE:** In the tables below, where default settings are listed for ICL 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)



Parameter	Value	Help Text
OEM Section Binary		This loads the OEM Section binary that will be merged into the output image generated by the In...

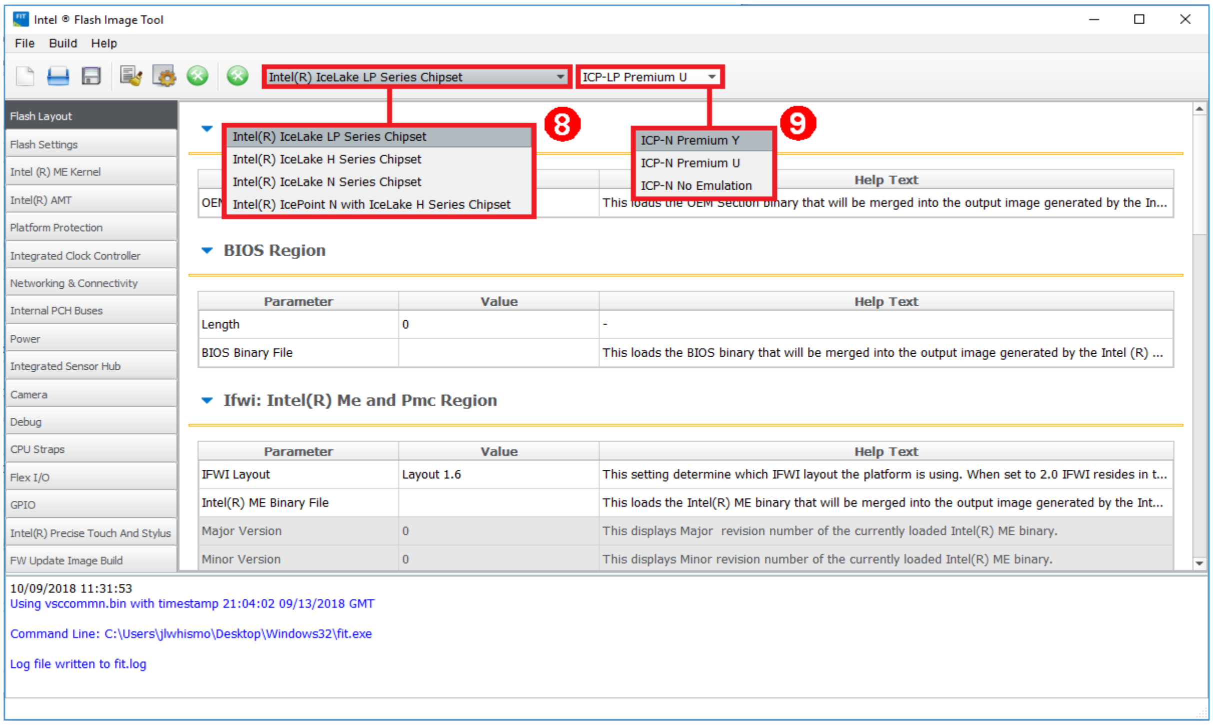
		Help Text
BIOS Binary File		This loads the BIOS binary that will be merged into the output image generated by the Intel (R) ...

Parameter	Value	Help Text
IFWI Layout	Layout 1.6	This setting determine which IFWI layout the platform is using. When set to 2.0 IFWI resides in t...
Intel(R) ME Binary File		This loads the Intel(R) ME binary that will be merged into the output image generated by the Int...
Major Version	0	This displays Major revision number of the currently loaded Intel(R) ME binary.
Minor Version	0	This displays Minor revision number of the currently loaded Intel(R) ME binary.

```
10/02/2018 07:06:42
Using vsccommn.bin with timestamp 20:58:37 05/01/2018 GMT

Command Line: C:\Users\jlwhismo\Desktop\AMT\13.0.0.1033\Tools\System_Tools\FIT\Windows32\fit.exe

Log file written to fit.log
```

#	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)



Intel(R) IceLake LP Series Chipset

ICP-LP Premium U

		Help Text
OEM		This loads the OEM section binary that will be merged into the output image generated by the In...

BIOS Region

Parameter	Value	Help Text
Length	0	-
BIOS Binary File		This loads the BIOS binary that will be merged into the output image generated by the Intel (R) ...

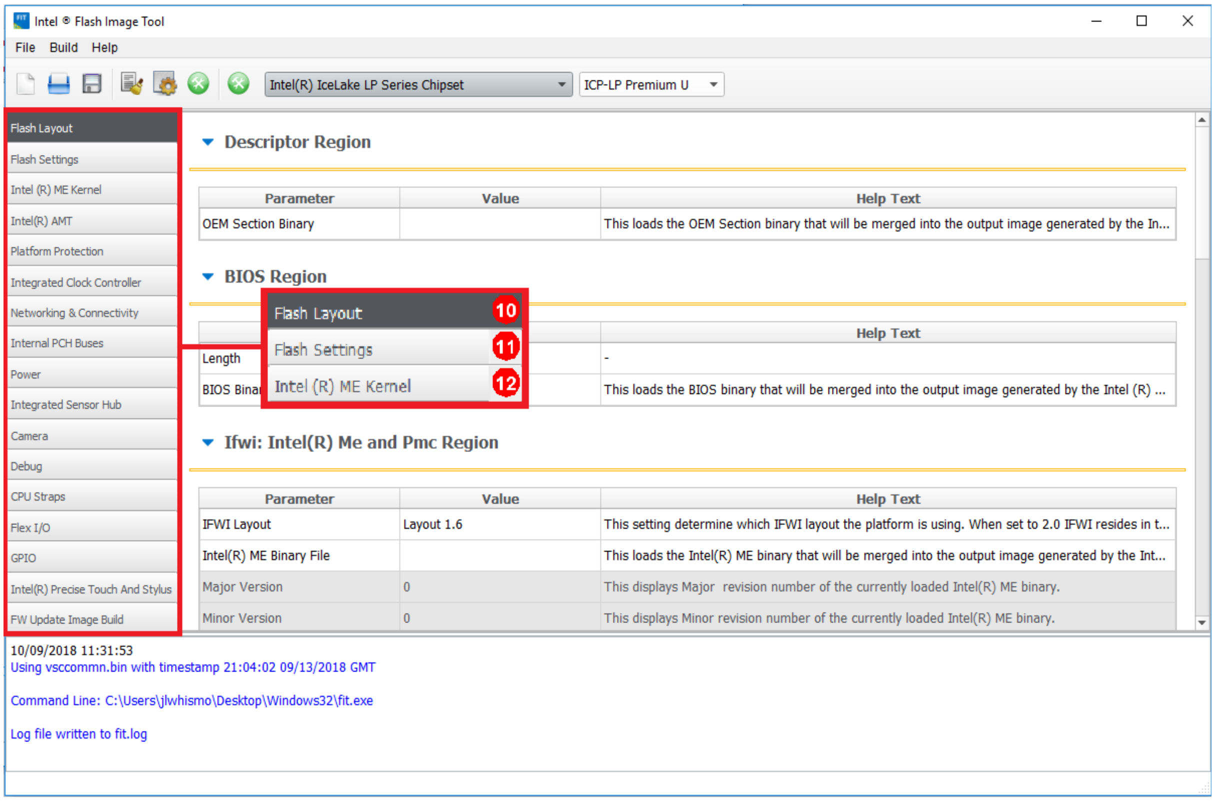
Ifwi: Intel(R) Me and Pmc Region

Parameter	Value	Help Text
IFWI Layout	Layout 1.6	This setting determine which IFWI layout the platform is using. When set to 2.0 IFWI resides in t...
Intel(R) ME Binary File		This loads the Intel(R) ME binary that will be merged into the output image generated by the Int...
Major Version	0	This displays Major revision number of the currently loaded Intel(R) ME binary.
Minor Version	0	This displays Minor revision number of the currently loaded Intel(R) ME binary.

```
10/09/2018 11:31:53
Using vsccommn.bin with timestamp 21:04:02 09/13/2018 GMT

Command Line: C:\Users\jlwhismo\Desktop\Windows32\fit.exe

Log file written to fit.log
```

#	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

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

#	Label	Contents
		

Intel(R) IceLake LP Series Chipset

ICP-LP Premium U

Descriptor Region

Parameter	Value	Help Text
OEM Section Binary		This loads the OEM Section binary that will be merged into the output image generated by the In...

BIOS Region

		Help Text
Length		-
BIOS Binar		This loads the BIOS binary that will be merged into the output image generated by the Intel (R) ...

Ifwi: Intel(R) Me and Pmc Region

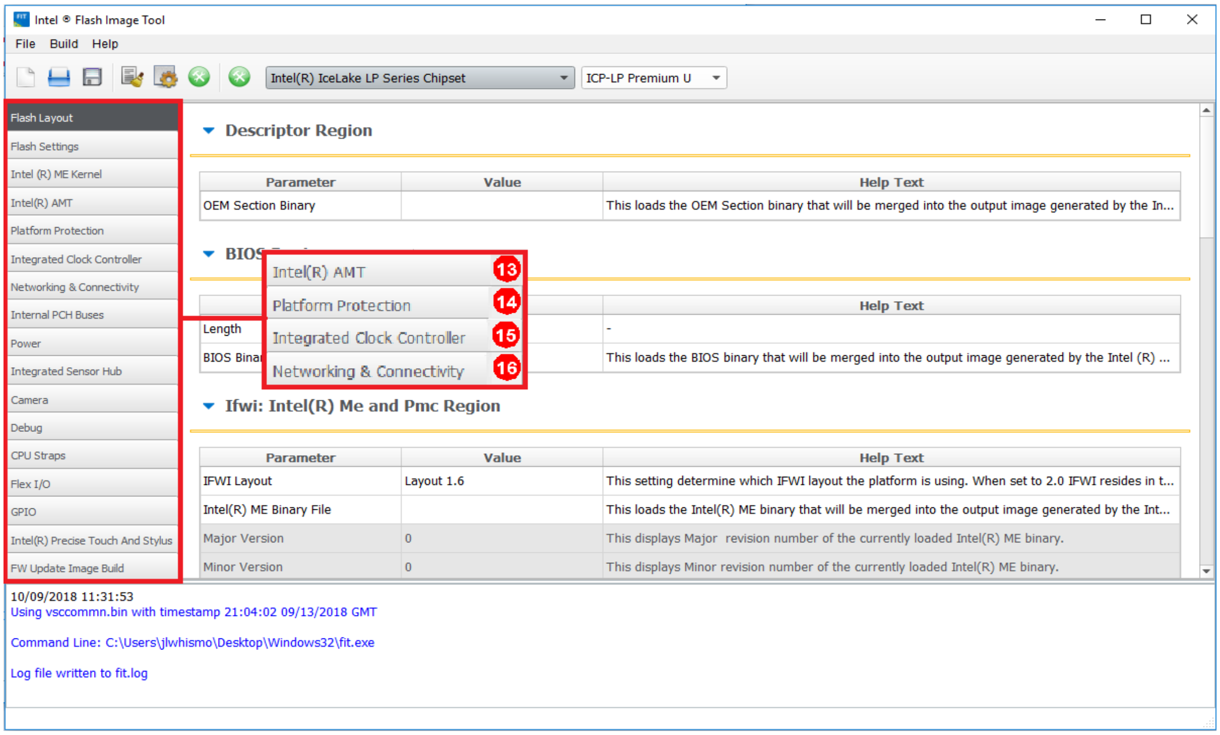
Parameter	Value	Help Text
IFWI Layout	Layout 1.6	This setting determine which IFWI layout the platform is using. When set to 2.0 IFWI resides in t...
Intel(R) ME Binary File		This loads the Intel(R) ME binary that will be merged into the output image generated by the Int...
Major Version	0	This displays Major revision number of the currently loaded Intel(R) ME binary.
Minor Version	0	This displays Minor revision number of the currently loaded Intel(R) ME binary.

```
10/09/2018 11:31:53
Using vsccommn.bin with timestamp 21:04:02 09/13/2018 GMT

Command Line: C:\Users\jlwhismo\Desktop\Windows32\fit.exe

Log file written to fit.log
```

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

#	Label	Contents
⑩	**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
⑪	**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 • VSCC Table - VSCC Entry • BIOS Configuration • OEM and Platform IDs • FPF Configuration
⑫	**Intel® ME Kernel Tab**	Intel® ME Kernel which contains (see Table 2-5): • Processor • Intel® ME Firmware Update • Intel® Services Configuration • Image Identification • Firmware Diagnostics • Post Manufacturing Lock • MCTP Configuration • Intel® ME Boot Configuration • Reserved

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

#	Label	Contents
		
13	**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
14	**Platform Protection Tab**	Platform Protection which contains (see Table 2-7): • Content Protection • Graphics uController • Hash Key Configuration for Bootguard / ISH • Exclusion Ranges • Descriptor Configuration • Boot Guard Configuration • Type-C Firmware Anti-Rollback Configuration • Intel® PTT Configuration • TPM Over SPI Bus Configuration • BIOS Guard Configuration • TXT Configuration • Crypto HW Support
15	**Integrated Clock Controller Tab**	Integrated Clock Controller which contains (see Table 2-8): • Integrated Clock Controller Policies • Profiles

Descriptor Region

Parameter	Value	Help Text
OEM Section Binary		This loads the OEM Section binary that will be merged into the output image generated by the In...

BIOS

Parameter	Value	Help Text
Length		-
BIOS Binar		This loads the BIOS binary that will be merged into the output image generated by the Intel (R) ...

Ifwi: Intel(R) Me and Pmc Region

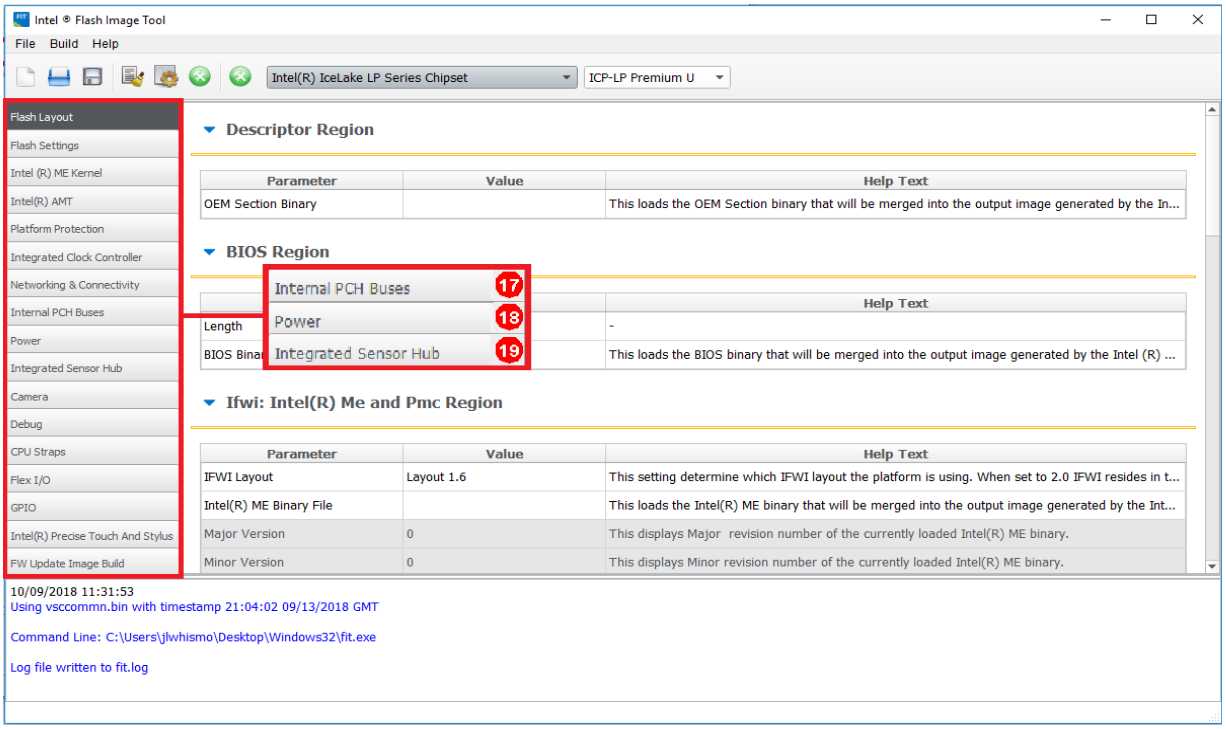
Parameter	Value	Help Text
IFWI Layout	Layout 1.6	This setting determine which IFWI layout the platform is using. When set to 2.0 IFWI resides in t...
Intel(R) ME Binary File		This loads the Intel(R) ME binary that will be merged into the output image generated by the Int...
Major Version	0	This displays Major revision number of the currently loaded Intel(R) ME binary.
Minor Version	0	This displays Minor revision number of the currently loaded Intel(R) ME binary.

```
10/09/2018 11:31:53
Using vsccommn.bin with timestamp 21:04:02 09/13/2018 GMT

Command Line: C:\Users\jlwhismo\Desktop\Windows32\fit.exe

Log file written to fit.log
```

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

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

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



Intel(R) IceLake LP Series Chipset

ICP-LP Premium U

Descriptor Region

Parameter	Value	Help Text
OEM Section Binary		This loads the OEM Section binary that will be merged into the output image generated by the In...

BIOS Region

		Help Text
Length		-
BIOS Binai		This loads the BIOS binary that will be merged into the output image generated by the Intel (R) ...

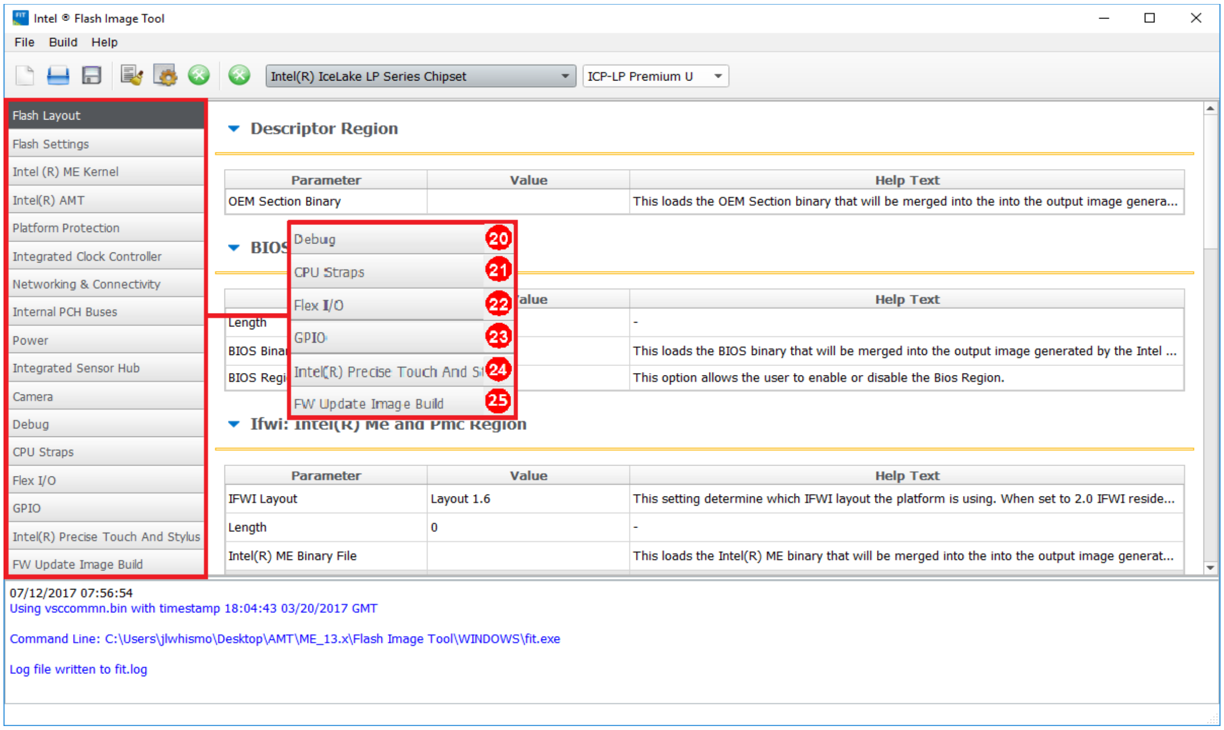
Ifwi: Intel(R) Me and Pmc Region

Parameter	Value	Help Text
IFWI Layout	Layout 1.6	This setting determine which IFWI layout the platform is using. When set to 2.0 IFWI resides in t...
Intel(R) ME Binary File		This loads the Intel(R) ME binary that will be merged into the output image generated by the Int...
Major Version	0	This displays Major revision number of the currently loaded Intel(R) ME binary.
Minor Version	0	This displays Minor revision number of the currently loaded Intel(R) ME binary.

```
10/09/2018 11:31:53
Using vsccommn.bin with timestamp 21:04:02 09/13/2018 GMT

Command Line: C:\Users\jlwhismo\Desktop\Windows32\fit.exe

Log file written to fit.log
```

#	Label	Contents
17	**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
18	**Power Tab**	Power which contains (see Table 2-11): • Platform Power • Deep Sx • PCH Thermal Reporting
19	**Integrated Sensor Hub Tab**	Integrated Sensor Hub which contains (see Table 2-12): • Integrated Sensor Hub • ISH Image • ISH Data

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



Intel(R) IceLake LP Series Chipset
ICP-LP Premium U

Descriptor Region

Parameter	Value	Help Text
OEM Section Binary		This loads the OEM Section binary that will be merged into the into the output image genera...

BIOS

Parameter	Value	Help Text
Length		-
BIOS Binar		This loads the BIOS binary that will be merged into the output image generated by the Intel ...
BIOS Regi		This option allows the user to enable or disable the Bios Region.

Ifwi: Intel(R) Me and Pmc Region

Parameter	Value	Help Text
IFWI Layout	Layout 1.6	This setting determine which IFWI layout the platform is using. When set to 2.0 IFWI reside...
Length	0	-
Intel(R) ME Binary File		This loads the Intel(R) ME binary that will be merged into the into the output image generat...

```
07/12/2017 07:56:54
Using vsccommn.bin with timestamp 18:04:43 03/20/2017 GMT

Command Line: C:\Users\jlwhismo\Desktop\AMT\ME_13.x\Flash Image Tool\WINDOWS\fit.exe

Log file written to fit.log
```

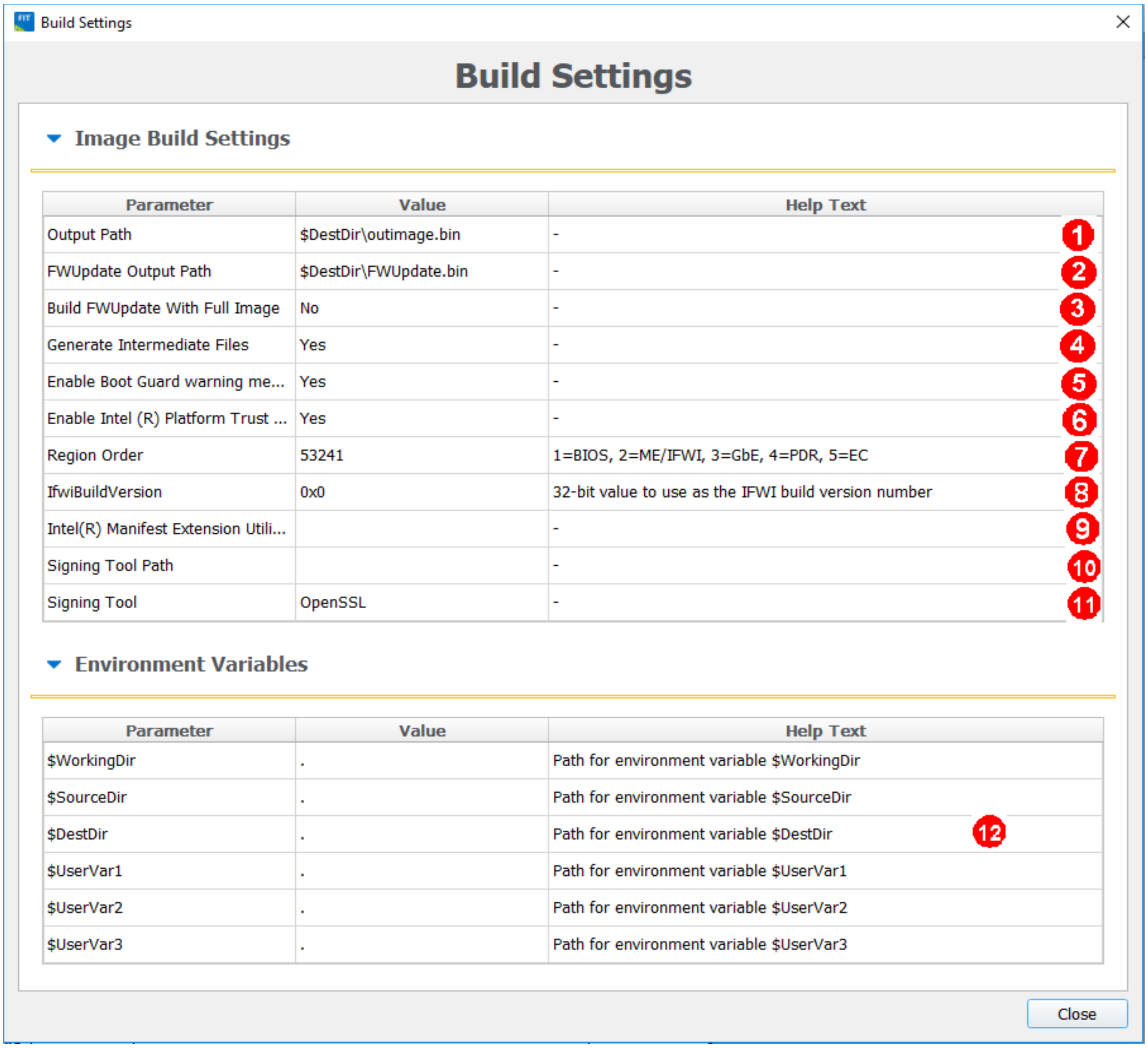
#	Label	Contents
⑳	**Debug Tab**	Debug which contains (see Table 2-13): • IDLM • Delayed Authentication Mode Configuration • Intel® Trace Hub Technology • Intel® ME Firmware Debugging Overrides • Direct Connection Interface Configuration • Early USB DBC over Type-A Configuration • eSPI Feature Overrides
㉑	**CPU Straps Tab**	CPU Straps which contain a detailed list of parameters (see Table 2-14) • CPU Straps
㉒	**Flex I/O Tab**	Flex I/O which contains (see Table 2-15): • Intel® RST for PCIe Configuration • PCIe Lane Reversal Configuration • PCIe Port Configuration • SATA / PCIe Combo Port Configuration • USB3 Port Configuration • USB2 Port Configuration • Type-C Subsystem Configuration • Thunderbolt Configuration • UFS Storage Configuration • Power Delivery PD Controller Configuration

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

#	Label	Contents
23	**GPIO Tab**	GPIO which contains (see Table 2-16): • LAN / GPIO Select • WLAN / GPIO Select • Platform Power / GPIO • ME Feature Pins • Touch Controller Pins • SMLink1 Pins • GPIO VCCIO Voltage Control • Thunderbolt LSx/BSSB-LS Configuration
24	**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
25	**FW Update Image Build**	FW Update Image Build which contains (see Table 2-18): • ME Image • PMC Image • OEM KM Image • IOM Image • MG Image • TBT Image • ISH Image • INUIT Image
	Console Window Area	Displays opening messages, log file entries, and build activity messages

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

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



Build Settings

Image Build Settings

Parameter	Value	Help Text
Output Path	$DestDir\outimage.bin	- ①
FWUpdate Output Path	$DestDir\FWUpdate.bin	- ②
Build FWUpdate With Full Image	No	- ③
Generate Intermediate Files	Yes	- ④
Enable Boot Guard warning me...	Yes	- ⑤
Enable Intel (R) Platform Trust ...	Yes	- ⑥
Region Order	53241	1=BIOS, 2=ME/IFWI, 3=GbE, 4=PDR, 5=EC ⑦
IfwiBuildVersion	0x0	32-bit value to use as the IFWI build version number ⑧
Intel(R) Manifest Extension Utili...		- ⑨
Signing Tool Path		- ⑩
Signing Tool	OpenSSL	- ⑪

Environment Variables

Parameter	Value	Help Text
$WorkingDir	.	Path for environment variable $WorkingDir
$SourceDir	.	Path for environment variable $SourceDir
$DestDir	.	Path for environment variable $DestDir ⑫
$UserVar1	.	Path for environment variable $UserVar1
$UserVar2	.	Path for environment variable $UserVar2
$UserVar3	.	Path for environment variable $UserVar3

#	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 3)

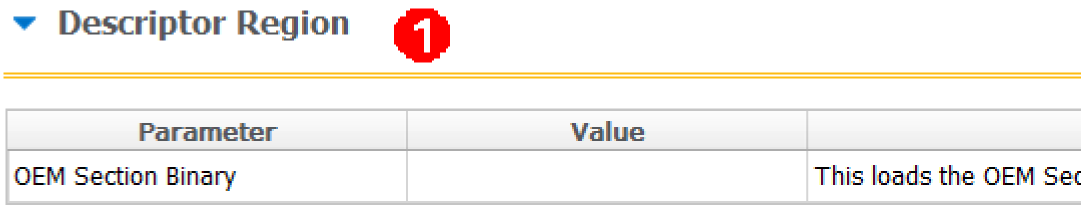
Click on Build Button in the top menu bar> Build Settings window pop up is displayed:			
④	**Generate Intermediate Files**	Yes	Yes/No - Yes is default
⑤	**Enable Boot Guard warning message at build time**	Yes	Yes/No - Yes is default
⑥	**Enable Intel (R) Platform Trust Technology warning message at build 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	**Intel® Manifest Extension Utility Path**	Yes	Yes/No - Yes is default
⑩	**Signing Tool Path**		This determines the path where the signing tool is located.
⑪	**Signing Tool**	OpenSSL	OpenSSL
⑫			$WorkingDir and $DestDir can be left at the default '.' Click on $SourceDir Value field and type in path where the Image Components are located for the Manageability Engine kit

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

Click on Build Button in the top menu bar> Build Settings window pop up is displayed:			
#	**Parameter**	**CRB**	**Values**
❺	**Region Order**	Yes	53241 - is default
❻	**IFWI Build Version**	Yes	0x0 is default
❼			$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 5)

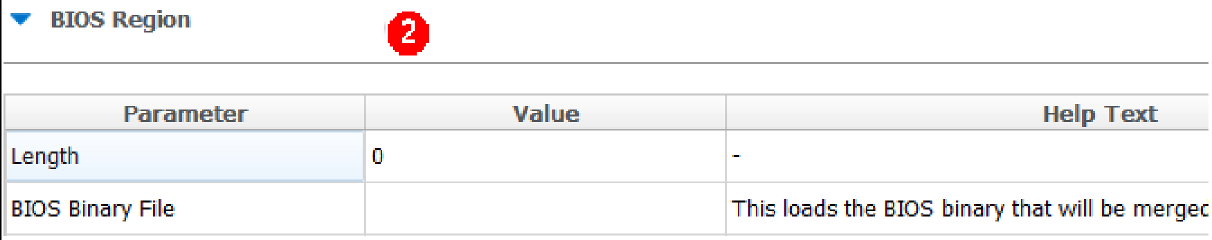
Click on Flash Layout in the left tabs menu> Descriptor Region is expanded by default:



Parameter	Value	
OEM Section Binary		This loads the OEM Sec

#	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.	ICL-YN ICL-UN	OEM Binary (optional)

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

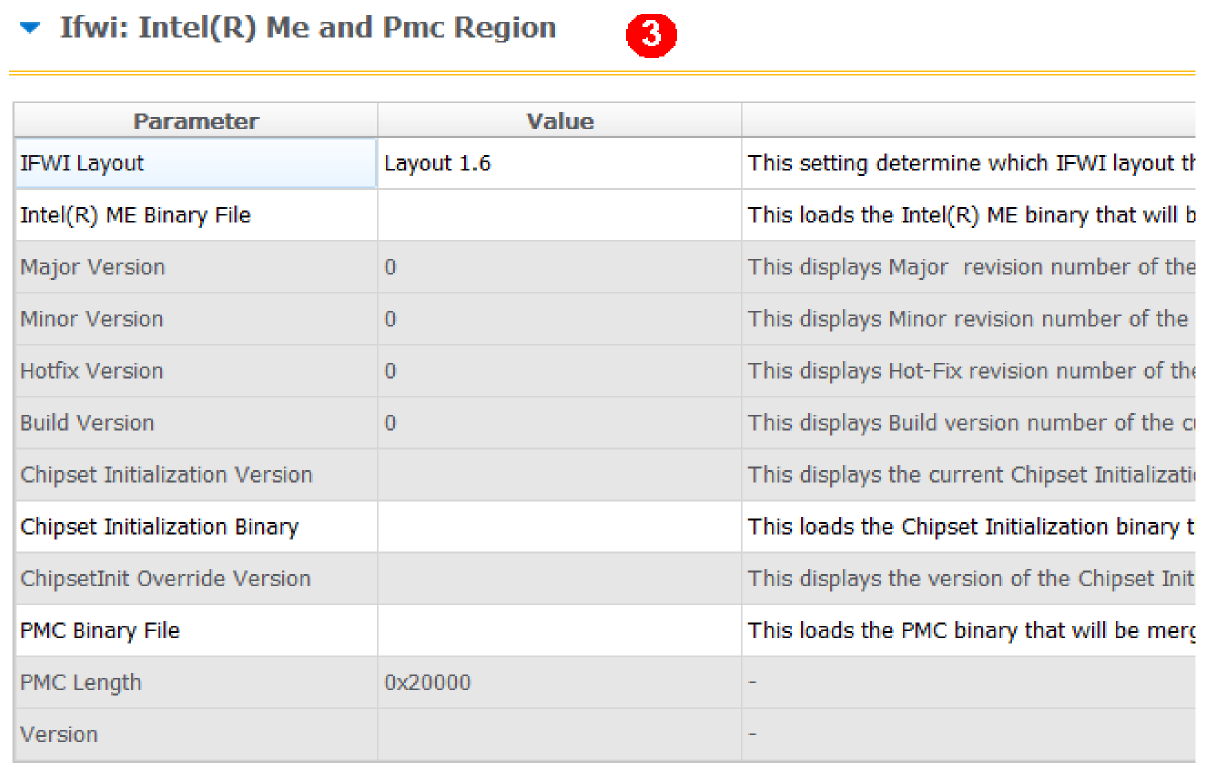


Parameter	Value	Help Text
Length	0	-
BIOS Binary File		This loads the BIOS binary that will be merge

#	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.	ICL-YN ICL-UN	biosimage.bin biosimage.bin

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

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



Ifwi: Intel(R) Me and Pmc Region ③

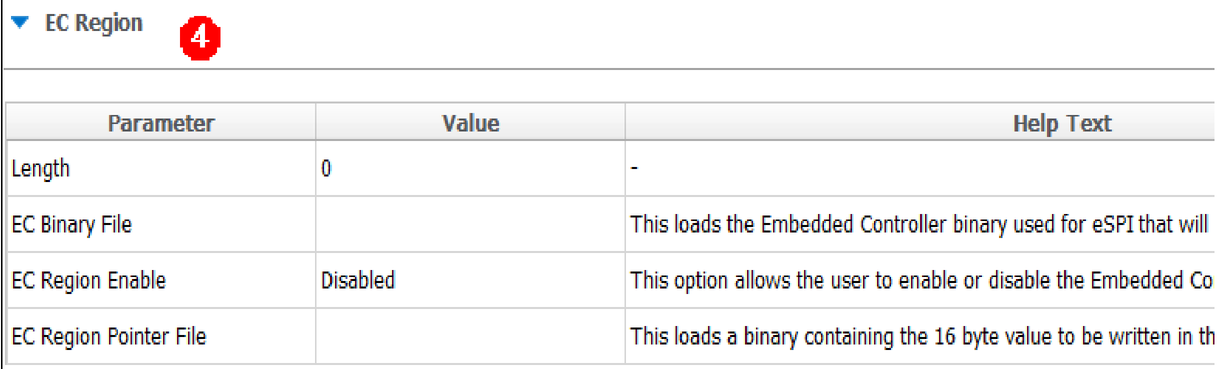
Parameter	Value	
IFWI Layout	Layout 1.6	This setting determine which IFWI layout th
Intel(R) ME Binary File		This loads the Intel(R) ME binary that will b
Major Version	0	This displays Major revision number of the
Minor Version	0	This displays Minor revision number of the
Hotfix Version	0	This displays Hot-Fix revision number of the
Build Version	0	This displays Build version number of the c
Chipset Initialization Version		This displays the current Chipset Initializati
Chipset Initialization Binary		This loads the Chipset Initialization binary t
ChipsetInit Override Version		This displays the version of the Chipset Init
PMC Binary File		This loads the PMC binary that will be merg
PMC Length	0x20000	-
Version		-

③	**IFWI Layout**	All	Layout 1.6
	Intel® CSME Binary File Navigate to your **Source Directory** (as specified in Table 2-2) and switch to the ME 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.	ICL-YN ICL-UN	meimage.bin meimage.bin
	Major Version - This displays Major revision number of the currently loaded IIntel® CSME binary.		
	Minor Version - This displays Minor revision number of the currently loaded IIntel® 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 5)

	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® ME binary. ***Note:*** When BIOS passes new Chipset Initialization settings to Intel® CSME, 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 Intel® CSME Region and programmed into the PCH. This global reset can be avoided by loading the proper chipset initialization binary in to the Intel® CSME 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 Intel® CSME 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 Intel® CSME are updated with same Chipset Initialization binary.	ICL-YN ICL-UN	Chipset.bin (Optional) 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.	ICL-YN ICL-UN	PMC.bin 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:

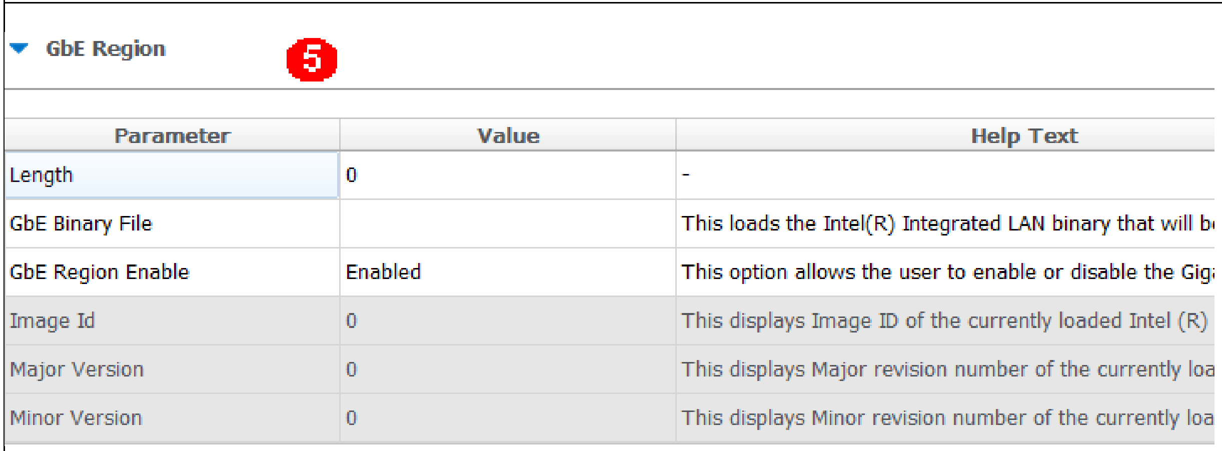


Parameter	Value	Help Text
Length	0	-
EC Binary File		This loads the Embedded Controller binary used for eSPI that will
EC Region Enable	Disabled	This option allows the user to enable or disable the Embedded Co
EC Region Pointer File		This loads a binary containing the 16 byte value to be written in th

#	Parameter	Platform	Settings
4	**EC Region**		
	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.	ICL-YN ICL-UN	EC Binary EC Binary
	EC Region Enable **Values: Enabled / Disabled** This option allows the user to enable or disable the Embedded Controller data region.	ICL-YN ICL-UN	Enabled 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	ICL-YN ICL-UN	EC Pointer Binary EC Pointer Binary

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

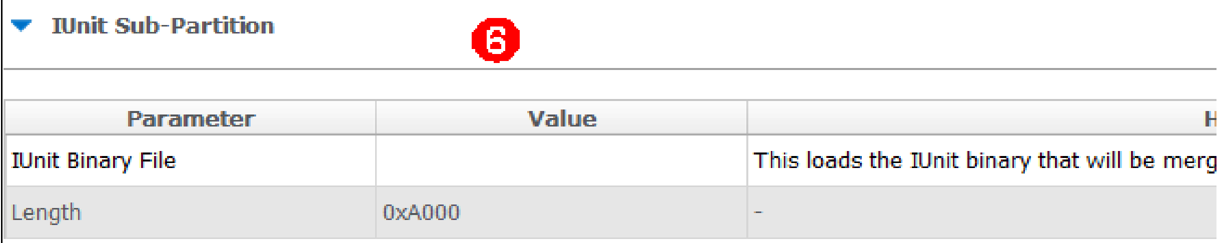
Click on Flash Layout in the left tabs menu> Gbe Region is expanded by default:



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**		
	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.	ICL-YN ICL-UN	N/A N/A
	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**:	ICL-YN ICL-UN	Disabled Disabled
	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:



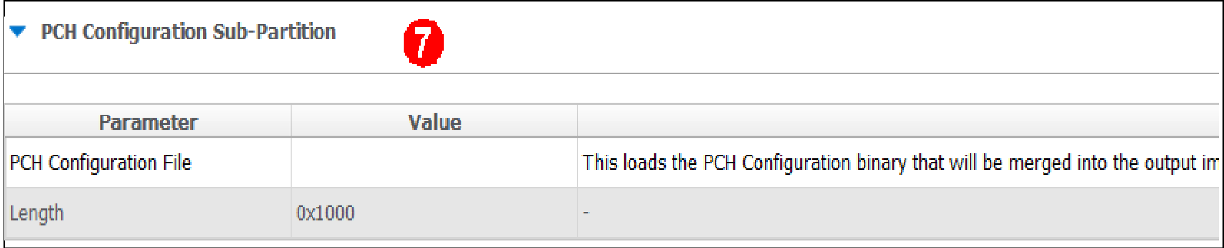
Parameter	Value	H
IUnit Binary File		This loads the IUnit binary that will be merg
Length	0xA000	-

#	Parameter	Platform	Settings

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

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.	ICL-YN ICL-UN	Iunit.bin (Optional) 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.		

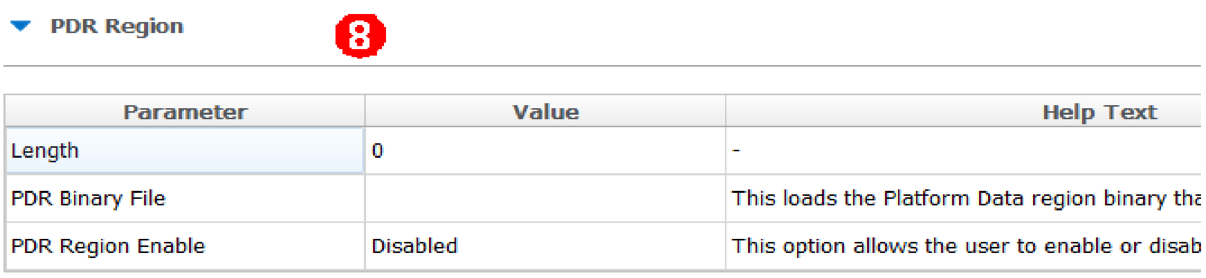
Click on Flash Layout in the left tabs menu> PCH Configuration Sub-Partion is expanded by default:



Parameter	Value	
PCH Configuration File		This loads the PCH Configuration binary that will be merged into the output im
Length	0x1000	-

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.	ICL-Y ICL-U	PCHC.bin PCHC.bin
	Length - This displays the length of the PCH 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:

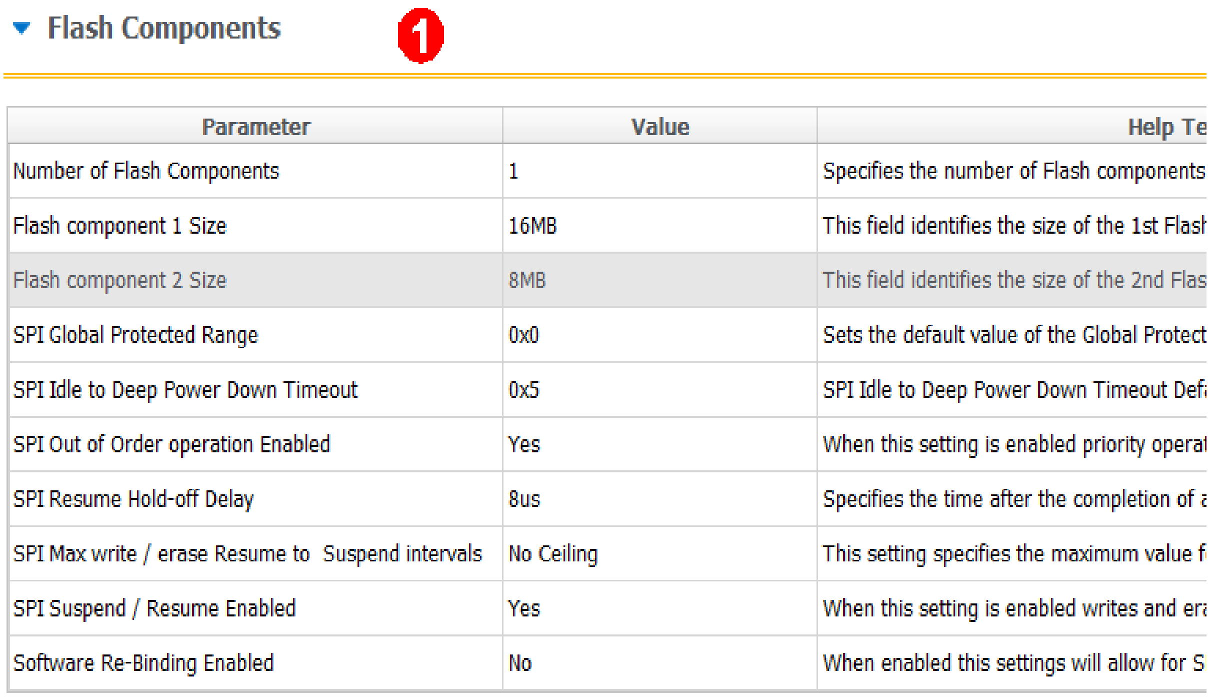


Parameter	Value	Help Text
Length	0	-
PDR Binary File		This loads the Platform Data region binary tha
PDR Region Enable	Disabled	This option allows the user to enable or disab

#	Parameter	Platform	Settings
⑧	**PDR Region -** This loads the Platform Data region binary that will be merged into the output image generated by the Intel® FIT tool.		
	PDR 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.	ICL-Y ICL-U	PDR.bin (Optional) 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.	ICL-Y ICL-U	Disabled Disabled

Table 2-4. - Flash Settings (Sheet 1 of 9)

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



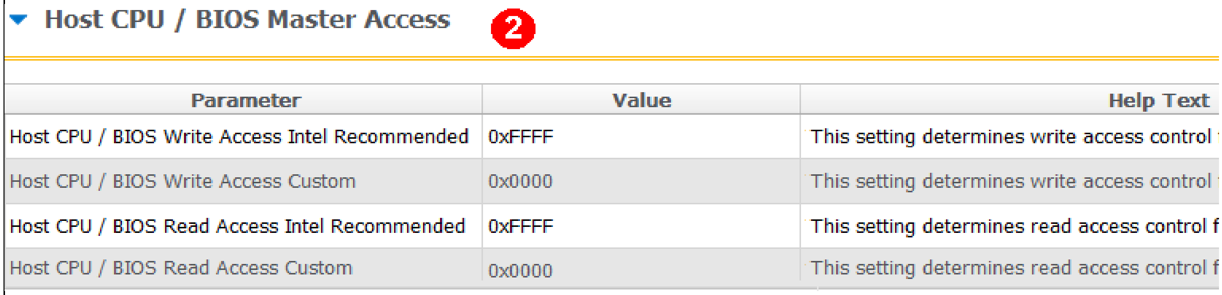
Parameter	Value	Help Te
Number of Flash Components	1	Specifies the number of Flash components
Flash component 1 Size	16MB	This field identifies the size of the 1st Flas
Flash component 2 Size	8MB	This field identifies the size of the 2nd Flas
SPI Global Protected Range	0x0	Sets the default value of the Global Protect
SPI Idle to Deep Power Down Timeout	0x5	SPI Idle to Deep Power Down Timeout Def
SPI Out of Order operation Enabled	Yes	When this setting is enabled priority operat
SPI Resume Hold-off Delay	8us	Specifies the time after the completion of
SPI Max write / erase Resume to Suspend intervals	No Ceiling	This setting specifies the maximum value f
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.	ICL-YN ICL-UN	1 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.	ICL-YN ICL-UN	16MB 16MB
	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'.	ICL-YN ICL-UN	Greyed Out Greyed Out
	SPI Global Protected Range - This sets the default value of the Global Protected Range register in the SPI Flash Controller.	ICL-YN ICL-UN	0x0 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.	ICL-YN ICL-UN	0x5 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.	ICL-YN ICL-UN	Yes 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.	ICL-YN ICL-UN	8us 8us

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

	SPI Max write / erase Resume to Suspend intervals - This setting specifies the maximum value for the write and erase Resume to Suspend intervals.	ICL-YN ICL-UN	No Ceiling 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.	ICL-YN ICL-UN	Yes Yes
	Software Re-Binding Enabled - When this setting is enabled it allow for the re-binding of the SPI part to a new PCH during manufacturing and re-manufacturing 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.	ICL-YN ICL-UN	No No

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



Host CPU / BIOS Master Access ②

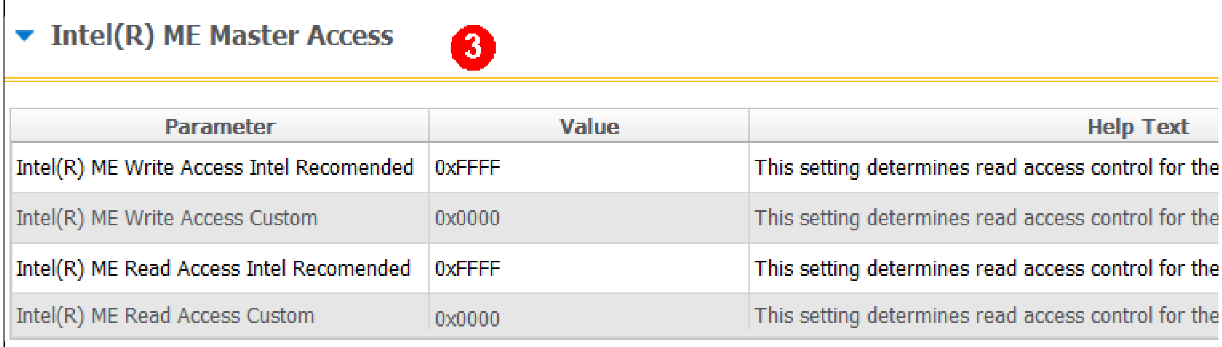
Parameter	Value	Help Text
Host CPU / BIOS Write Access Intel Recommended	0xFFFF	This setting determines write access control
Host CPU / BIOS Write Access Custom	0x0000	This setting determines write access control
Host CPU / BIOS Read Access Intel Recommended	0xFFFF	This setting determines read access control f
Host CPU / BIOS Read Access Custom	0x0000	This setting determines read access control f

#	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 Ice Lake LP SPI Programming guide further details.	ICL-YN ICL-UN	0xFFFF 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**	ICL-YN ICL-UN	Hex Input

Table 2-4. - Flash Settings (Sheet 3 of 9)

	Host CPU / BIOS Read Access **Values: 0xFFFF, 0x000F, 0x001F, 0x010F, 0x011F** - This setting determines read access control for the BIOS region. **0xFFFF** = Debug/Manufacturing **0x000F =** Production **0x001F =** Production with access to PDR (should ONLY be used if PDR region is implemented). **0x010F** = Production with access to EC **0x011F** = Production with access to EC and PDR **Custom** = User custom Host / BIOS Read Access values For further details on Region Access Control see Ice Lake LP SPI Programming guide.	ICL-YN ICL-UN	0xFFFF 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**	ICL-YN ICL-UN	Hex Input

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



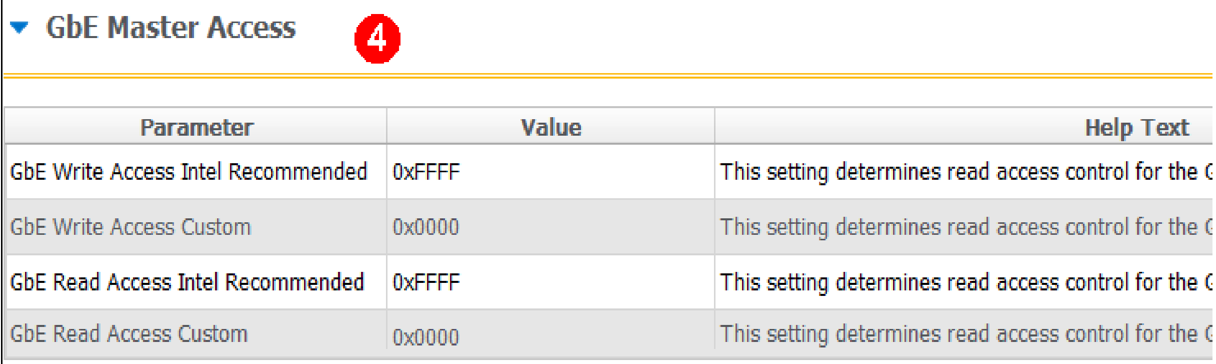
Parameter	Value	Help Text
Intel(R) ME Write Access Intel Recomended	0xFFFF	This setting determines read access control for the
Intel(R) ME Write Access Custom	0x0000	This setting determines read access control for the
Intel(R) ME Read Access Intel Recomended	0xFFFF	This setting determines read access control for the
Intel(R) ME Read Access Custom	0x0000	This setting determines read access control for the

#	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 Ice Lake LP SPI Programming guide further details.	ICL-YN ICL-UN	0xFFFF 0xFFFF
	Intel® ME Write Access Custom - This setting allows free form user customized Intel® ME Write Access regions permissions ***Note:*** This setting is grayed out unless Custom is selected under the Intel® ME Write Access Intel Recommended drop down menu. ***Warning:*** **Setting region access permission values outside of Intel recommendation could result in compromised platform security**	ICL-YN ICL-UN	Hex Input

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

	Intel® ME Read Access Intel Recommended **Values: 0xFFF, 0x00D** - 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 Ice Lake LP SPI Programming guide further details.	ICL-YN ICL-UN	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**	ICL-YN ICL-UN	Hex Input

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



GbE Master Access ④

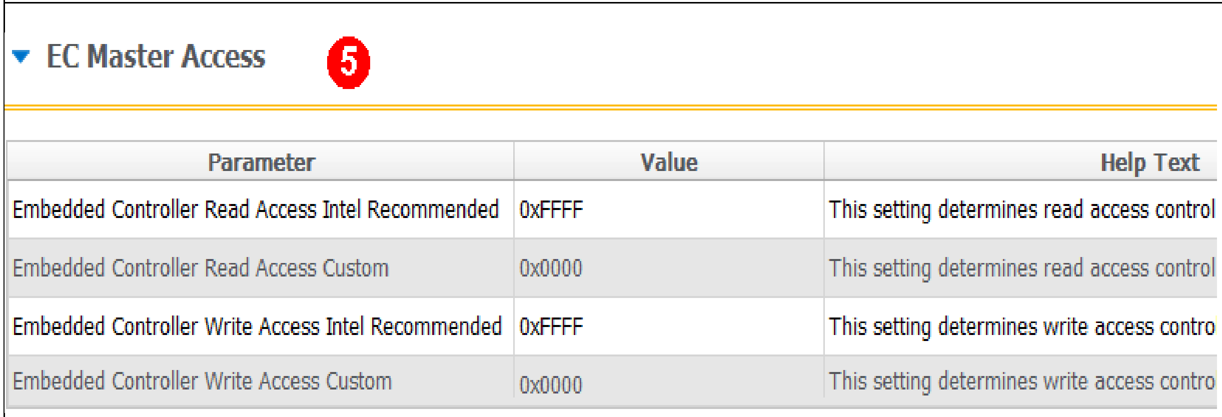
Parameter	Value	Help Text
GbE Write Access Intel Recommended	0xFFFF	This setting determines read access control for the
GbE Write Access Custom	0x0000	This setting determines read access control for the
GbE Read Access Intel Recommended	0xFFFF	This setting determines read access control for the
GbE Read Access Custom	0x0000	This setting determines read access control for the

#	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 Ice Lake LP SPI Programming guide further details.	ICL-YN ICL-UN	0xFFFF 0xFFFF
	GbE Write Access Custom - This setting allows free form user customized GbE Write Access regions permissions ***Note:*** This setting is grayed out unless Custom is selected under the GbE Write Access Intel Recommended drop down menu. ***Warning:*** **Setting region access permission values outside of Intel recommendation could result in compromised platform security**	ICL-YN ICL-UN	Hex Input

Table 2-4. - Flash Settings (Sheet 5 of 9)

	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 Ice Lake LP SPI Programming guide further details.	ICL-YN ICL-UN	0xFFFF 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**	ICL-YN ICL-UN	Hex Input

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



EC Master Access

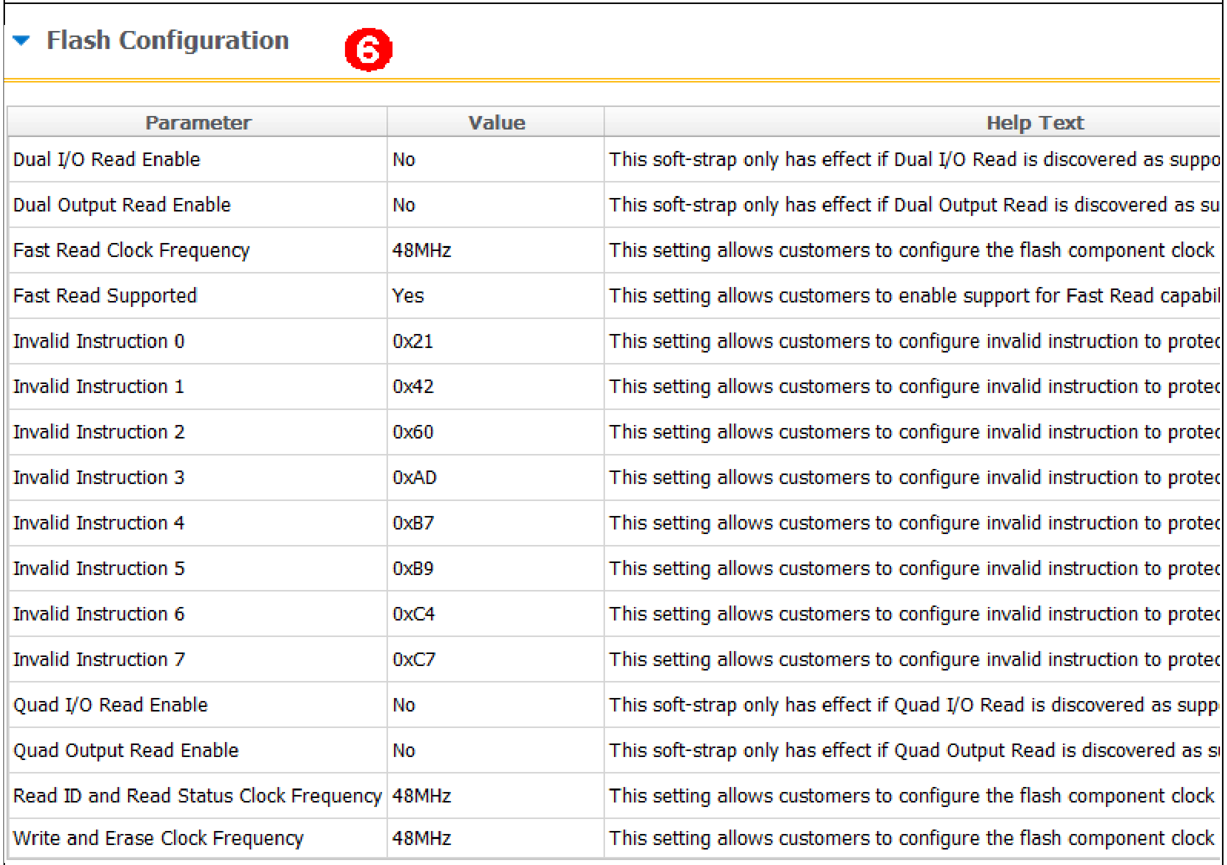
Parameter	Value	Help Text
Embedded Controller Read Access Intel Recommended	0xFFFF	This setting determines read access control
Embedded Controller Read Access Custom	0x0000	This setting determines read access control
Embedded Controller Write Access Intel Recommended	0xFFFF	This setting determines write access contro
Embedded Controller Write Access Custom	0x0000	This setting determines write access contro

#	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 Ice Lake LP SPI Programming guide further details.	ICL-YN ICL-UN	0xFFFF 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**	ICL-YN ICL-UN	Hex Input

Table 2-4. - Flash Settings (Sheet 6 of 9)

	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 Ice Lake LP SPI Programming guide further details.	ICL-YN ICL-UN	0xFFFF 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**	ICL-YN ICL-UN	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	No	This soft-strap only has effect if Dual I/O Read is discovered as suppo
Dual Output Read Enable	No	This soft-strap only has effect if Dual Output Read is discovered as su
Fast Read Clock Frequency	48MHz	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	No	This soft-strap only has effect if Quad I/O Read is discovered as supp
Quad Output Read Enable	No	This soft-strap only has effect if Quad Output Read is discovered as su
Read ID and Read Status Clock Frequency	48MHz	This setting allows customers to configure the flash component clock
Write and Erase Clock Frequency	48MHz	This setting allows customers to configure the flash component clock

#	Parameter	Platform	Settings
⑥	**Flash Configuration**		

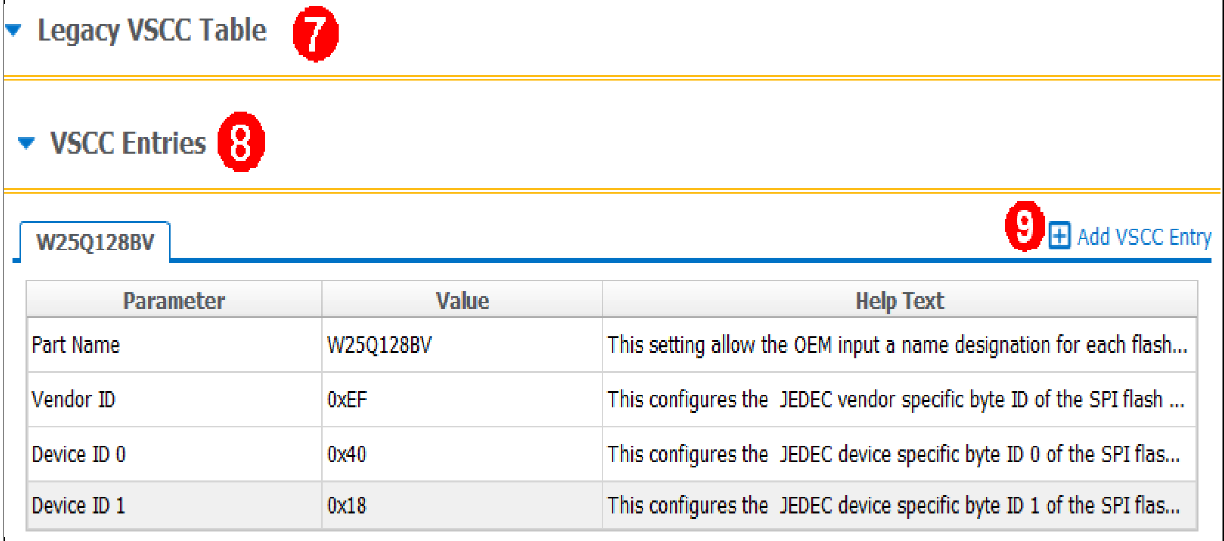
Table 2-4. - Flash Settings (Sheet 7 of 9)

	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 Ice Lake LP SPI Programming guide for further details.	ICL-YN ICL-UN	Yes 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 Ice Lake LP SPI Programming guide for further details.	ICL-YN ICL-UN	Yes Yes
	Fast Read Clock Frequency **Values: 17MHz, 30MHz, 48MHz** - This setting allows the customer to configure the flash component clock frequency setting for Fast Read. See Ice Lake LP SPI Programming guide for further details.	ICL-YN ICL-UN	48MHz 48MHz
	Fast Read Supported **Values: Yes/No** - This setting allows the customer to enable support for Fast Read capabilities for flash components. See Ice 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.	ICL-YN ICL-UN	Yes Yes
	Invalid Instruction 0 - This setting allows the customer to configure invalid instruction to protect against Chip Erase. See Ice Lake LP SPI Programming guide for further details. **Note:** This setting should be set to '0' if there are not Invalid instructions.	ICL-YN ICL-UN	0x00000021 0x00000021
	Invalid Instruction 1 - This setting allows the customer to configure invalid instruction to protect against Chip Erase. See Ice Lake LP SPI Programming guide for further details. **Note:** This setting should be set to '0' if there are not Invalid instructions.	ICL-YN ICL-UN	0x00000042 0x00000042
	Invalid Instruction 2 - This setting allows the customer to configure invalid instruction to protect against Chip Erase. See Ice Lake LP SPI Programming guide for further details. **Note:** This setting should be set to '0' if there are not Invalid instructions.	ICL-YN ICL-UN	0x00000060 0x00000060
	Invalid Instruction 3 - This setting allows the customer to configure invalid instruction to protect against Chip Erase. See Ice Lake LP SPI Programming guide for further details. **Note:** This setting should be set to '0' if there are not Invalid instructions.	ICL-YN ICL-UN	0x000000AD 0x000000AD
	Invalid Instruction 4 - This setting allows the customer to configure invalid instruction to protect against Chip Erase. See Ice Lake LP SPI Programming guide for further details. **Note:** This setting should be set to '0' if there are not Invalid instructions.	ICL-YN ICL-UN	0x000000B7 0x000000B7
	Invalid Instruction 5 - This setting allows the customer to configure invalid instruction to protect against Chip Erase. See Ice Lake LP SPI Programming guide for further details. **Note:** This setting should be set to '0' if there are not Invalid instructions.	ICL-YN ICL-UN	0x000000B9 0x000000B9
	Invalid Instruction 6 - This setting allows the customer to configure invalid instruction to protect against Chip Erase. See Ice Lake LP SPI Programming guide for further details. **Note:** This setting should be set to '0' if there are not Invalid instructions.	ICL-YN ICL-UN	0x000000C4 0x000000C4
	Invalid Instruction 7 - This setting allows the customer to configure invalid instruction to protect against Chip Erase. See Ice Lake LP SPI Programming guide for further details. **Note:** This setting should be set to '0' if there are not Invalid instructions.	ICL-YN ICL-UN	0x000000C7 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 Ice Lake LP SPI Programming guide for further details.	ICL-YN ICL-UN	Yes 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 Ice Lake LP SPI Programming guide for further details.	ICL-YN ICL-UN	Yes Yes
	Read ID and Read Status clock frequency **Values: 17MHz, 30MHz, 48MHz** - This setting allows the customer to configure the flash component clock frequency setting for Read ID and Read Status. See Ice Lake LP SPI Programming guide for further details.	ICL-YN ICL-UN	48MHz 48MHz

Table 2-4. - Flash Settings (Sheet 8 of 9)

	Write and Erase clock frequency **Values: 17MHz, 30MHz, 48MHz** - This setting allows the customer to configure the flash component clock frequency setting for Write and Erase. See Ice Lake / Ice Lake LP SPI Programming guide for further details.	ICL-YN ICL-UN	48MHz 48MHz

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

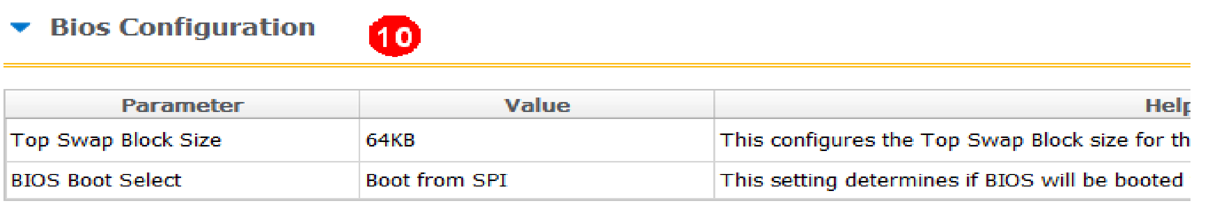


Parameter	Value	Help Text
Part Name	W25Q128BV	This setting allow the OEM input a name designation for each flash...
Vendor ID	0xEF	This configures the JEDEC vendor specific byte ID of the SPI flash ...
Device ID 0	0x40	This configures the JEDEC device specific byte ID 0 of the SPI flas...
Device ID 1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

#	Parameter	Platform	Settings
⑦	**Flash Settings - VSCC Table** **VSCC Entries**		
	W25Q128BV		
⑧	**VSCC Entry**	ICL-YN ICL-UN	
	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.	ICL-YN ICL-UN	Winbond Winbond
	Vendor ID - This configures the JEDEC vendor specific byte ID of the SPI flash component. See Ice Lake LP SPI Programming guide for further details.	ICL-YN ICL-UN	0xEF 0xEF
	Device ID 0 - This configures the JEDEC device specific byte ID 0 of the SPI flash component. See Ice Lake LP SPI Programming guide for further details.	ICL-YN ICL-UN	0x40 0x40
	Device ID 1 - This configures the JEDEC device specific byte ID 1 of the SPI flash component. See Ice Lake LP SPI Programming guide for further details.	ICL-YN ICL-UN	0x18 0x18
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 9)

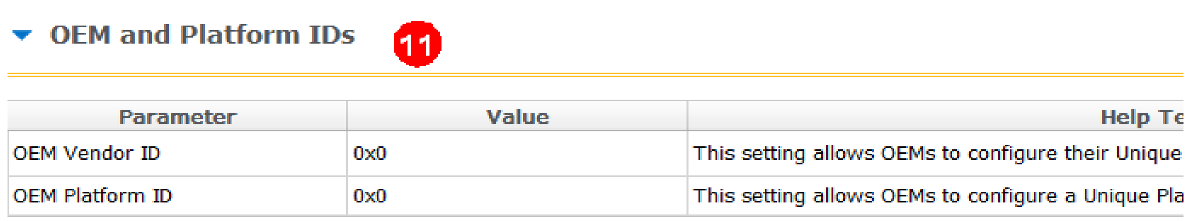


Bios Configuration 10

Parameter	Value	Hel
Top Swap Block Size	64KB	This configures the Top Swap Block size for th
BIOS Boot Select	Boot from SPI	This setting determines if BIOS will be booted

#	Parameter	Platform	
10	**BIOS Configuration** **Top Swap Block Size** **Values: 64KB, 128KB, 256KB, 512KB, 1MB** - This configures the Top Swap Block size for the platform. For further details see Ice Lake LP Platform Controller Hub EDS.	ICL-YN ICL-UN	128KB 128KB
	BIOS Boot Select **Values: Boot from SPI / Boot from LPC** This setting determines if BIOS will be booted from LPC or SPI.	ICL-YN ICL-UN	Boot from SPI Boot from SPI

Click on Flash Settings in the left tabs menu > OEM and Platform IDs

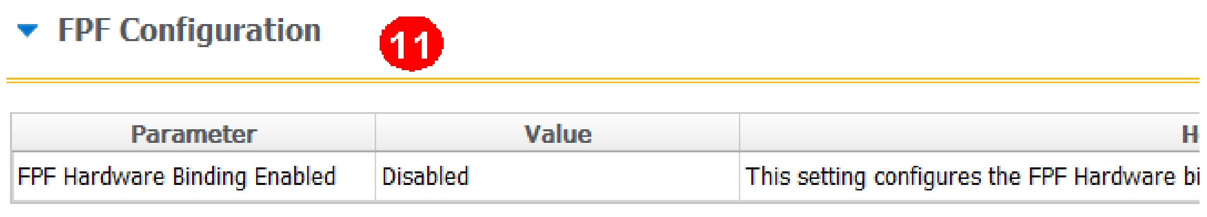


OEM and Platform IDs 11

Parameter	Value	Help Te
OEM Vendor ID	0x0	This setting allows OEMs to configure their Unique
OEM Platform ID	0x0	This setting allows OEMs to configure a Unique Pla

#	Parameter	Platform	
11	**OEM Vendor ID -** This is a free form 32bit field that allows the OEM to configure their unique Vendor identifier in the firmware image.	ICL-YN ICL-UN	
	OEM Platform ID - This is a free form 32bit field that allows the OEM to configure their unique platform identifier in the firmware image.	ICL-YN ICL-UN	

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



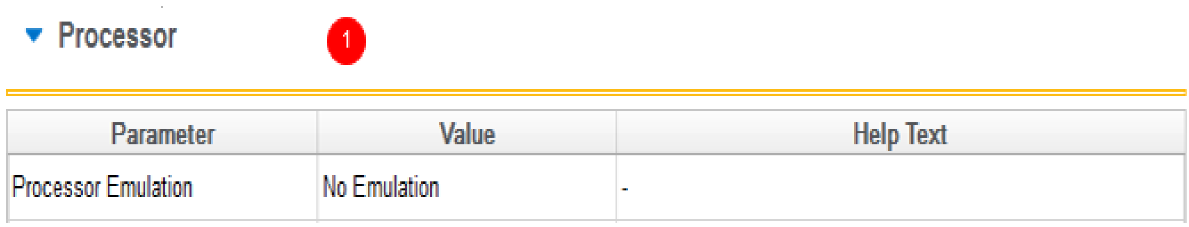
FPF Configuration 11

Parameter	Value	H
FPF Hardware Binding Enabled	Disabled	This setting configures the FPF Hardware bi

#	Parameter	Platform	
12	**FPF Configuration** ***Note:***		
	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.	ICL-YN ICL-UN	Disabled Disabled

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

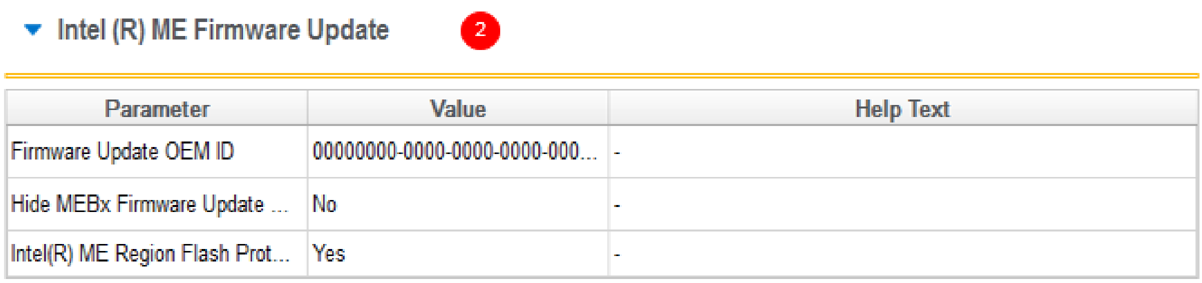
Click on Intel® ME Kernel in the left tabs menu> Processor is expanded by default:



Parameter	Value	Help Text
Processor Emulation	No Emulation	-

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

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

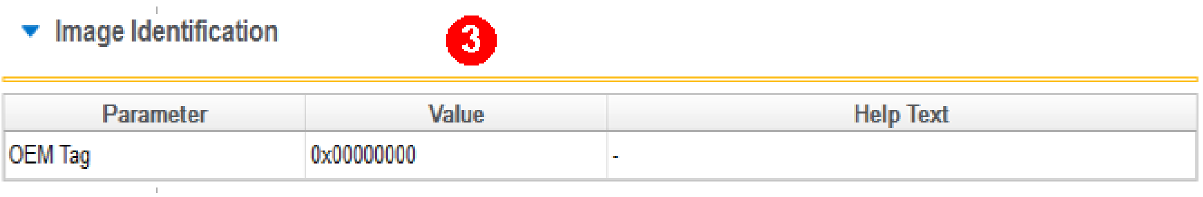


Parameter	Value	Help Text
Firmware Update OEM ID	00000000-0000-0000-0000-000...	-
Hide MEBx Firmware Update ...	No	-
Intel(R) ME Region Flash Prot...	Yes	-

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

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

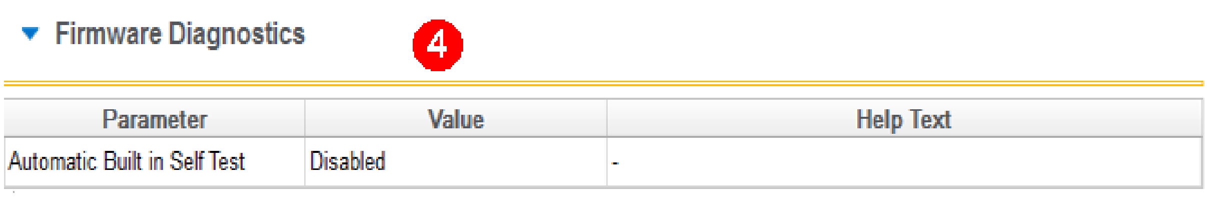
Table 2-5. - Intel® ME Kernel (Sheet 2 of 4)



Parameter	Value	Help Text
OEM Tag	0x00000000	-

#	Parameter	Platform	Settings
③	**Intel® ME Kernel - 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.	ICL-YN ICL-UN	0x00000000 0x00000000

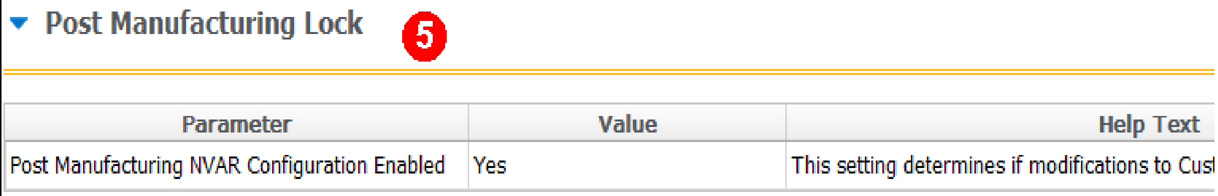
Click on Intel® ME Kernel in the left tabs menu> Firmware Diagnostics is expanded by default:



Parameter	Value	Help Text
Automatic Built in Self Test	Disabled	-

#	Parameter	Platform	Settings
④	**Intel® ME Kernel - 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.	ICL-YN ICL-UN	Disabled Disabled

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

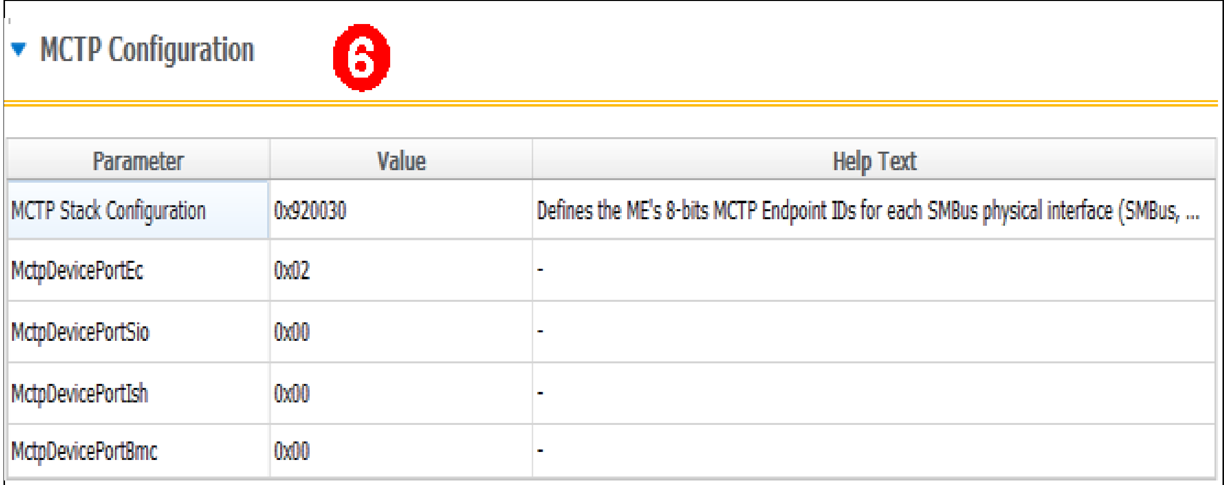


Parameter	Value	Help Text
Post Manufacturing NVAR Configuration Enabled	Yes	This setting determines if modifications to Cust

#	Parameter	Platform	Settings
⑤	**Post Manufacturing Lock**		
	Post Manufacturing NVAR Configuration Enabled - This setting determines if modifications to Customer configurable NVARs is to be allowed after close of manufacturing.	ICL-YN ICL-UN	Yes Yes

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

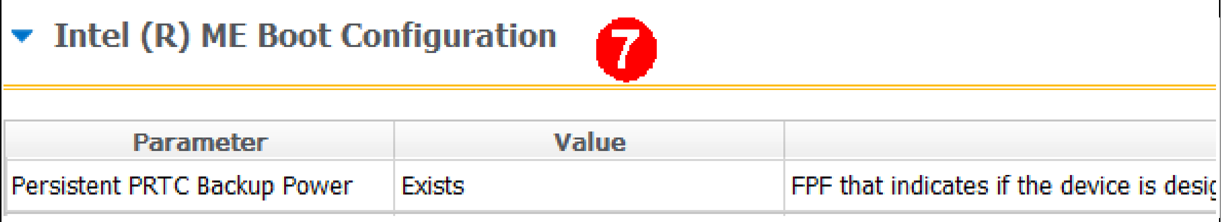
Table 2-5. - Intel® ME Kernel (Sheet 3 of 4)



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	**Intel® ME Kernel - 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.	ICL-YN ICL-UN	0x920030 0x920030
	MctpDevicePortEc	ICL-YN ICL-UN	0x02 0x02
	MctpDevicePortSio	ICL-YN ICL-UN	0x00 0x00
	MctpDevicePortIsh	ICL-YN ICL-UN	0x00 0x00
	MctpDevicePortBmc	ICL-YN ICL-UN	0x00 0x00

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

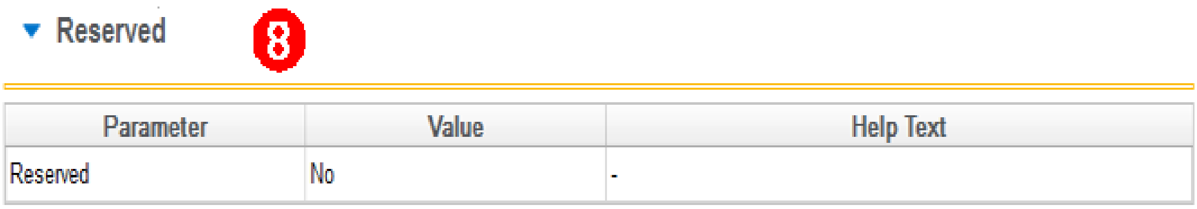


Parameter	Value	
Persistent PRTC Backup Power	Exists	FPF that indicates if the device is desig

#	Parameter	Platform	Settings
⑦	**Intel® ME Boot Configuration**		
	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	ICL-YN ICL-UN	Exists Exists

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

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



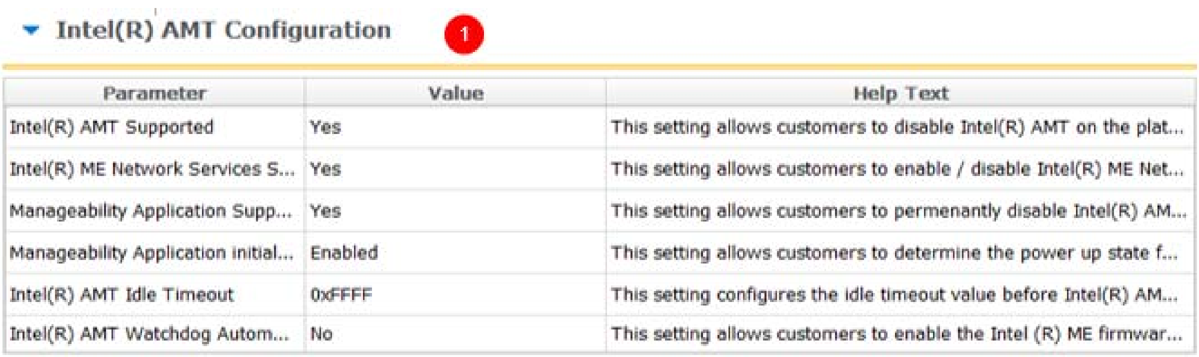
▼ Reserved ⑧

Parameter	Value	Help Text
Reserved	No	-

⑧	**Intel® ME Kernel - Reserved**		
	Reserved **Values: Yes/No**	ICL-YN ICL-UN	No No

Table 2-6. - Intel® AMT (Sheet 1 of 7)

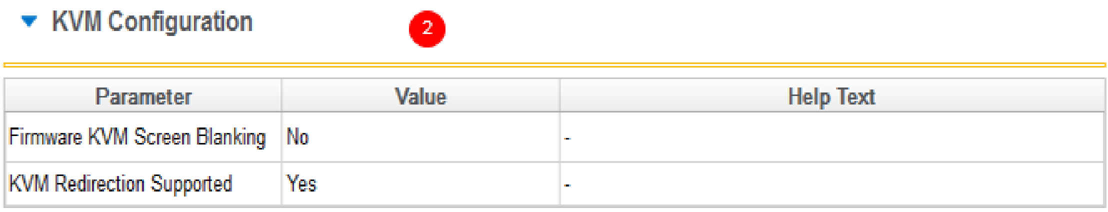
Click on Intel® AMT in the left tabs menu> Intel® AMT is expanded by default:



Parameter	Value	Help Text
Intel(R) AMT Supported	Yes	This setting allows customers to disable Intel(R) AMT on the plat...
Intel(R) ME Network Services S...	Yes	This setting allows customers to enable / disable Intel(R) ME Net...
Manageability Application Supp...	Yes	This setting allows customers to permenantly disable Intel(R) AM...
Manageability Application initial...	Enabled	This setting allows customers to determine the power up state f...
Intel(R) AMT Idle Timeout	0xFFFF	This setting configures the idle timeout value before Intel(R) AM...
Intel(R) AMT Watchdog Autom...	No	This setting allows customers to enable the Intel (R) ME firmwar...

#	Parameter	Platform	Settings
①	**Intel® AMT - 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.	ICL-YN ICL-UN	No No No
	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.	ICL-YN ICL-UN	No No No
	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.	ICL-YN ICL-UN	No No No
	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.	ICL-YN ICL-UN	Disabled Disabled Disabled
	Intel® AMT Idle Timeout **Values: 0xFFFF** - This setting configures the idle timeout value before Intel® AMT enters into an off state.	ICL-YN ICL-UN	0xFFFF 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.	ICL-YN ICL-UN	No No No

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

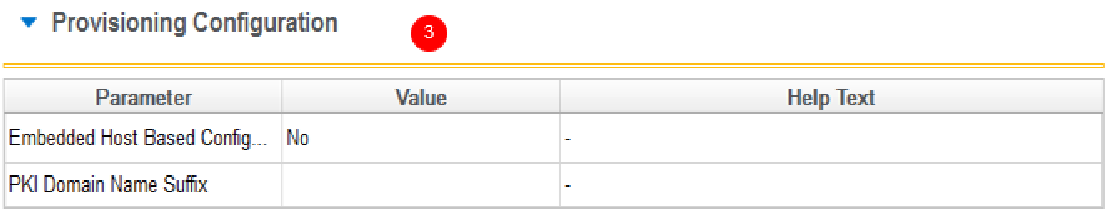


Parameter	Value	Help Text
Firmware KVM Screen Blanking	No	-
KVM Redirection Supported	Yes	-

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

#	Parameter	Platform	Settings
②	**Intel® AMT - 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.	ICL-YN ICL-UN	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.	ICL-YN ICL-UN	No No

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

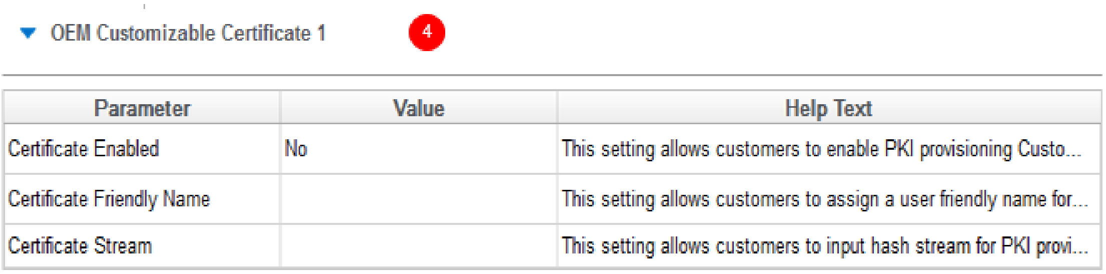


Provisioning Configuration

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

#	Parameter	Platform	
③	**Intel® AMT - Provisioning Configuration**		
	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.	ICL-YN ICL-UN	No 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.	ICL-YN ICL-UN	- -

Click on Intel® AMT in the left tabs menu> OEM Customizable Certificate 1 is expanded by default:



OEM Customizable Certificate 1

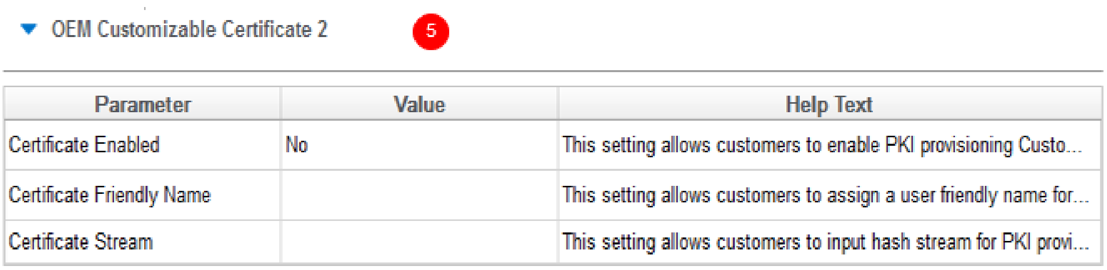
Parameter	Value	Help Text
Certificate Enabled	No	This setting allows customers to enable PKI provisioning Custo...
Certificate Friendly Name		This setting allows customers to assign a user friendly name for...
Certificate Stream		This setting allows customers to input hash stream for PKI provi...

#	Parameter	Platform	Settings
④	**Intel® AMT - OEM Customizable Certificate 1**		
	Certificate Enabled **Values: Yes/No** - This setting allows customers to enable PKI provisioning Custom Certificate 1.	ICL-YN ICL-UN	No No

Table 2-6. - Intel® AMT (Sheet 3 of 7)

	Certificate Friendly Name - This setting allows customers to assign a user friendly name for PKI provisioning Custom Certificate 1. Maximum of 32 characters.	ICL-YN ICL-UN	- -
	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.	ICL-YN ICL-UN	- -

Click on Intel® AMT in the left tabs menu> OEM Customizable Certificate 2 is expanded by default:

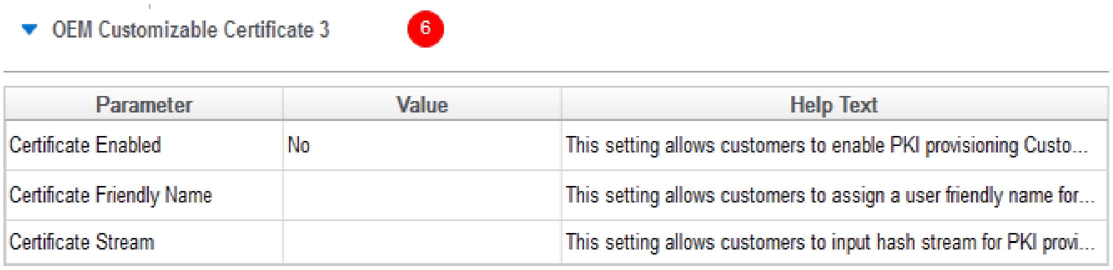


OEM Customizable Certificate 2 5

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	**Intel® AMT - OEM Customizable Certificate 2**		
	Certificate Enabled **Values: Yes / No** - This setting allows customers to enable PKI provisioning Custom Certificate 2.	ICL-YN ICL-UN	No No
	Certificate Friendly Name - This setting allows customers to assign a user friendly name for PKI provisioning Custom Certificate 2. Maximum of 32 characters.	ICL-YN ICL-UN	- -
	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.	ICL-YN ICL-UN	- -

Click on Intel® AMT in the left tabs menu> OEM Customizable Certificate 3 is expanded by default:



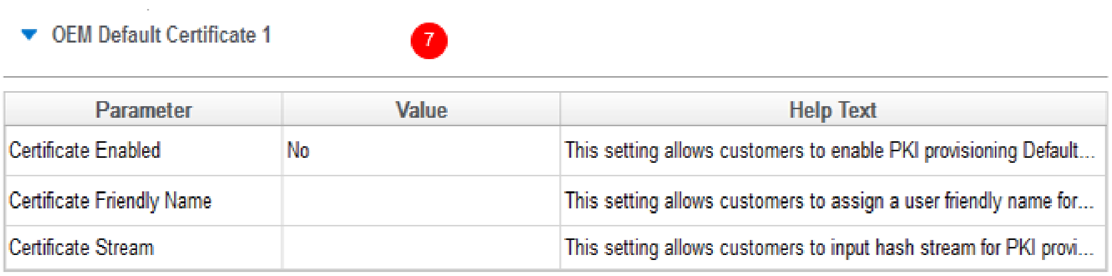
OEM Customizable Certificate 3 6

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
6	**Intel® AMT - OEM Customizable Certificate 3**		
	Certificate Enabled **Values: Yes / No** - This setting allows customers to enable PKI provisioning Custom Certificate 3.	ICL-YN ICL-UN	No No
	Certificate Friendly Name - This setting allows customers to assign a user friendly name for PKI provisioning Custom Certificate 3. Maximum 32 characters.	ICL-YN ICL-UN	- -
	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.	ICL-YN ICL-UN	- -

Table 2-6. - Intel® AMT (Sheet 4 of 7)

Click on Intel® AMT in the left tabs menu> OEM Default Certificate 1 is expanded by default:

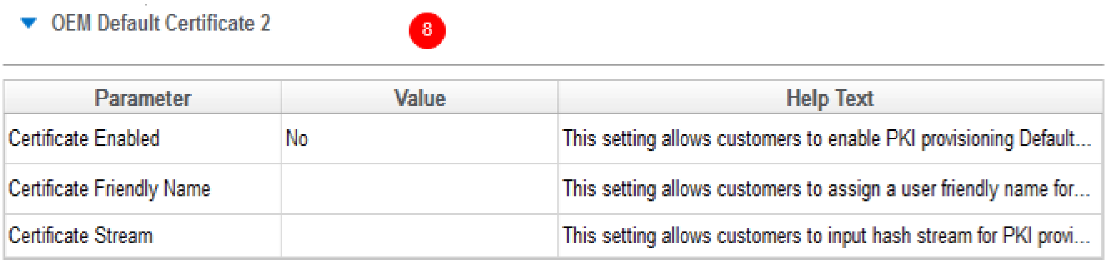


▼ OEM Default Certificate 1 ⑦

Parameter	Value	Help Text
Certificate Enabled	No	This setting allows customers to enable PKI provisioning Default...
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
❼	**Intel® AMT - OEM Default Certificate 1**		
	Certificate Enabled **Values: Yes/No** - This setting allows customers to enable PKI provisioning Default certificate 1.	ICL-YN ICL-UN	No No
	Certificate Friendly Name - This setting allows customers to assign a user friendly name for PKI provisioning Default Certificate 1. Maximum 32 characters.	ICL-YN ICL-UN	- -
	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.	ICL-YN ICL-UN	- -

Click on Intel® AMT in the left tabs menu> OEM Default Certificate 2 is expanded by default:



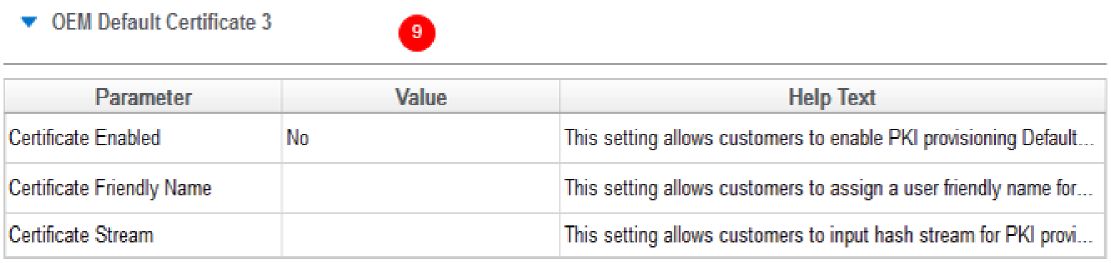
▼ OEM Default Certificate 2 ⑧

Parameter	Value	Help Text
Certificate Enabled	No	This setting allows customers to enable PKI provisioning Default...
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
❽	**Intel® AMT - OEM Default Certificate 2**		
	Certificate Enabled **Values: Yes/No** - This setting allows customers to enable PKI provisioning Default certificate 2.	ICL-YN ICL-UN	No No
	Certificate Friendly Name - This setting allows customers to assign a user friendly name for PKI provisioning Default Certificate 2. Maximum 32 characters.	ICL-YN ICL-UN	- -
	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.	ICL-YN ICL-UN	- -

Click on Intel® AMT in the left tabs menu> OEM Default Certificate 3 is expanded by default:

Table 2-6. - Intel® AMT (Sheet 5 of 7)

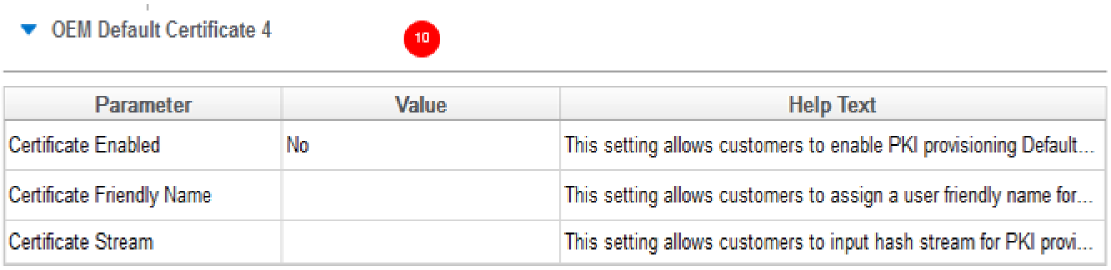


OEM Default Certificate 3

Parameter	Value	Help Text
Certificate Enabled	No	This setting allows customers to enable PKI provisioning Default...
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
9	**Intel® AMT - OEM Default Certificate 3**		
	Certificate Enabled **Values: Yes/No** - This setting allows customers to enable PKI provisioning Default certificate 3.	ICL-YN ICL-UN	No No
	Certificate Friendly Name - This setting allows customers to assign a user friendly name for PKI provisioning Default Certificate 3. Maximum 32 characters.	ICL-YN ICL-UN	- -
	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.	ICL-YN ICL-UN	- -

Click on Intel® AMT in the left tabs menu> OEM Default Certificate 4 is expanded by default:



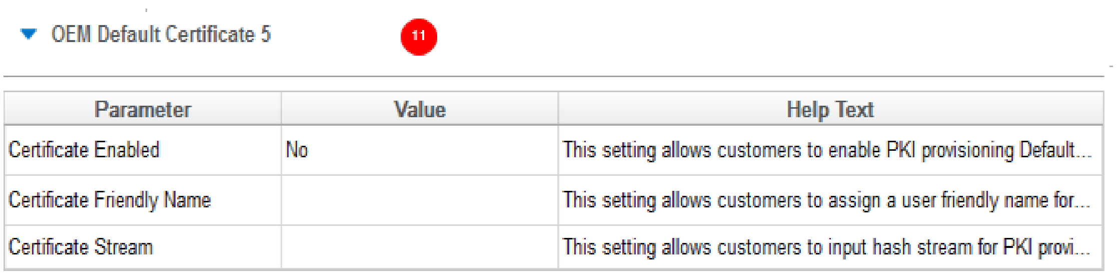
OEM Default Certificate 4

Parameter	Value	Help Text
Certificate Enabled	No	This setting allows customers to enable PKI provisioning Default...
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
10	**Intel® AMT - OEM Default Certificate 4**		
	Certificate Enabled **Values: Yes/No** - This setting allows customers to enable PKI provisioning Default certificate 4.	ICL-YN ICL-UN	No No
	Certificate Friendly Name - This setting allows customers to assign a user friendly name for PKI provisioning Default Certificate 4.	ICL-YN ICL-UN	- -
	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.	ICL-YN ICL-UN	- -

Click on Intel® AMT in the left tabs menu> OEM Default Certificate 5 is expanded by default:

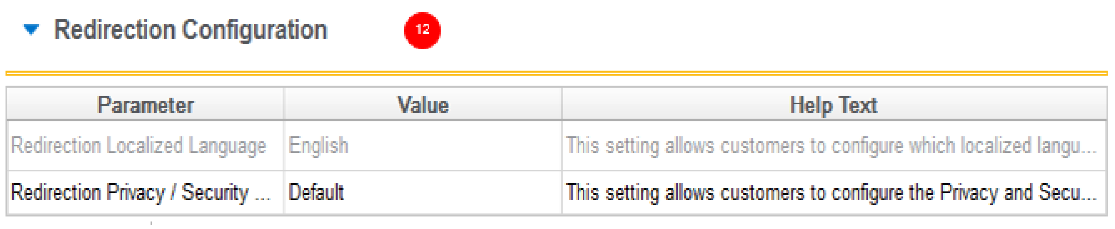
Table 2-6. - Intel® AMT (Sheet 6 of 7)



Parameter	Value	Help Text
Certificate Enabled	No	This setting allows customers to enable PKI provisioning Default...
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
11	**Intel® AMT - OEM Default Certificate 5**		
	Certificate Enabled **Values: Yes/No** - This setting allows customers to enable PKI provisioning Default certificate 5.	ICL-YN ICL-UN	No No
	Certificate Friendly Name - This setting allows customers to assign a user friendly name for PKI provisioning Default Certificate 5.	ICL-YN ICL-UN	- -
	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.	ICL-YN ICL-UN	- -

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

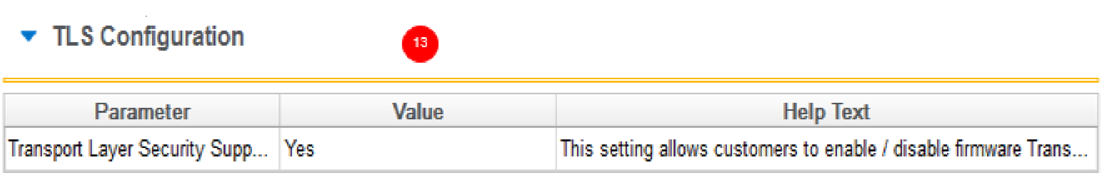


Parameter	Value	Help Text
Redirection Localized Language	English	This setting allows customers to configure which localized langu...
Redirection Privacy / Security ...	Default	This setting allows customers to configure the Privacy and Secu...

#	Parameter	Platform	Settings
12	**Intel® AMT - 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).	ICL-YN ICL-UN	English 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.	ICL-YN ICL-UN	Default Default

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

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



TLS Configuration

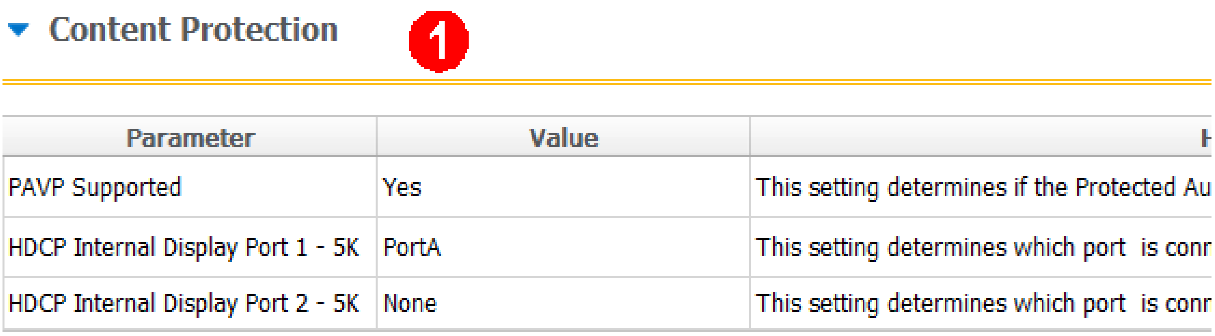
13

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

#	Parameter	Platform	Settings
13	**Intel® AMT - TLS Configuration**		
	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.	ICL-YN ICL-UN	No No

Table 2-7. - Platform Protection (Sheet 1 of 9)

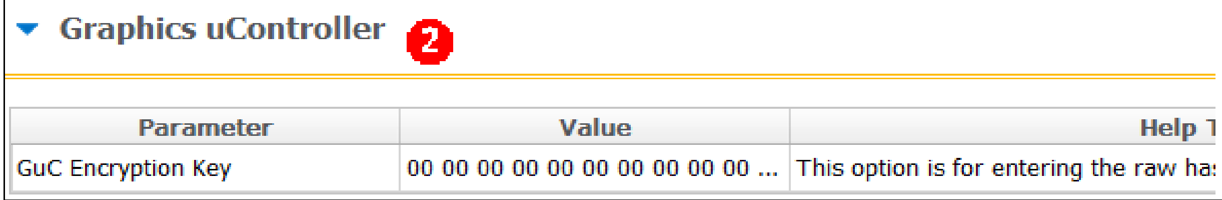
Click on Platform Protection in the left tabs menu> Content Protection is expanded by default:



Parameter	Value	H
PAVP Supported	Yes	This setting determines if the Protected Au
HDCP Internal Display Port 1 - 5K	PortA	This setting determines which port is conr
HDCP Internal Display Port 2 - 5K	None	This setting determines which port is conr

#	Parameter	Platform	Settings
①	**Platform Protection - Content Protection**		
	PAVP Supported **Values: Yes/No** This setting determines if the Protected Audio Video Path (PAVP) feature will be permanently disabled in the FW image.	ICL-YN ICL-UN	Yes 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.	ICL-YN ICL-UN	None None
	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.	ICL-YN ICL-UN	None None

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

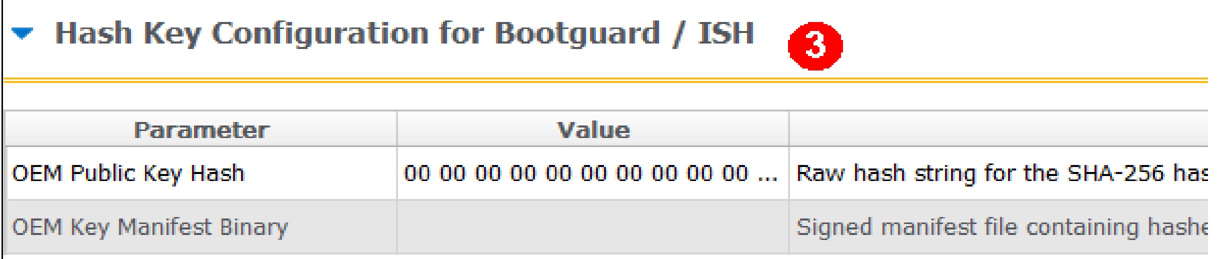


Parameter	Value	Help 1
GuC Encryption Key	00 00 00 00 00 00 00 00 00 00 ...	This option is for entering the raw ha:

#	Parameter	Platform	Settings
②	**Platform Protection - Graphics UController**		
	GuC Encryption Key **Values:** This option is for entering the raw hash 256 bit string or certificate file for the Graphics uController.	ICL-YN ICL-UN	0x00000000 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 9)

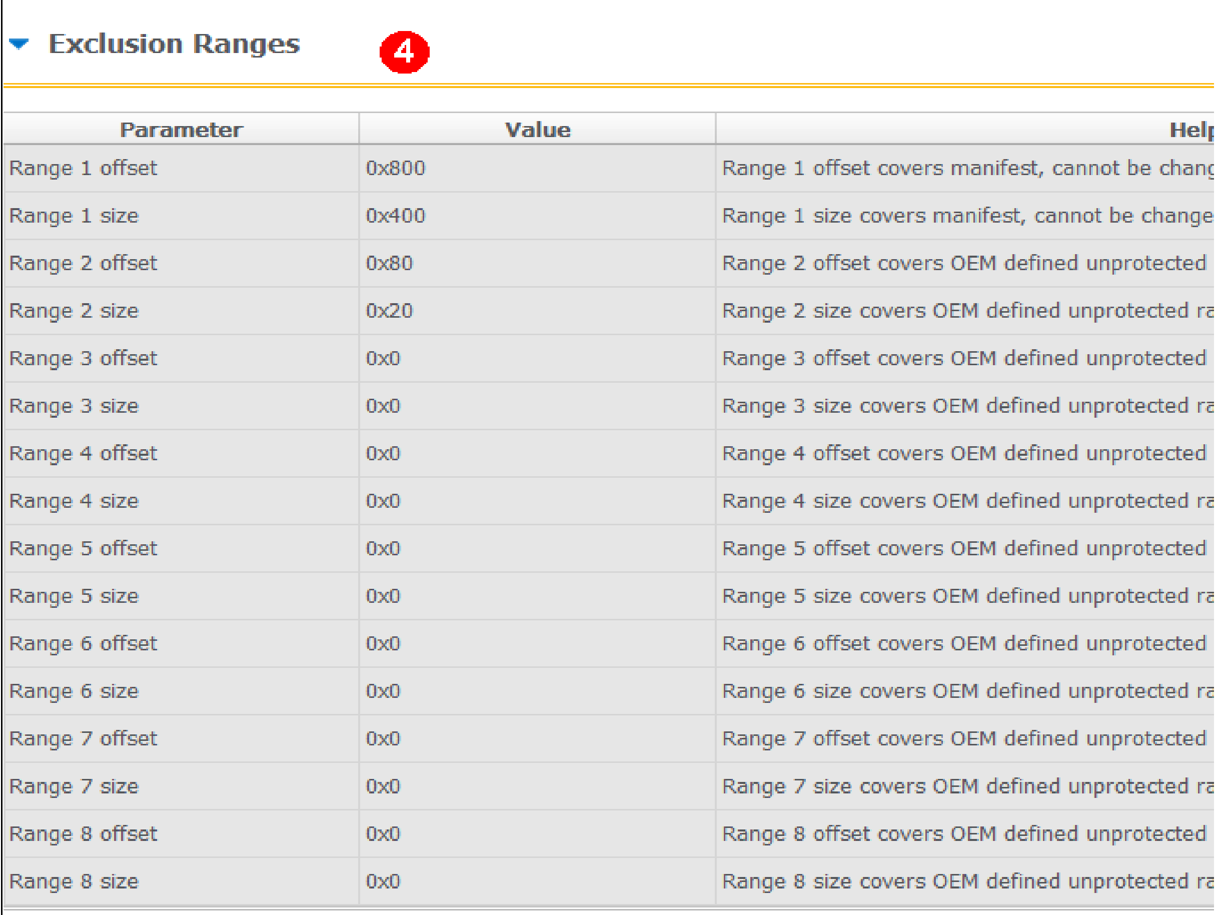


Hash Key Configuration for Bootguard / ISH ③

Parameter	Value	
OEM Public Key Hash	00 00 00 00 00 00 00 00 00 00 ...	Raw hash string for the SHA-256 has
OEM Key Manifest Binary		Signed manifest file containing hashe

#	Parameter	Platform	
③	**Platform Protection - 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 256-bit field represents the SHA-256 hash of the OEM public key corresponding to the private key used to sign the BIOS-SM or ISH image. Please see Appendix F for further details.	ICL-YN ICL-UN	0x00000000 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).	ICL-YN ICL-UN	
Click on Platform Protection in the left tabs menu> Exclusion Ranges is expanded by default:			

Table 2-7. - Platform Protection (Sheet 3 of 9)



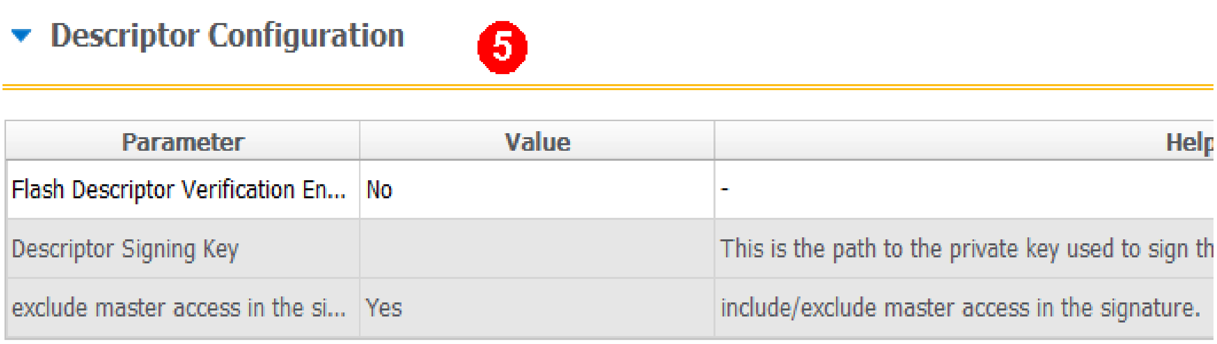
Parameter	Value	Hel
Range 1 offset	0x800	Range 1 offset covers manifest, cannot be chang
Range 1 size	0x400	Range 1 size covers manifest, cannot be change
Range 2 offset	0x80	Range 2 offset covers OEM defined unprotected
Range 2 size	0x20	Range 2 size covers OEM defined unprotected ra
Range 3 offset	0x0	Range 3 offset covers OEM defined unprotected
Range 3 size	0x0	Range 3 size covers OEM defined unprotected ra
Range 4 offset	0x0	Range 4 offset covers OEM defined unprotected
Range 4 size	0x0	Range 4 size covers OEM defined unprotected ra
Range 5 offset	0x0	Range 5 offset covers OEM defined unprotected
Range 5 size	0x0	Range 5 size covers OEM defined unprotected ra
Range 6 offset	0x0	Range 6 offset covers OEM defined unprotected
Range 6 size	0x0	Range 6 size covers OEM defined unprotected ra
Range 7 offset	0x0	Range 7 offset covers OEM defined unprotected
Range 7 size	0x0	Range 7 size covers OEM defined unprotected ra
Range 8 offset	0x0	Range 8 offset covers OEM defined unprotected
Range 8 size	0x0	Range 8 size covers OEM defined unprotected ra

#	Parameter	Platform	
4	**Platform Protection - Exclusion Ranges** ***Note:*** The values for Range 1 and 2 are automatically populated and not user configurable. The remaining Range 3-8 values are configurable by the OEM to allow for unprotected ranges not covered by the descriptor signature these settings are only configurable when Flash Descriptor Verification Enabled setting is configured to "Yes".		
	Range 1 offset	ICL-YN ICL-UN	0x800 0x800
	Range 1 size	ICL-YN ICL-UN	0x400 0x400
	Range 2 offset	ICL-YN ICL-UN	0x80 0x80
	Range 2 size	ICL-YN ICL-UN	0x20 0x20
	Range 3 offset **Values:** This offset covers Range 3 OEM defined unprotected range start	ICL-YN ICL-UN	0x0 0x0
	Range 3 size **Values:** This offset covers Range 3 OEM defined unprotected range length	ICL-YN ICL-UN	0x0 0x0
	Range 4 offset **Values:** This offset covers Range 4 OEM defined unprotected range start	ICL-YN ICL-UN	0x0 0x0

Table 2-7. - Platform Protection (Sheet 4 of 9)

	Range 4 size **Values:** This offset covers Range 4OEM defined unprotected range length	ICL-YN ICL-UN	0x0 0x0
	Range 5 offset **Values:** This offset covers Range 5 OEM defined unprotected range start	ICL-YN ICL-UN	0x0 0x0
	Range 5 size **Values:** This offset covers Range 5 OEM defined unprotected range length	ICL-YN ICL-UN	0x0 0x0
	Range 6 offset **Values:** This offset covers Range 6 OEM defined unprotected range start	ICL-YN ICL-UN	0x0 0x0
	Range 6 size **Values:** This offset covers Range 6 OEM defined unprotected range length	ICL-YN ICL-UN	0x0 0x0
	Range 7 offset **Values:** This offset covers Range 7 OEM defined unprotected range start	ICL-YN ICL-UN	0x0 0x0
	Range 7 size **Values:** This offset covers Range 7 OEM defined unprotected range length	ICL-YN ICL-UN	0x0 0x0
	Range 8 offset **Values:** This offset covers Range 8 OEM defined unprotected range start	ICL-YN ICL-UN	0x0 0x0
	Range 8 size **Values:** This offset covers Range 8 OEM defined unprotected range length	ICL-YN ICL-UN	0x0 0x0

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



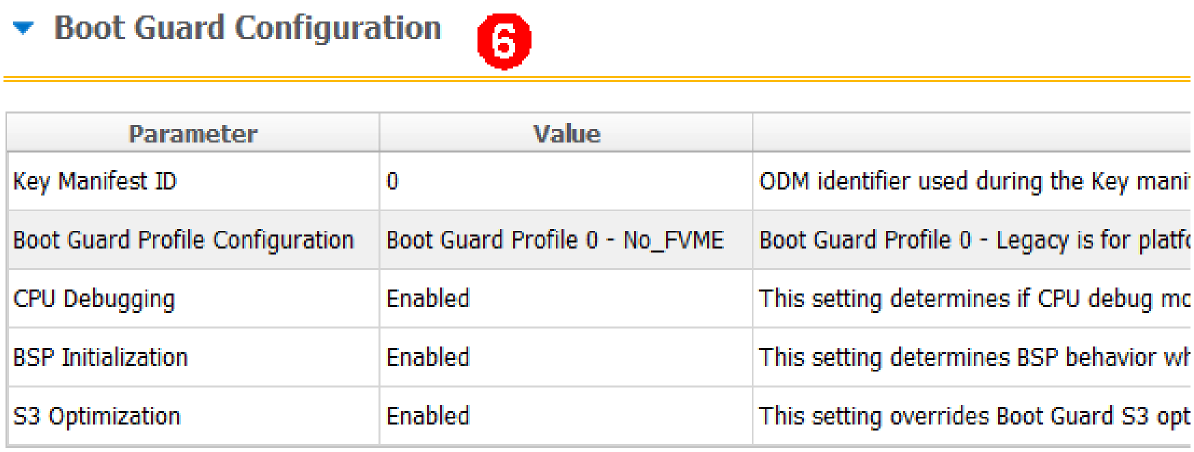
Descriptor Configuration

Parameter	Value	Help
Flash Descriptor Verification En...	No	-
Descriptor Signing Key		This is the path to the private key used to sign th
exclude master access in the si...	Yes	include/exclude master access in the signature.

#	Parameter	Platform	
⑤	**Platform Protection - Descriptor Configuration**		
	Flash Descriptor Verification Enabled **Value: Yes/No** This settings enables / disables Flash Descriptor verification.	ICL-YN ICL-UN	No No
	Descriptor Signing Key This is the path to the private key used to sign the Descriptor, while public key hash of it is included in the OEM hash manifest. This setting is only configurable when Flash Descriptor Verification is enabled (See Platform Integrity/Fdv Enabled).	ICL-YN ICL-UN	None None
	exclude master access in the signature **Value: Yes/No** This setting excludes the region master access values in the descriptor signature.	ICL-YN ICL-UN	Yes Yes

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

Table 2-7. - Platform Protection (Sheet 5 of 9)

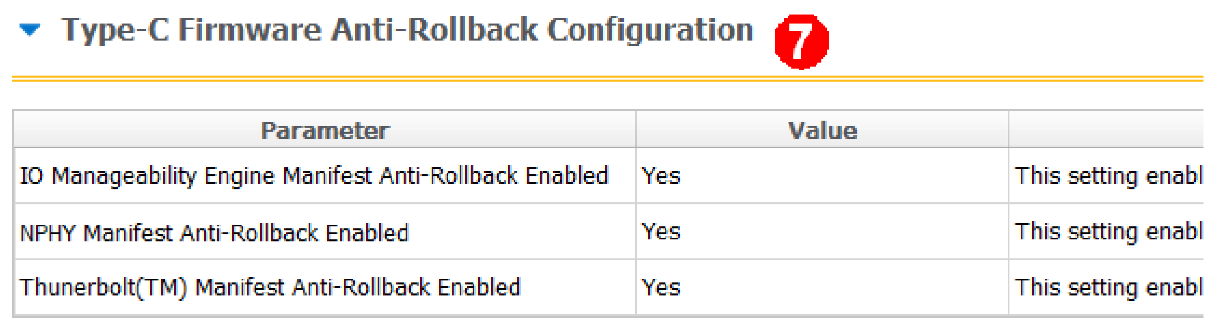


Boot Guard Configuration ⑥

Parameter	Value	
Key Manifest ID	0	ODM identifier used during the Key mani
Boot Guard Profile Configuration	Boot Guard Profile 0 - No_FVME	Boot Guard Profile 0 - Legacy is for platf
CPU Debugging	Enabled	This setting determines if CPU debug mc
BSP Initialization	Enabled	This setting determines BSP behavior wh
S3 Optimization	Enabled	This setting overrides Boot Guard S3 opt

#	Parameter	Platform	Settings
⑥	**Platform Protection - 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.	ICL-YN ICL-UN	0x0 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.	ICL-YN ICL-UN	Boot Guard Profile 0 - No_FVME 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.	ICL-YN ICL-UN	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).	ICL-YN ICL-UN	Enabled Enabled
	S3 Optimization **Values: Enabled / Disabled** This setting overrides Boot Guard S3 optimization. ***Note:*** Used for testing only.	ICL-YN ICL-UN	Enabled Enabled
Click on Platform Protection in the left tabs menu> Type-C Firmware Anti-Rollback Configuration is expanded by default:			

Table 2-7. - Platform Protection (Sheet 6 of 9)

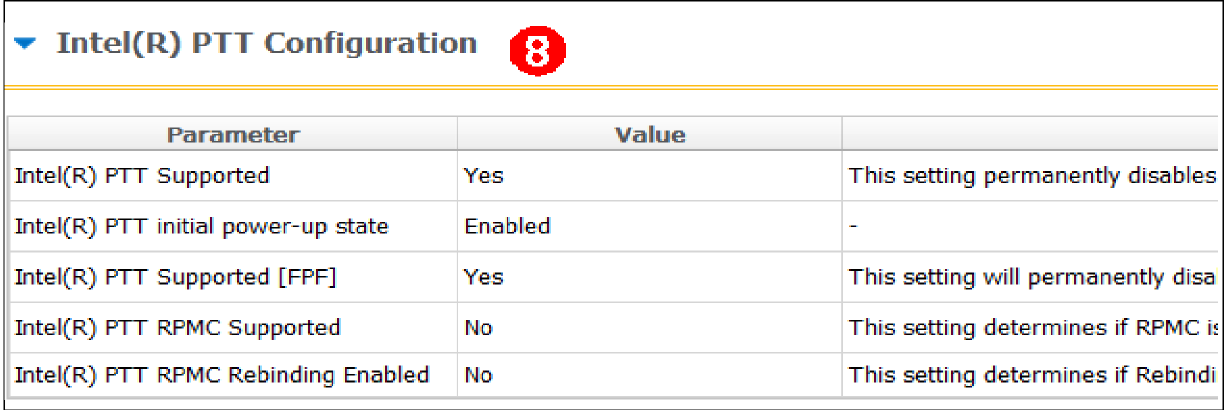


Type-C Firmware Anti-Rollback Configuration

Parameter	Value	
IO Manageability Engine Manifest Anti-Rollback Enabled	Yes	This setting enabl
NPHY Manifest Anti-Rollback Enabled	Yes	This setting enabl
Thunerbolt(TM) Manifest Anti-Rollback Enabled	Yes	This setting enabl

#	Parameter	Platform	Settings
⑦	**Platform Protection - Boot Guard Configuration**		
	IO Manageability Engine Manifest Anti-Rollback Enabled **Values: Yes / No** - This setting enables Anti-Rollback for the Type-C Subsystem IO Manageability Engine binary.	ICL-YN ICL-UN	Yes Yes
	NPHY Manifest Anti-Rollback Enabled **Values: Yes / No** - This setting enables Anti-Rollback for the Type-C Subsystem NPHY binary.	ICL-YN ICL-UN	Yes Yes
	Thunderbolt$^{(TM)}$ Manifest Anti-Rollback Enabled **Values: Yes / No** - This setting enables Anti-Rollback for the Type-C Subsystem Thunderbolt$^{(TM)}$ binary.	ICL-YN ICL-UN	Yes Yes

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



Intel(R) PTT Configuration

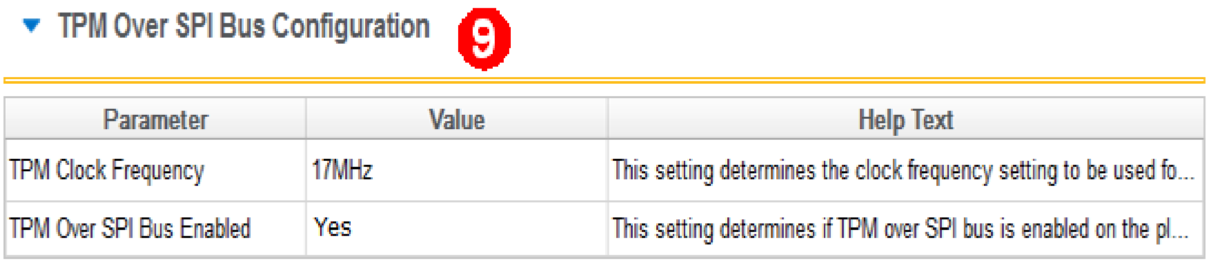
Parameter	Value	
Intel(R) PTT Supported	Yes	This setting permanently disables
Intel(R) PTT initial power-up state	Enabled	-
Intel(R) PTT Supported [FPF]	Yes	This setting will permanently disa
Intel(R) PTT RPMC Supported	No	This setting determines if RPMC is
Intel(R) PTT RPMC Rebinding Enabled	No	This setting determines if Rebindi

#	Parameter	Platform	Settings
⑧	**Platform Protection - Intel® PTT Configuration**		
	Intel® PTT initial power-up state **Values: Enabled / Disabled** - This setting determines if Intel® PTT is enabled on platform power-up.	ICL-YN ICL-UN	Enabled Enabled
	Intel® PTT Supported **Values: Yes / No** - This setting permanently disables Intel® PTT in the firmware image.	ICL-YN ICL-UN	Yes Yes

Table 2-7. - Platform Protection (Sheet 7 of 9)

	Intel® PTT Supported [FPF] **Values: Yes/No** - This setting will permanently disable Intel® PTT through platform FPFs. **Caution:** Using this option will permanently disable Intel® PTT on the platform hardware.	ICL-YN ICL-UN	Yes Yes
	Intel® PTT RPMC Supported **Values: Yes/No** - This setting determines if RPMC is enabled for Intel® PTT. ***Note:*** The SPI parts being used need to support RPMC in order to use this feature.	ICL-YN ICL-UN	No No
	Intel® PTT RPMC Rebinding Enabled **Values: Yes/No** - This setting determines if Rebinding of RPMC enabled SPI parts is supported.	ICL-YN ICL-UN	No No

Click on Platform Protection in the left tabs menu> TPM Over SPI Bus Configuration is expanded by default:

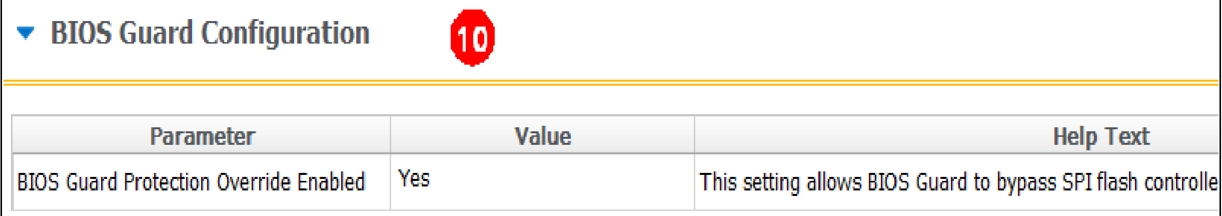


TPM Over SPI Bus Configuration

Parameter	Value	Help Text
TPM Clock Frequency	17MHz	This setting determines the clock frequency setting to be used fo...
TPM Over SPI Bus Enabled	Yes	This setting determines if TPM over SPI bus is enabled on the pl...

#	Parameter	Platform	Settings
⑨	**Platform Protection - TPM Over SPI Bus Configuration**		
	TPM Clock Frequency **Values: 17MHz, 30MHz, 48MHz** - This setting determines the clock frequency setting to be used for the TPM over SPI bus.	ICL-YN ICL-UN	17MHz 17MHz
	TPM Over SPI Bus Enabled **Values: Yes/No** - This setting determines if TPM over SPI bus is enabled on the platform.	ICL-YN ICL-UN	Yes Yes

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



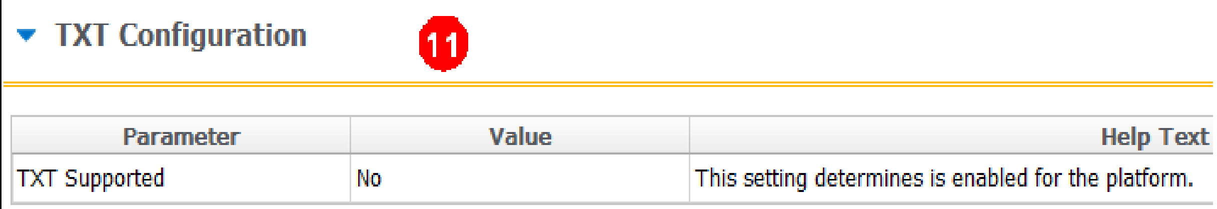
BIOS Guard Configuration

Parameter	Value	Help Text
BIOS Guard Protection Override Enabled	Yes	This setting allows BIOS Guard to bypass SPI flash controlle

#	Parameter	Platform	Settings
⑩	**Platform Protection - BIOS Guard Configuration**		
	BIOS Guard Protection Override Enabled This setting allows BIOS Guard to bypass SPI flash controller protections (i.e. Protected Range Registers and Top Swap).	ICL-YN ICL-UN	Yes Yes

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

Table 2-7. - Platform Protection (Sheet 8 of 9)

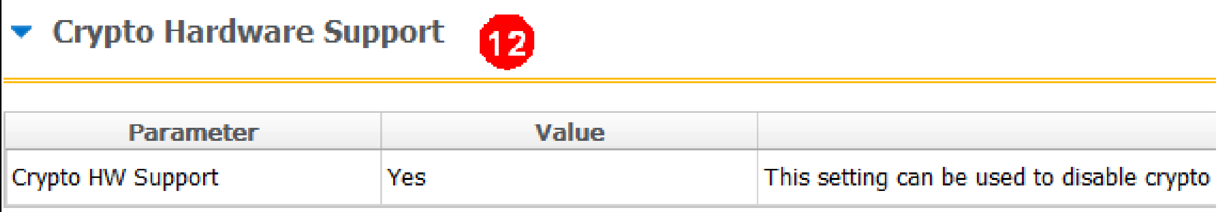


TXT Configuration

Parameter	Value	Help Text
TXT Supported	No	This setting determines is enabled for the platform.

#	Parameter	Platform	Settings
11	**Platform Protection - TXT Configuration**		
	TXT Supported **Values: Yes / No** - This setting determines if enabled for the platform.	ICL-YN ICL-UN	No No

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

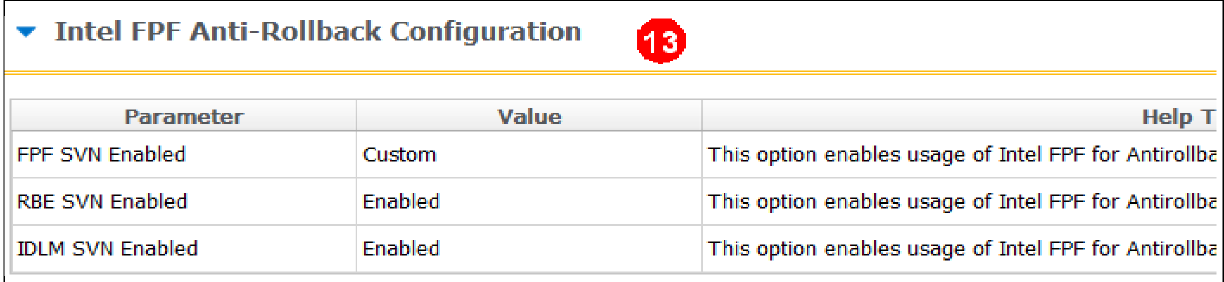


Crypto Hardware Support

Parameter	Value	
Crypto HW Support	Yes	This setting can be used to disable crypto

#	Parameter	Platform	Settings
12	**Platform Protection - Crypto HW Support**		
	Crypto HW Support **Values: Yes / No** - This setting can be used to disable crypto functionality. This setting disables all crypto related features.	ICL-YN ICL-UN	Yes Yes

Click on Platform Protection in the left tabs menu> Intel FPF Anti-Rollback Configuration is expanded by default:



Intel FPF Anti-Rollback Configuration

Parameter	Value	Help T
FPF SVN Enabled	Custom	This option enables usage of Intel FPF for Antirollba
RBE SVN Enabled	Enabled	This option enables usage of Intel FPF for Antirollba
IDLM SVN Enabled	Enabled	This option enables usage of Intel FPF for Antirollba

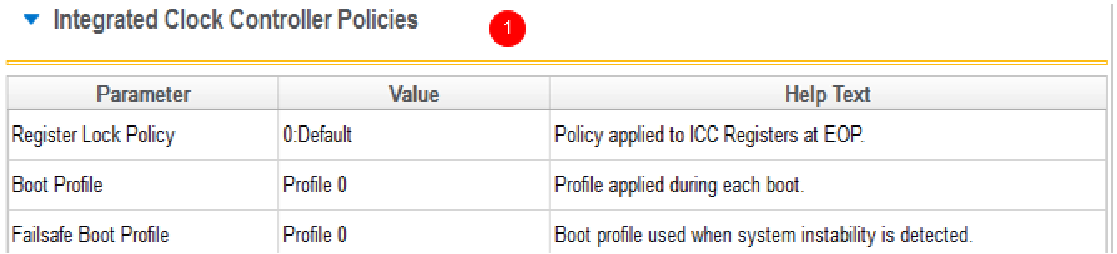
#	Parameter	Platform	Settings
13	**Intel FPF Anti-Rollback Configuration**		
	FPF SVN Enabled **Values: Enabled / Disabled** - This option enables usage of Intel FPF of the Anti-Rollback mechanism for all firmware components.	ICL-Y ICL-U	Custom Custom

Table 2-7. - Platform Protection (Sheet 9 of 9)

	RBE SVN Enabled **Values: Enabled/Disabled** - This option enables usage of Intel FPF of the Anti-Rollback mechanism for the RBE SVN firmware component.	ICL-Y ICL-U	Enabled Enabled

Table 2-8. - Integrated Clock Controller (Sheet 1 of 7)

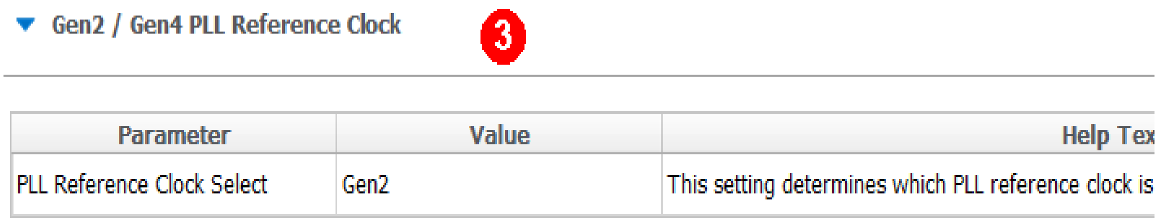
Click on Integrated Clock Controller in the left tabs menu> Integrated Clock Controller Policies are expanded by default:



Parameter	Value	Help Text
Register Lock Policy	0:Default	Policy applied to ICC Registers at EOP.
Boot Profile	Profile 0	Profile applied during each boot.
Failsafe Boot Profile	Profile 0	Boot profile used when system instability is detected.

#	Parameter	Platform	Settings
❶	**Integrated Clock Controller - Integrated Clock Controller Policies**		
	Register Lock Policy ***Note:*** Leave settings at Intel® FIT default values	ICL-YN ICL-UN	0: Default 0: Default
	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.	ICL-YN ICL-UN	Profile 0 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.	ICL-YN ICL-UN	Profile 0 Profile 0

Click on Integrated Clock Controller in the left tabs menu> Gen2 / Gen4 PLL Reference Clock is expanded by default:

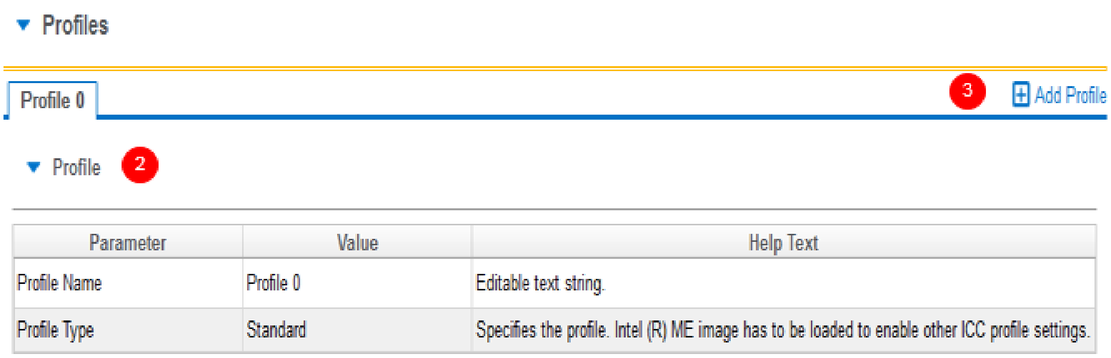


Parameter	Value	Help Tex
PLL Reference Clock Select	Gen2	This setting determines which PLL reference clock is

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

#	Parameter	Platform	Settings
③	**Gen2 / Gen4 PLL Reference Clock** **Values: Gen2/Gen4** This setting determines which PLL reference clock is being used to supply the 100MHz to the CPU and PCIe root ports and their corresponding PCIe devices. Note: Gen4 can only be enabled if the CPU supports it.	ICL-YN ICL-UN	Gen2 Gen2

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



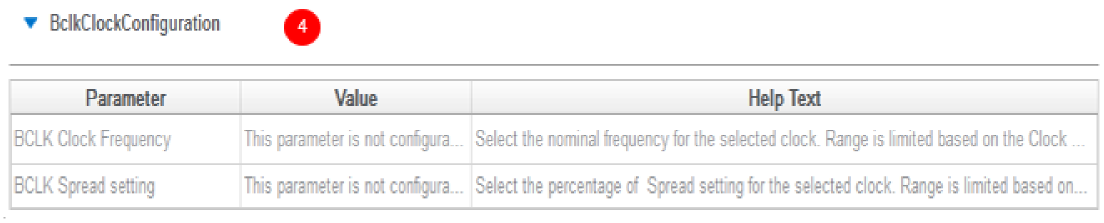
Parameter	Value	Help Text
Profile Name	Profile 0	Editable text string.
Profile Type	Standard	Specifies the profile. Intel (R) ME image has to be loaded to enable other ICC profile settings.

#	Parameter	Platform	Settings
②	**Integrated Clock Controller - Profiles - Profile 0** **Note:** Intel® ME image has to be loaded to enable other ICC profile settings. **For ICL/CFL-Y/U,** 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. **For** ICL/CFL-Y/U**,** Intel® FIT provides 5 pre-defined ICC profiles to choose from. •**Standard** •**Adaptive** **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**"	ICL-YN ICL-UN	Standard 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.	ICL-YN ICL-UN	Profile 0 Profile 0
	Profile Type Available ICC profiles for ICL/CFL-Y/U are Standard, Adaptive. This parameter indicates which pre- defined profile selected for each profile#. Double click on value column of this parameter to choose from available options.	ICL-YN ICL-UN	Standard Standard

Table 2-8. - Integrated Clock Controller (Sheet 3 of 7)

	+ 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**.**	ICL-YN ICL-UN	

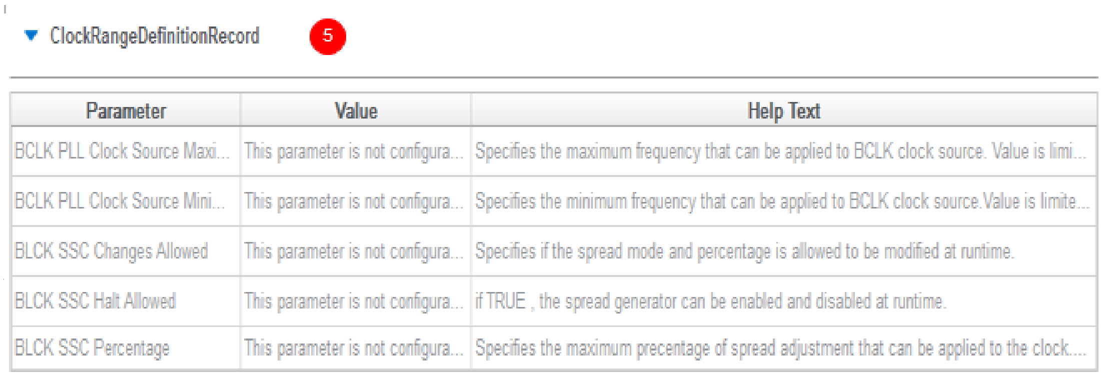
Click on Integrated Clock Controller in the left tabs menu> Profiles >Profile> Bclk Clock Configuration is expanded by default:



Parameter	Value	Help Text
BCLK Clock Frequency	This parameter is not configura...	Select the nominal frequency for the selected clock. Range is limited based on the Clock ...
BCLK Spread setting	This parameter is not configura...	Select the percentage of Spread setting for the selected clock. Range is limited based on...

#	Parameter	Platform	Settings
④	**Integrated Clock Controller - Profiles - Profile BclkClockConfiguration**		
	BCLK Clock Frequency - This parameter allows user to select the nominal frequency for the selected clock. Range is limited based on the Clock Range Definition record and HW SKU. **Standard Setting Profile Type -** Option is grayed out. **Adaptive Setting Profile Type -** Option is able to be edited.	ICL-YN ICL-UN	
	BCLK Spread Setting - This parameter allows user to select the percentage of Spread setting for the selected clock. Range is limited based on the Clock Range Definition record and HW SKU. **BCLK Clock Frequency** **Standard Setting Profile Type -** Option is grayed out. **Adaptive Setting Profile Type -** Option is able to be edited.	ICL-YN ICL-UN	

Click on Integrated Clock Controller in the left tabs menu> Profiles >Profile> Clock Range Definition Record is expanded by default:



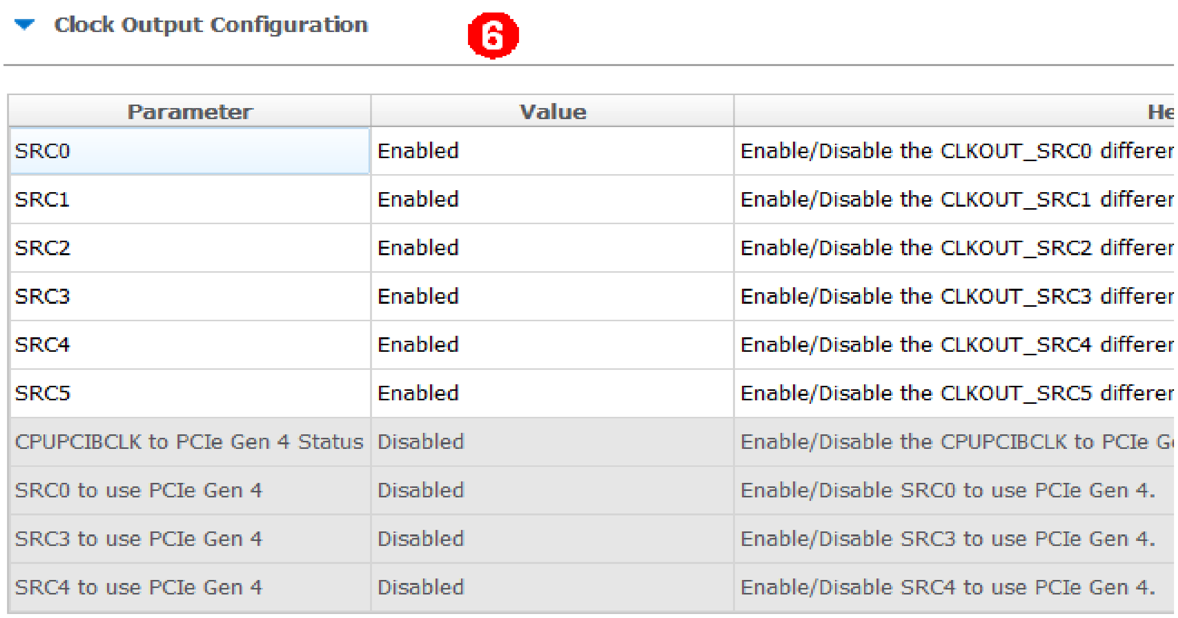
Parameter	Value	Help Text
BCLK PLL Clock Source Maxi...	This parameter is not configura...	Specifies the maximum frequency that can be applied to BCLK clock source. Value is limi...
BCLK PLL Clock Source Mini...	This parameter is not configura...	Specifies the minimum frequency that can be applied to BCLK clock source.Value is limite...
BLCK SSC Changes Allowed	This parameter is not configura...	Specifies if the spread mode and percentage is allowed to be modified at runtime.
BLCK SSC Halt Allowed	This parameter is not configura...	if TRUE , the spread generator can be enabled and disabled at runtime.
BLCK SSC Percentage	This parameter is not configura...	Specifies the maximum precentage of spread adjustment that can be applied to the clock....

#	Parameter	Platform	Settings
⑤	**Integrated Clock Controller - Profiles - Profile ClockRangeDefinitionRecord**		

Table 2-8. - Integrated Clock Controller (Sheet 4 of 7)

	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.	ICL-YN ICL-UN	
	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.	ICL-YN ICL-UN	
	BCLK SSC Changes Allowed - This parameter allows user to specify if the spread mode and percentage is allowed to be modified at runtime or not. if set to **“True’:** Runtime modification is allowed. **Standard Setting Profile Type -** Option is grayed out. **Adaptive Setting Profile Type -** Option is able to be edited.	ICL-YN ICL-UN	
	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.	ICL-YN ICL-UN	
	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.	ICL-YN ICL-UN	

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



Clock Output Configuration ⑥

Parameter	Value	He
SRC0	Enabled	Enable/Disable the CLKOUT_SRC0 differer
SRC1	Enabled	Enable/Disable the CLKOUT_SRC1 differer
SRC2	Enabled	Enable/Disable the CLKOUT_SRC2 differer
SRC3	Enabled	Enable/Disable the CLKOUT_SRC3 differer
SRC4	Enabled	Enable/Disable the CLKOUT_SRC4 differer
SRC5	Enabled	Enable/Disable the CLKOUT_SRC5 differer
CPUPCIBCLK to PCIe Gen 4 Status	Disabled	Enable/Disable the CPUPCIBCLK to PCIe G
SRC0 to use PCIe Gen 4	Disabled	Enable/Disable SRC0 to use PCIe Gen 4.
SRC3 to use PCIe Gen 4	Disabled	Enable/Disable SRC3 to use PCIe Gen 4.
SRC4 to use PCIe Gen 4	Disabled	Enable/Disable SRC4 to use PCIe Gen 4.

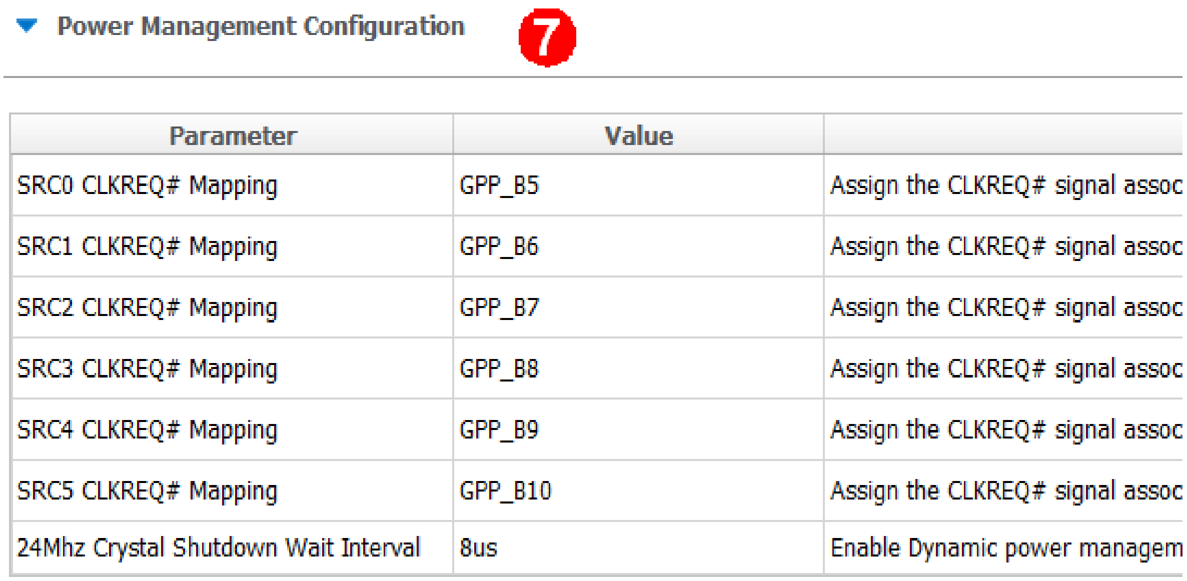
#	Parameter	Platform	Settings
⑥	**Integrated Clock Controller - Profiles - Profile Clock Output Configuration**		

Table 2-8. - Integrated Clock Controller (Sheet 5 of 7)

	ITPXDP,SRC[0:5] **Values: Enabled / Disabled** These parameters come under the Power Management section and they control Enabling /Disabling of specific Output Clocks at boot time. These settings should match with platform hardware design. For CRB, recommend keeping defaults for bring up with Intel® ME FW. These parameters are specifically used to Enable/Disable the respective CLKOUT_XXX differential output buffers	ICL-YN ICL-UN	Enabled Enabled
	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 CRB, recommend keeping defaults for bring up with Intel® ME FW. These parameters are specifically used to Enable/Disable the respective CLKOUT_XXX differential output buffers	ICL-YN ICL-UN	Enabled Enabled
	SRC1 **Values: Enabled / Disabled** Enables or Disables the CLKOUT_SRC1 differential output buffer.	ICL-YN ICL-UN	Enabled Enabled
	SRC2 **Values: Enabled / Disabled** Enables or Disables the CLKOUT_SRC2 differential output buffer.	ICL-YN ICL-UN	Enabled Enabled
	SRC3 **Values: Enabled / Disabled** Enables or Disables the CLKOUT_SRC3 differential output buffer.	ICL-YN ICL-UN	Enabled Enabled
	SRC4 **Values: Enabled / Disabled** Enables or Disables the CLKOUT_SRC4 differential output buffer.	ICL-YN ICL-UN	Enabled Enabled
	SRC5 **Values: Enabled / Disabled** Enables or Disables the CLKOUT_SRC5 differential output buffer.	ICL-YN ICL-UN	Enabled Enabled
	SRC6 **Values: Enabled / Disabled** Enables or Disables the CLKOUT_SRC6 differential output buffer.	ICL-YN ICL-UN	NA NA
	CPUPCIBCLK to PCIe Gen 4 Status **Values: Enabled / Disabled** This setting Enables or Disables Gen 4 support for CPUPCIBCLK	ICL-YN ICL-UN	Disabled Disabled
	SRC0 to use PCIe Gen 4 **Values: Enabled / Disabled** This setting Enables or Disables Gen 4 support for SRC0	ICL-YN ICL-UN	Disabled Disabled
	SRC3 to use PCIe Gen 4 **Values: Enabled / Disabled** This setting Enables or Disables Gen 4 support for SRC3	ICL-YN ICL-UN	Disabled Disabled
	SRC4 to use PCIe Gen 4 **Values: Enabled / Disabled** This setting Enables or Disables Gen 4 support for SRC4	ICL-YN ICL-UN	Disabled Disabled

Table 2-8. - Integrated Clock Controller (Sheet 6 of 7)

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



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

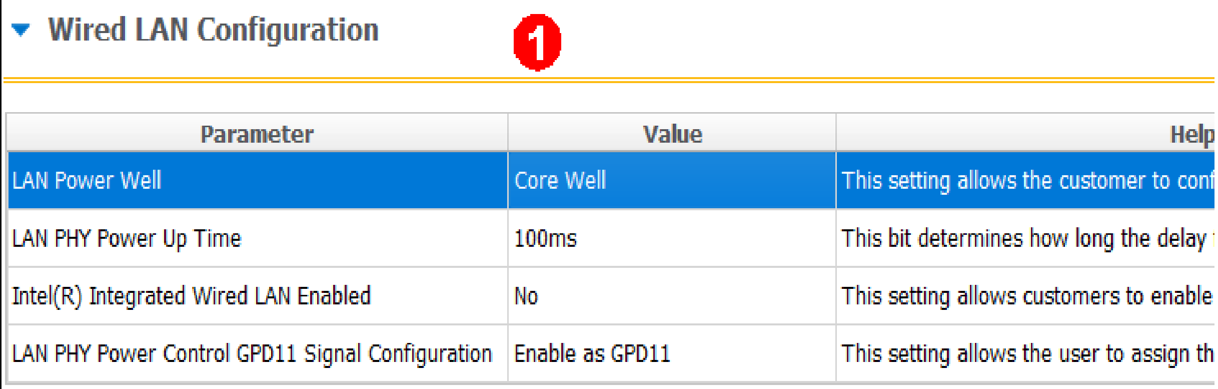
#	Parameter	Platform	Settings
⑦	**Integrated Clock Controller - Profiles - Profile Power Management Configuration** Configuring CLKREQ# and assigning GPIO depends on how CLKOUT_SRCx configuration via FIT is done (Enabled or Disabled) and if CLKREQ is required or not. **Please refer to Appendix B.3 (How to configure CLKREQ# parameters)** for the detail of CLKREQ configuration for SRC Output clocks. Please configure CLKREQ parameters accordingly.		
	SRC0[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 - ICL/CFL H/S Only** Possible configuration: Select one of the GPIOs from the list to map it as a CLKREQ# for specific SRC# Output put clock. This parameter controls association of dynamic CLKREQ control with SRC (PCIe) clocks.	ICL-YN ICL-UN	GPP_B5 GPP_B5
	SRC1 CLKREQ# Mapping Assign the CLKREQ# signal associated with CLKOUT_SRC1.	ICL-YN ICL-UN	GPP_B6 GPP_B6
	SRC2 CLKREQ# Mapping Assign the CLKREQ# signal associated with CLKOUT_SRC2.	ICL-YN ICL-UN	GPP_B7 GPP_B7
	SRC3 CLKREQ# Mapping Assign the CLKREQ# signal associated with CLKOUT_SRC3.	ICL-YN ICL-UN	GPP_B8 GPP_B8
	SRC4 CLKREQ# Mapping Assign the CLKREQ# signal associated with CLKOUT_SRC4.	ICL-YN ICL-UN	GPP_B9 GPP_B9

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

	SRC5 CLKREQ# Mapping Assign the CLKREQ# signal associated with CLKOUT_SRC5.	ICL-YN ICL-UN	GPP_B10 GPP_B10
	24MHz Crystal Shutdown Wait Interval This parameter allows user to Enable Dynamic power management of Crystal. Upon the event that all conditions (other than this wait timer itself) are satisfied for iSCLK crystal shutdown, a timer is started. Once it expires and there are no wake events, iSCLK will shutdown crystal. **Note:** Recommendation is to leave setting at default value.	ICL-YN ICL-UN	8us 8us

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

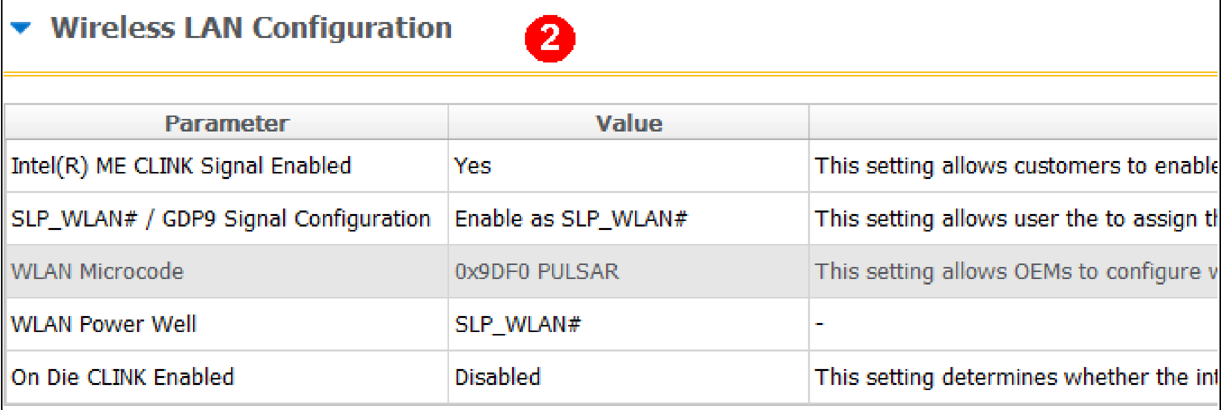
Click on Networking & Connectivity in the left tabs menu> Wired LAN Configuration is expanded by default:



Parameter	Value	Help
LAN Power Well	Core Well	This setting allows the customer to conf
LAN PHY Power Up Time	100ms	This bit determines how long the delay
Intel(R) Integrated Wired LAN Enabled	No	This setting allows customers to enable
LAN PHY Power Control GPD11 Signal Configuration	Enable as GPD11	This setting allows the user to assign th

#	Parameter	Platform	Settings
①	**Networking & Connectivity - 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#.	ICL-YN ICL-UN	Core Well Core Well
	LAN PHY Power Up Time **Values: 50ms, 100ms**	ICL-YN ICL-UN	100ms 100ms
	Intel® Integrated Wired LAN Enabled **Values: Yes/No -** This setting enables or disables the Intel® Integrated LAN.	ICL-YN ICL-UN	No No
	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".	ICL-YN ICL-UN	Enable as GPD11 Enable as GPD11

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



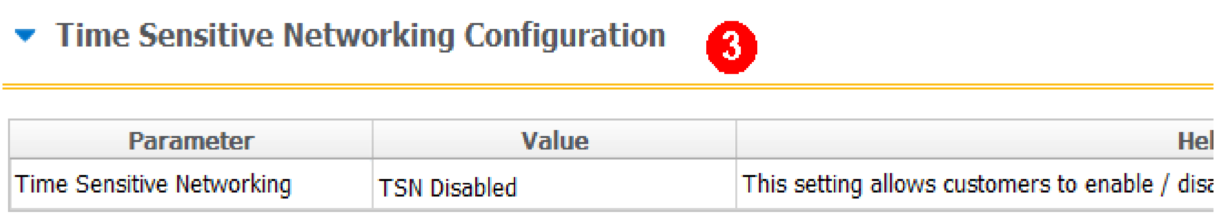
Parameter	Value	
Intel(R) ME CLINK Signal Enabled	Yes	This setting allows customers to enable
SLP_WLAN# / GDP9 Signal Configuration	Enable as SLP_WLAN#	This setting allows user the to assign th
WLAN Microcode	0x9DF0 PULSAR	This setting allows OEMs to configure w
WLAN Power Well	SLP_WLAN#	-
On Die CLINK Enabled	Disabled	This setting determines whether the int

#	Parameter	Platform	Settings
②	**Networking & Connectivity - Wireless LAN Configuration**		

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

	CLINK Enabled **Values: Yes/No** - This setting allows customers to enable / disable the Wireless LAN CLINK signal through Intel® ME firmware. **Note:** For using Intel® vPro™ Wireless solutions this should be set to "Yes".	ICL-YN ICL-UN	No No
	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#".	ICL-YN ICL-UN	Enable as SLP_WLAN# Enabled as SLP_WLAN #
	WLAN Microcode - This setting allow OEMs to configure which Intel® Wireless LAN card microcode to load into the firmware image.	ICL-YN ICL-UN	0x9DF0 0x9DF0
	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#.	ICL-YN ICL-UN	SLP_WLAN# SLP_WLAN#
	On Die CLINK Enabled **Values: Enabled/Disabled** This setting determines whether the internal On-die CLINK port is enabled.	ICL-YN ICL-UN	Disabled Disabled

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



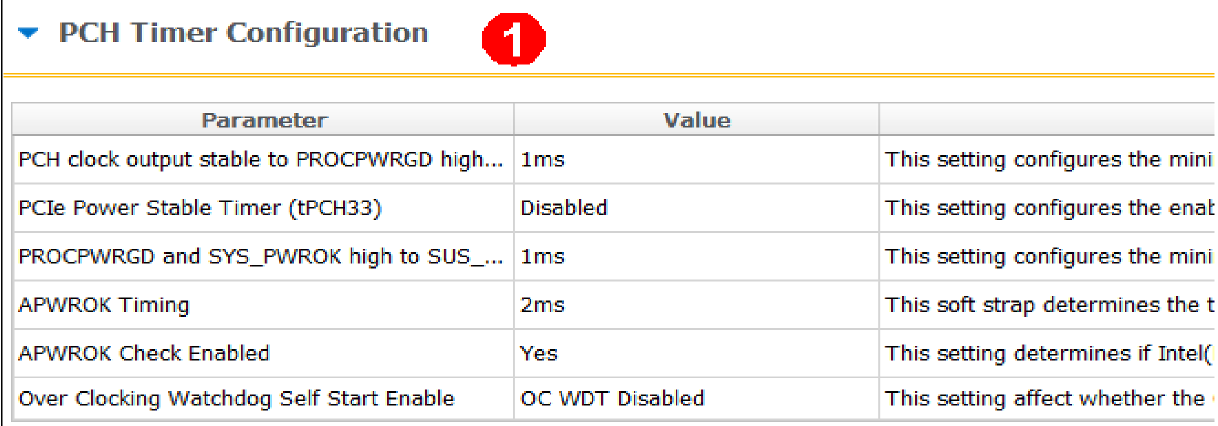
Time Sensitive Networking Configuration

Parameter	Value	Hel
Time Sensitive Networking	TSN Disabled	This setting allows customers to enable / disa

#	Parameter	Platform	Settings
③	**Time Sensitive Networking** **Values: TSN Enable / TSN Disabled** ***Note:*** Time Sensitive Networking and Wired LAN are mutually exclusive only one other these features can enabled on the platform.	ICL-YN ICL-UN	Disabled Disabled

Table 2-10. - Internal PCH Buses (Sheet 1 of 4)

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



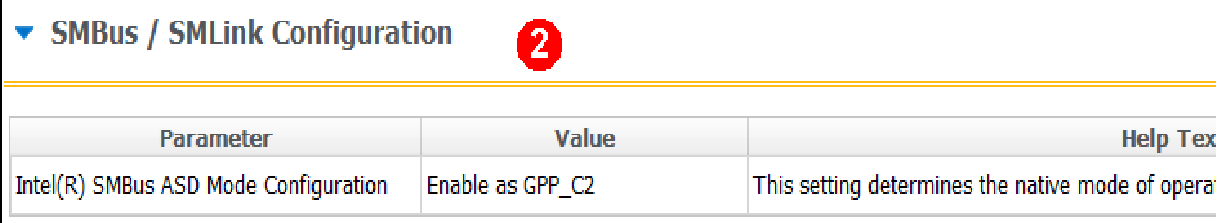
PCH Timer Configuration ①

Parameter	Value	
PCH clock output stable to PROCPWRGD high...	1ms	This setting configures the mini
PCIe Power Stable Timer (tPCH33)	Disabled	This setting configures the enat
PROCPWRGD and SYS_PWROK high to SUS_...	1ms	This setting configures the mini
APWROK Timing	2ms	This soft strap determines the t
APWROK Check Enabled	Yes	This setting determines if Intel(
Over Clocking Watchdog Self Start Enable	OC WDT Disabled	This setting affect whether the

#	Parameter	Platform	Settings
①	**Internal PCH Buses - PCH Timer Configuration**		
	PCH clock output stable to PROCPWRGD high (tPCH45) **Values: 100ms, 50ms, 5ms, 1ms** - This setting configures the minimum timing from XCK_PLL locked to CPUPWRGD high. For further details see Ice Lake LP Platform Controller Hub EDS.	ICL-YN ICL-UN	1ms 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".	ICL-YN ICL-UN	Disabled 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 Ice Lake LP Platform Controller Hub EDS.	ICL-YN ICL-UN	1ms 1ms
	APWROK Timing **Values: 2ms, 4ms, 8ms, 16ms** - This soft strap determines the time between the SLP_A# pin de-asserting and the APWROK timer expiration. For further details see Ice Lake LP Platform Controller Hub EDS.	ICL-YN ICL-UN	2ms 2ms
	APWROK Check Enabled **Values: Yes/No** - This setting determines if Intel® ME should de-assert SLP_A# and wait for APWROK or not.	ICL-YN ICL-UN	Yes Yes
	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	ICL-YN ICL-UN	OC WDT Disabled 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 4)

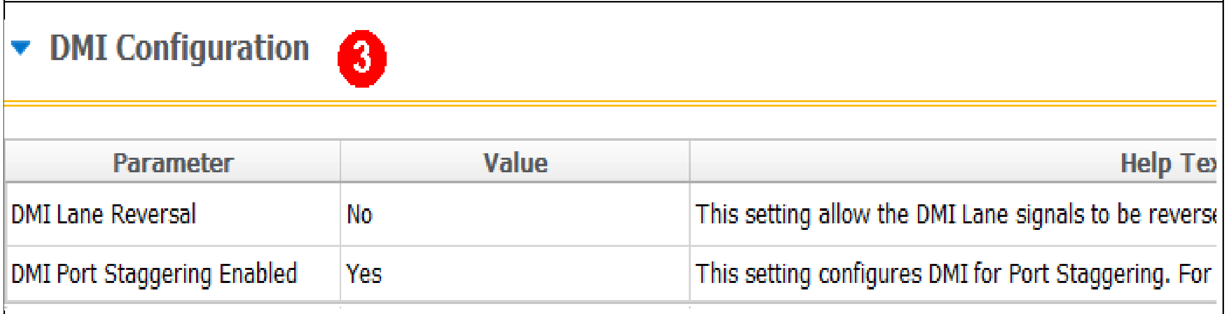


SMBus / SMLink Configuration

Parameter	Value	Help Tex
Intel(R) SMBus ASD Mode Configuration	Enable as GPP_C2	This setting determines the native mode of opera

#	Parameter	Platform	Settings
②	**Internal PCH Buses - SMBus / SMLink Configuration**		
	Intel® SMBus ASD Mode Configuration This setting determines the native mode of operation for the Intel® SMBus ASD signal.	ICL-YN ICL-UN	Enable as GPP_C2 Enable as GPP_C2

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

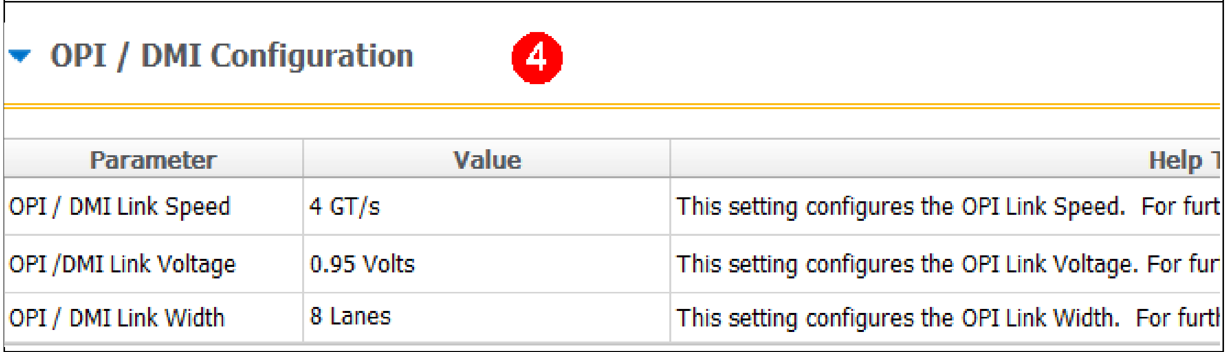


DMI Configuration

Parameter	Value	Help Tex
DMI Lane Reversal	No	This setting allow the DMI Lane signals to be reverse
DMI Port Staggering Enabled	Yes	This setting configures DMI for Port Staggering. For

#	Parameter	Platform	Settings
③	**Internal PCH Buses - DMI Configuration**		
	DMI Lane Reversal **Values: Yes/No** - This setting allows the DMI Lane signals to be reversed. For further details see Ice Lake LP Platform Controller Hub EDS.	ICL-YN ICL-UN	No No
	DMI Port Staggering **Values: Yes/No** - This setting configures DMI for Port Staggering. For further details see Ice Lake LP Platform Controller Hub EDS.	ICL-YN ICL-UN	Yes Yes

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



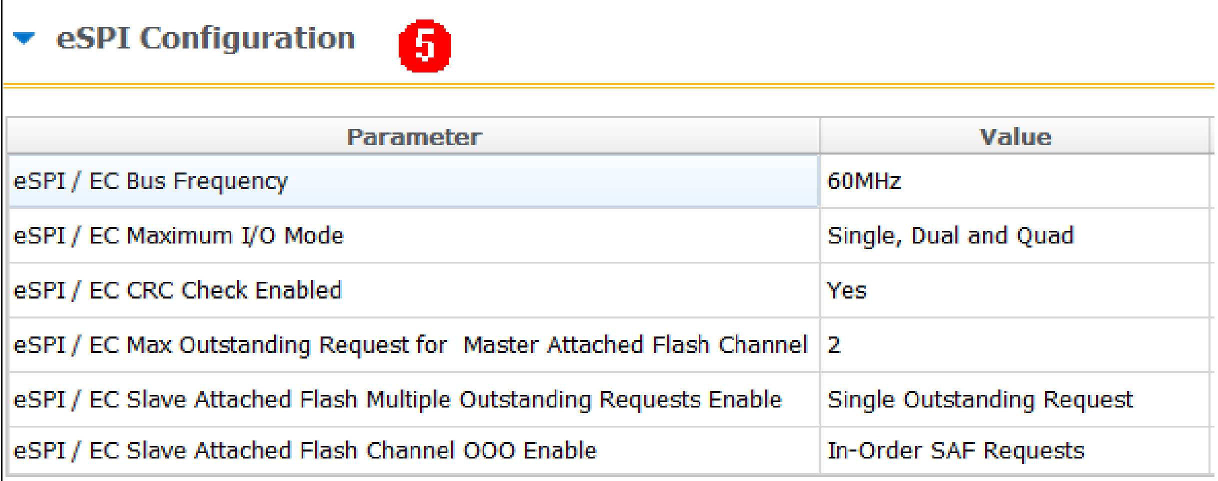
OPI / DMI Configuration

Parameter	Value	Help T
OPI / DMI Link Speed	4 GT/s	This setting configures the OPI Link Speed. For furt
OPI /DMI Link Voltage	0.95 Volts	This setting configures the OPI Link Voltage. For fur
OPI / DMI Link Width	8 Lanes	This setting configures the OPI Link Width. For furtl

#	Parameter	Platform	Settings

Table 2-10. - Internal PCH Buses (Sheet 3 of 4)

④	**Internal PCH Buses - OPI / DMI Configuration**		
	OPI Link Speed **Values: GT2/GT4 -** This setting configures the OPI / DMI Link Speed. For further details see Ice Lake PCH EDS.	ICL-YN ICL-UN	4 GT/s 4 GT/s
	OPI Link Voltage **Values: 0.85 Volts, 0.95 Volts -** This setting configures the OPI / DMI Link Voltage. For further details see Ice Lake PCH EDS.	ICL-YN ICL-UN	0.95 Volts 0.95 Volts
	OPI Link Width **Values: 1 Lanes, 2 Lanes, 4 Lanes, 8 Lanes -** This setting configures the OPI / DMI Link Width. For further details see Ice Lake PCH EDS.	ICL-YN ICL-UN	8 Lanes 8 Lanes
Click on Internal PCH Buses in the left tabs menu> eSPI Configuration is expanded by default:			



eSPI Configuration ⑤

Parameter	Value
eSPI / EC Bus Frequency	60MHz
eSPI / EC Maximum I/O Mode	Single, Dual and Quad
eSPI / EC CRC Check Enabled	Yes
eSPI / EC Max Outstanding Request for Master Attached Flash Channel	2
eSPI / EC Slave Attached Flash Multiple Outstanding Requests Enable	Single Outstanding Request
eSPI / EC Slave Attached Flash Channel OOO Enable	In-Order SAF Requests

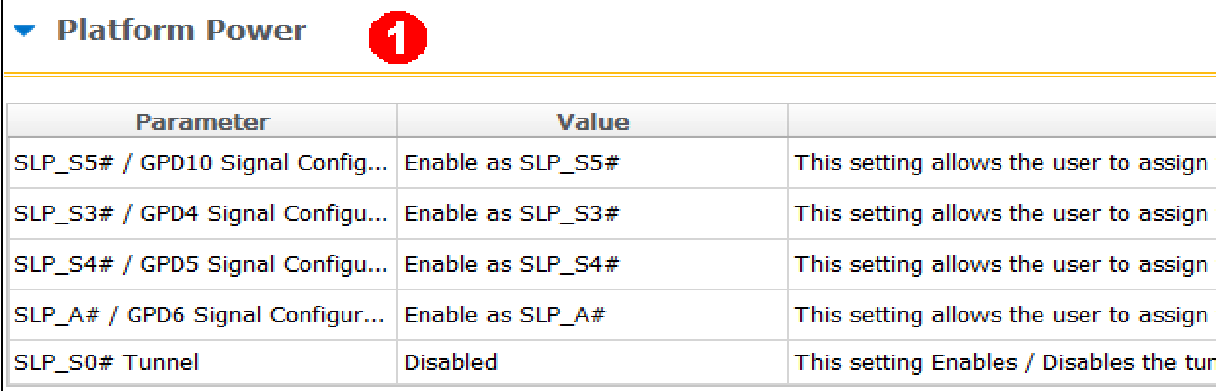
#	Parameter	Platform	Settings
⑤	**Internal PCH Buses - eSPI Configuration**		
	eSPI / EC Bus Frequency **Values: 20MHz, 24MHz, 30MHz, 40MHz, 60MHz** This setting determines the maximum frequency of the eSPI bus that is supported by the eSPI Master and platform configuration. ***Note:*** The actual frequency depends on trace length, number of eSPI Slaves, etc.	ICL-YN ICL-UN	60MHz 60MHz
	eSPI / EC Maximum I/O Mode **Values: Single, Single and Dual, Single and Quad, Single Dual and Quad** This setting determines the maximum IO Mode (Single/Dual/Quad) of the eSPI bus that is supported by the eSPI Master and specific platform configuration. ***Note:*** 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.	ICL-YN ICL-UN	Single, Dual and Quad Single, Dual and Quad
	eSPI / EC CRC Check Enabled **Values: Yes/No** This setting enables CRC checking on eSPI Slave 0 channel.	ICL-YN ICL-UN	Yes Yes

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

	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.	ICL-YN ICL-UN	2 2
	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.	ICL-YN ICL-UN	Single Outstanding Request Single Outstanding Request
	eSPI / EC Slave Attached Flash Channel OOO Enable **Values: In-Order SAF Requests, Out-of-Order SAF Requests** This setting enables Out or Order requests on the eSPI / EC Slave Attached Flash device.	ICL-YN ICL-UN	In-Order SAF Requests In-Order SAF Requests

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

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

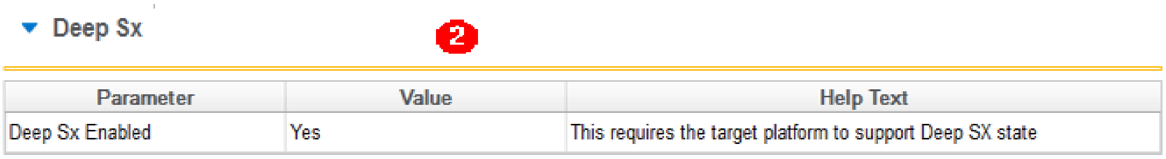


Platform Power ①

Parameter	Value	
SLP_S5# / GPD10 Signal Config...	Enable as SLP_S5#	This setting allows the user to assign
SLP_S3# / GPD4 Signal Configu...	Enable as SLP_S3#	This setting allows the user to assign
SLP_S4# / GPD5 Signal Configu...	Enable as SLP_S4#	This setting allows the user to assign
SLP_A# / GPD6 Signal Configur...	Enable as SLP_A#	This setting allows the user to assign
SLP_S0# Tunnel	Disabled	This setting Enables / Disables the tur

#	Parameter	Platform	Settings
①	**Power - 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 Ice Lake LP Platform Controller Hub EDS.	ICL-YN ICL-UN	SLP_S3# 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 Ice Lake LP Platform Controller Hub EDS.	ICL-YN ICL-UN	SLP_S4# 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 Ice Lake LP Platform Controller Hub EDS.	ICL-YN ICL-UN	SLP_S5# 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 Ice Lake LP Platform Controller Hub EDS.	ICL-YN ICL-UN	SLP_A# 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.	ICL-YN ICL-UN	Disabled Disabled

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



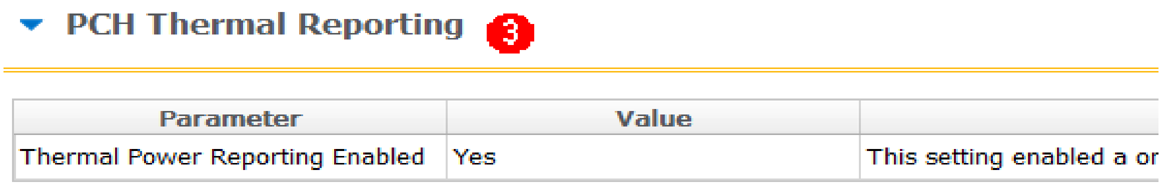
Deep Sx ②

Parameter	Value	Help Text
Deep Sx Enabled	Yes	This requires the target platform to support Deep SX state

#	Parameter	Platform	Settings
②	**Power - Deep Sx**		
	Deep Sx Enabled **Values: Yes/ No -** This setting enables / disables support for Deep Sx operation. For further details see Ice Lake LP Platform Controller Hub EDS. **Note:** Support for Deep Sx is board design dependent.	ICL-YN ICL-UN	No No

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

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



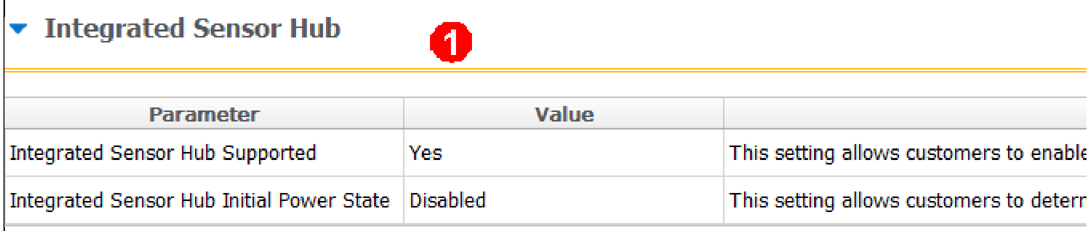
PCH Thermal Reporting 3

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

#	Parameter	Platform	Settings
3	**Power - 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.	ICL-YN ICL-UN	Yes Yes

Table 2-12. - Integrated Sensor Hub

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

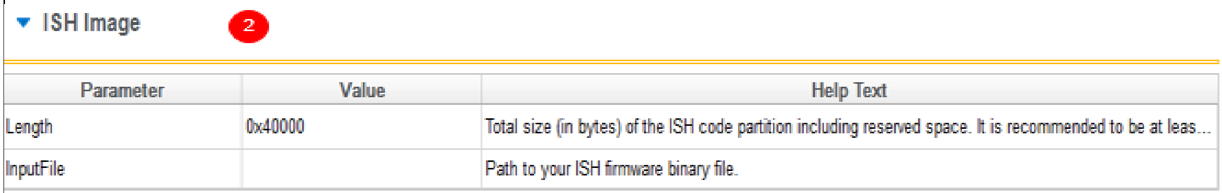


Integrated Sensor Hub

Parameter	Value	
Integrated Sensor Hub Supported	Yes	This setting allows customers to enable
Integrated Sensor Hub Initial Power State	Disabled	This setting allows customers to determ

#	Parameter	Platform	Settings
①	**Integrated Sensor Hub**		
	Integrated Sensor Hub Supported **Values: Yes/No** This setting allows customers to disable ISH on the platform.	ICL-YN ICL-UN	No 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.	ICL-YN ICL-UN	Disabled Disabled

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

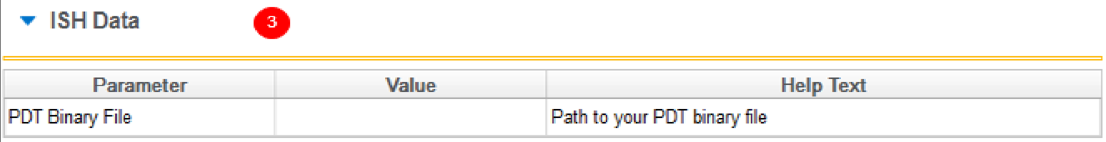


ISH Image

Parameter	Value	Help Text
Length	0x40000	Total size (in bytes) of the ISH code partition including reserved space. It is recommended to be at leas...
InputFile		Path to your ISH firmware binary file.

#	Parameter	Platform	Settings
②	**Integrated Sensor Hub - ISH Image**		
	Length - Total size (in bytes) of the ISH code partition including reserved space. It is recommended to be at least 256kb.		
	Input File	ICL-YN ICL-UN	

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



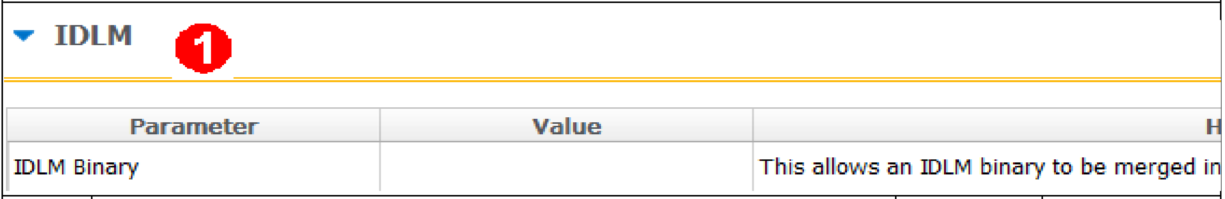
ISH Data

Parameter	Value	Help Text
PDT Binary File		Path to your PDT binary file

#	Parameter	Platform	Settings
③	**Integrated Sensor Hub - ISH Data**		
	PDT Binary File	ICL-YN ICL-UN	Path for PDT Binary file Path for PDT Binary file

Table 2-13. - Debug (Sheet 1 of 5)

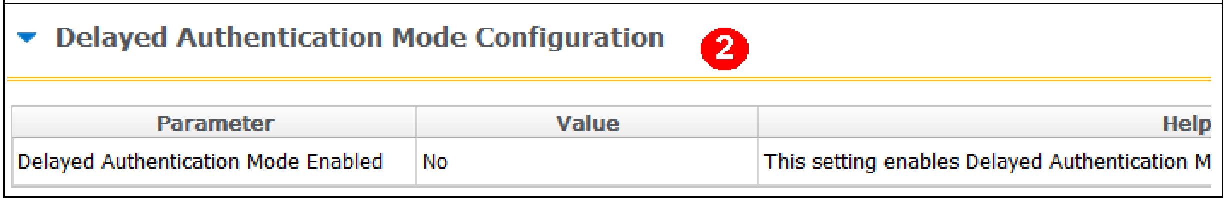
Click on Debug in the left tabs menu> Intel® ME Firmware Debugging Overrides is expanded by default:



Parameter	Value	H
IDLM Binary		This allows an IDLM binary to be merged in

#	Parameter	Platform	Settings
①	**Debug - IDLM**		
	IDLM Binary This allows an IDLM binary to be merged into output image built by Intel® FIT.	ICL-YN ICL-UN	

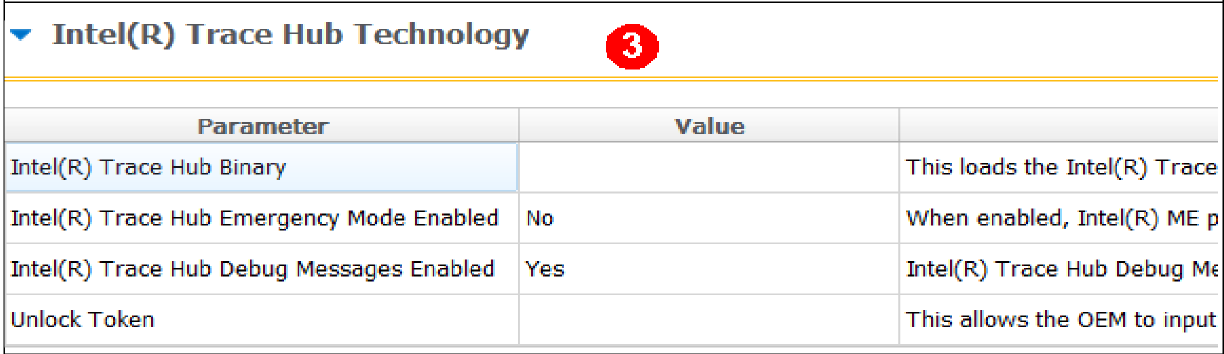
Click on Debug in the left tabs menu> Delayed Authentication Mode is expanded by default:



Parameter	Value	Help
Delayed Authentication Mode Enabled	No	This setting enables Delayed Authentication M

#	Parameter	Platform	Settings
②	**Debug - Delayed Authentication Mode**		
	Delayed Authentication Mode Enabled **Values: Yes/No** This setting enables Delayed Authentication Mode on the platform.	ICL-YN ICL-UN	No No

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



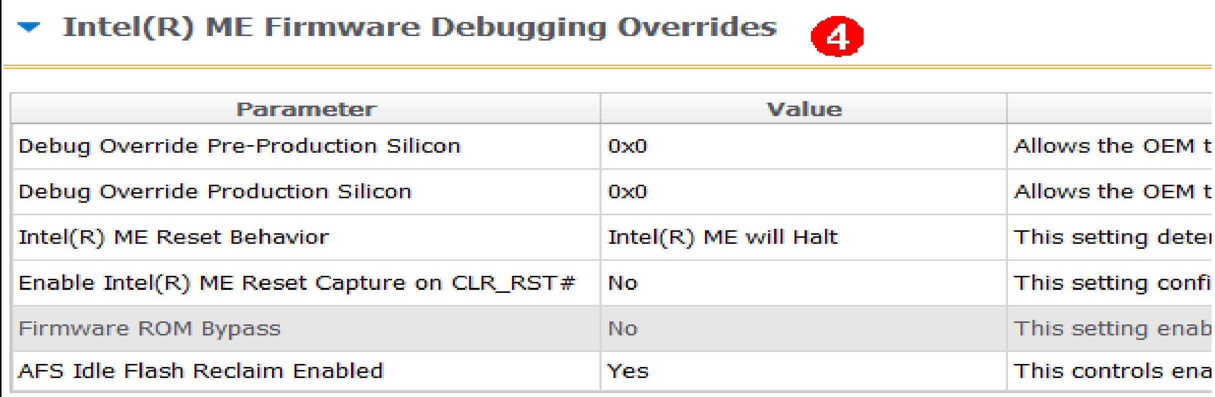
Parameter	Value	
Intel(R) Trace Hub Binary		This loads the Intel(R) Trace
Intel(R) Trace Hub Emergency Mode Enabled	No	When enabled, Intel(R) ME p
Intel(R) Trace Hub Debug Messages Enabled	Yes	Intel(R) Trace Hub Debug Me
Unlock Token		This allows the OEM to input

#	Parameter	Platform	Settings
③	**Debug - 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.	ICL-YN ICL-UN	Trace Hub Binary Trace Hub Binary

Table 2-13. - Debug (Sheet 2 of 5)

	Intel® Trace Hub Emergency Mode Enabled **Values: Yes/No** - This setting enable / disables Intel® Trace Hub in the firmware base image.	ICL-YN ICL-UN	No No
	Intel® Trace Hub Debug Message Enabled **Values: Yes/No** - This setting enables/disables the Intel® Trace Hub debug messages. **Note:** When enabling this setting you also need to enable Intel® Trace Hub Soft Enable setting for proper operation.	ICL-YN ICL-UN	Yes Yes
	Unlock Token This allows the OEM to input an Unlock Token binary file for closed chassis debug.	ICL-YN ICL-UN	

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



Intel(R) ME Firmware Debugging Overrides ④

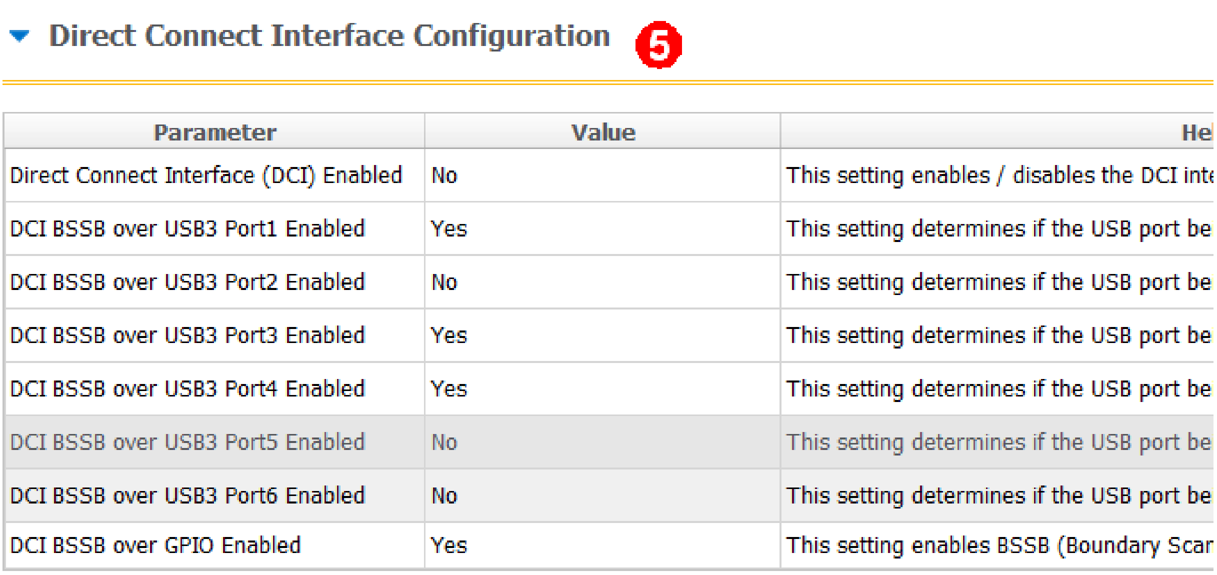
Parameter	Value	
Debug Override Pre-Production Silicon	0x0	Allows the OEM t
Debug Override Production Silicon	0x0	Allows the OEM t
Intel(R) ME Reset Behavior	Intel(R) ME will Halt	This setting dete
Enable Intel(R) ME Reset Capture on CLR_RST#	No	This setting confi
Firmware ROM Bypass	No	This setting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

#	Parameter	Platform	Settings
④	**Debug - 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.	ICL-YN ICL-UN	0x00000000 0x00000000
	Debug Override Production Silicon - Allows the OEM to control FW features to assist with production platform debugging. **Bit 0:** Extend DRAM_INIT_DONE timeout to 30 minutes (default timeout 15 seconds) **Bit 1:** Disable Host Reset Timer **Bit 2:** Disable CPU_RESET_DONE timeout **Note:** Certain options do not work when the descriptor is locked.	ICL-YN ICL-UN	0x00000000 0x00000000
	Intel® ME Reset Behavior 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.	ICL-YN ICL-UN	Intel® ME will Halt Intel® ME will Halt
	Enable Intel® ME Reset Capture on CLR_RST#	ICL-YN ICL-UN	No No

Table 2-13. - Debug (Sheet 3 of 5)

	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.	ICL-YN ICL-UN	No 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.	ICL-YN ICL-UN	Yes Yes

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



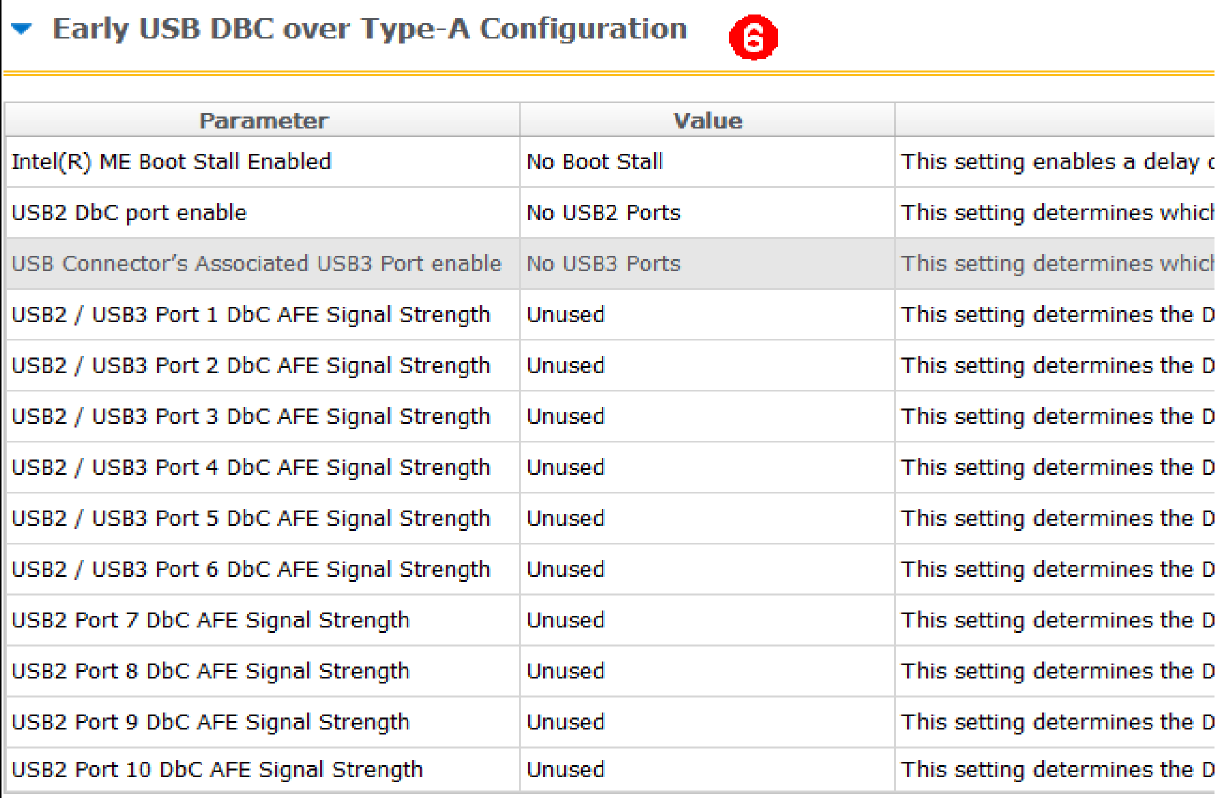
Direct Connect Interface Configuration ⑤

Parameter	Value	He
Direct Connect Interface (DCI) Enabled	No	This setting enables / disables the DCI int
DCI BSSB over USB3 Port1 Enabled	Yes	This setting determines if the USB port be
DCI BSSB over USB3 Port2 Enabled	No	This setting determines if the USB port be
DCI BSSB over USB3 Port3 Enabled	Yes	This setting determines if the USB port be
DCI BSSB over USB3 Port4 Enabled	Yes	This setting determines if the USB port be
DCI BSSB over USB3 Port5 Enabled	No	This setting determines if the USB port be
DCI BSSB over USB3 Port6 Enabled	No	This setting determines if the USB port be
DCI BSSB over GPIO Enabled	Yes	This setting enables BSSB (Boundary Sca

#	Parameter	Platform	Settings
⑤	**Debug - 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		
	Direct Connect Interface (DCI) Enabled **Values: Yes/No** - This setting enables / disables the DCI interface used for Intel® Trace Hub debugging.	ICL-YN ICL-UN	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.	ICL-YN ICL-UN	Yes 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.	ICL-YN ICL-UN	Yes Yes

Table 2-13. - Debug (Sheet 4 of 5)

	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.	ICL-YN ICL-UN	No No
	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.	ICL-YN ICL-UN	No No
	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.	ICL-YN ICL-UN	No No
	DCI BSSB over USB3 Port 6 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.	ICL-YN ICL-UN	No No
Click on Debug in the left tabs menu> Early USB DBC Type-A Configuration is expanded by default:			

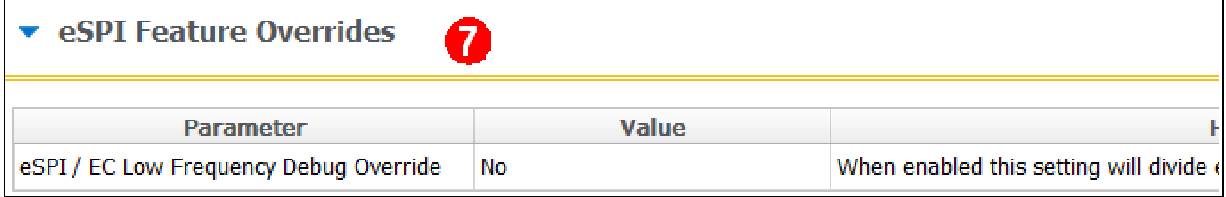


Parameter	Value	
Intel(R) ME Boot Stall Enabled	No Boot Stall	This setting enables a delay c
USB2 DbC port enable	No USB2 Ports	This setting determines whic
USB Connector's Associated USB3 Port enable	No USB3 Ports	This setting determines whic
USB2 / USB3 Port 1 DbC AFE Signal Strength	Unused	This setting determines the D
USB2 / USB3 Port 2 DbC AFE Signal Strength	Unused	This setting determines the D
USB2 / USB3 Port 3 DbC AFE Signal Strength	Unused	This setting determines the D
USB2 / USB3 Port 4 DbC AFE Signal Strength	Unused	This setting determines the D
USB2 / USB3 Port 5 DbC AFE Signal Strength	Unused	This setting determines the D
USB2 / USB3 Port 6 DbC AFE Signal Strength	Unused	This setting determines the D
USB2 Port 7 DbC AFE Signal Strength	Unused	This setting determines the D
USB2 Port 8 DbC AFE Signal Strength	Unused	This setting determines the D
USB2 Port 9 DbC AFE Signal Strength	Unused	This setting determines the D
USB2 Port 10 DbC AFE Signal Strength	Unused	This setting determines the D

Table 2-13. - Debug (Sheet 5 of 5)

#	Parameter	Platform	Settings
⑥	**Debug - Early USB DBC Type-A Configuration**		
	Intel® ME Boot Stall Enabled This setting enables a delay during Intel® ME FW bring-up to allow USB DCI to be established and Early DbC arbitration to be granted.	ICL-YN ICL-UN	No Boot Stall No Boot Stall
	USB2 DbC port enable This setting determines which USB2 ports are enabled for Early DbC debugging.	ICL-YN ICL-UN	No USB2 Ports No USB2 Ports
	USB Connectors associated USB3 Port enable This setting determines which USB3 ports goes to the target USB2 ports connector for Early DbC debugging.	ICL-YN ICL-UN	No USB3 Ports No USB3 Ports
	USB2 / USB3 Port 1 DbC AFE Signal Strength This setting determines the DbC Analog Front End signal strength for USB2 / USB3 port 1.	ICL-YN ICL-UN	Unused Unused
	USB2 / USB3 Port 2 DbC AFE Signal Strength This setting determines the DbC Analog Front End signal strength for USB2 / USB3 port 2.	ICL-YN ICL-UN	Unused Unused
	USB2 / USB3 Port 3 DbC AFE Signal Strength This setting determines the DbC Analog Front End signal strength for USB2 / USB3 port 3.	ICL-YN ICL-UN	Unused Unused
	USB2 / USB3 Port 4 DbC AFE Signal Strength This setting determines the DbC Analog Front End signal strength for USB2 / USB3 port 4.	ICL-YN ICL-UN	Unused Unused
	USB2 / USB3 Port 5 DbC AFE Signal Strength This setting determines the DbC Analog Front End signal strength for USB2 / USB3 port 5.	ICL-YN ICL-UN	Unused Unused
	USB2 / USB3 Port 6 DbC AFE Signal Strength This setting determines the DbC Analog Front End signal strength for USB2 / USB3 port 6.	ICL-YN ICL-UN	Unused Unused
	USB2 Port 7 DbC AFE Signal Strength This setting determines the DbC Analog Front End signal strength for USB2 port 7.	ICL-YN ICL-UN	Unused Unused
	USB2 Port 8 DbC AFE Signal Strength This setting determines the DbC Analog Front End signal strength for USB2 port 8.	ICL-YN ICL-UN	Unused Unused
	USB2 Port 9 DbC AFE Signal Strength This setting determines the DbC Analog Front End signal strength for USB2 port 9.	ICL-YN ICL-UN	Unused Unused
	USB2 Port 10 DbC AFE Signal Strength This setting determines the DbC Analog Front End signal strength for USB2 port 10.	ICL-YN ICL-UN	Unused Unused

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



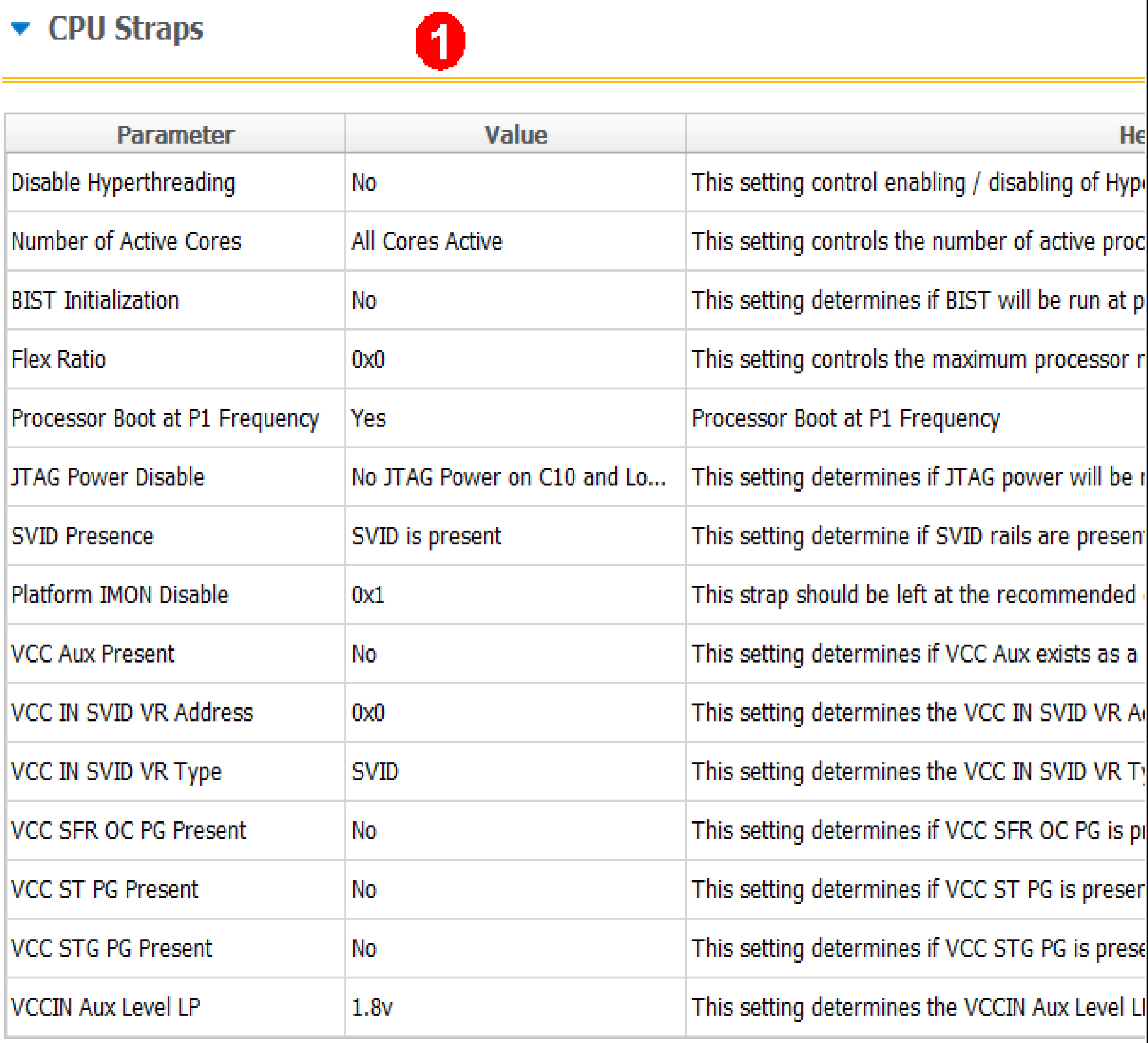
eSPI Feature Overrides ⑦

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

#	Parameter	Platform	Settings
⑦	**Debug - eSPI Feature Overrides**		
	eSPI / EC Low Frequency Debug Override When enabled this setting will divide eSPI clock frequency by 8. ***Note:*** This setting should only be used for debugging purposes. Leaving this setting enable will impact eSPI performance.	ICL-YN ICL-UN	No No

Table 2-14. - CPU Straps (Sheet 1 of 2)

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



Parameter	Value	He
Disable Hyperthreading	No	This setting control enabling / disabling of Hyp
Number of Active Cores	All Cores Active	This setting controls the number of active proc
BIST Initialization	No	This setting determines if BIST will be run at p
Flex Ratio	0x0	This setting controls the maximum processor r
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 will be r
SVID Presence	SVID is present	This setting determine if SVID rails are presen
Platform IMON Disable	0x1	This strap should be left at the recommended
VCC Aux Present	No	This setting determines if VCC Aux exists as a
VCC IN SVID VR Address	0x0	This setting determines the VCC IN SVID VR A
VCC IN SVID VR Type	SVID	This setting determines the VCC IN SVID VR T
VCC SFR OC PG Present	No	This setting determines if VCC SFR OC PG is p
VCC ST PG Present	No	This setting determines if VCC ST PG is preser
VCC STG PG Present	No	This setting determines if VCC STG PG is prese
VCCIN Aux Level LP	1.8v	This setting determines the VCCIN Aux Level L

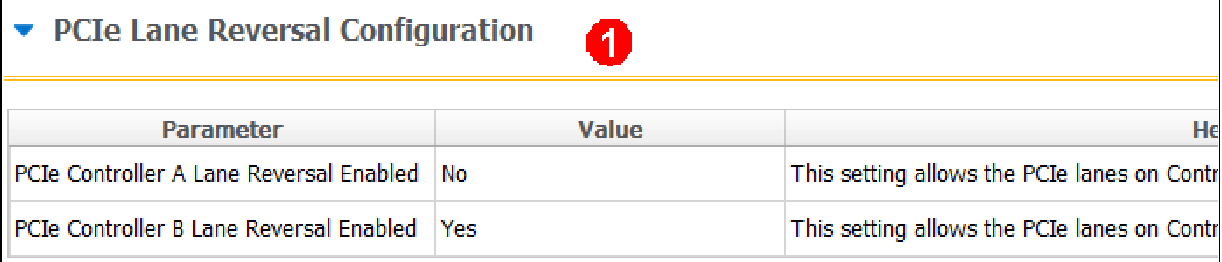
#	Parameter	Platform	Settings
1	**CPU Straps - CPU Straps**		
	Disable Hyperthreading **Values: Yes/No** This setting controls enabling or disabling of Hyper threading. **Note:** This strap is intended for debugging purposes only. See BIOS Spec for more details on enabling / disabling Hyperthreading.	ICL-YN ICL-UN	No No

Table 2-14. - CPU Straps (Sheet 2 of 2)

	Number of Active Cores **Values: All, 1, 2, 3, 4, 5, 6, 7, 8** 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.	ICL-YN ICL-UN	All All
	BIST Initialization **Values: Yes/No** This setting determines if BIST will be run at platform reset after BIOS requested actions. **Note:** This strap is intended for debugging purposes only.	ICL-YN ICL-UN	No No
	Flex Ratio This setting controls the maximum processor non-turbo ratio. **Note:** This strap is intended for debugging purposes only. See BIOS Spec for more details on maximum processor non-turbo ratio configuration.	ICL-YN ICL-UN	0x0 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.	ICL-YN ICL-UN	Yes 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.	ICL-YN ICL-UN	No JTAG Power on C10 and Lower 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.	ICL-YN ICL-UN	SVID Present SVID Present
	Platform IMON Disable This strap should be left at the recommended default setting.	ICL-YN ICL-UN	0x0 0x0
	VCCIN Aux Present **Values: Yes/No** This setting determines if VCC Aux exists as a separate VR.	ICL-YN ICL-UN	No No
	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.	ICL-YN ICL-UN	0x0 0x0
	VCC SVID VR Type **Values: SVID/Fixed VR** This setting determines the VCC IN SVID VR Type. See Processor EDS for details.	ICL-YN ICL-UN	SVID SVID
	VCC SFR OC PG Present **Values: Yes/No** This setting determines if VCC SFR OC PG is present on the platform.	ICL-YN ICL-UN	No No
	VCC ST PG Present **Values: Yes/No** This setting determines if VCC ST PG is present on the platform.	ICL-YN ICL-UN	No No
	VCC STG PG Present **Values: Yes/No** This setting determines if VCC STG PG is present on the platform.	ICL-YN ICL-UN	No No
	VCCIN Aux Level LP **Values: 1.8v/1.65v** This setting determines the VCCIN Aux Level LP Voltage. ***Note:*** On Y based MCPs this setting can be configured to 1.65v. On all other MCP types set to 1.8v	ICL-YN ICL-UN	1.65v or 1.8v 1.8v

Table 2-15. - Flex I/O Straps (Sheet 1 of 14)

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

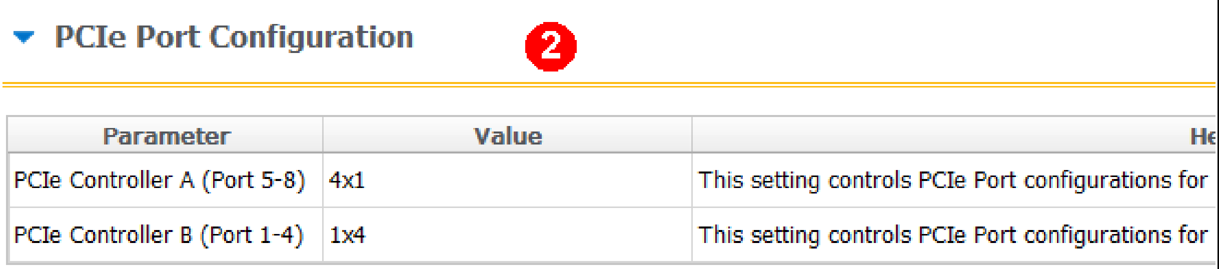


PCIe Lane Reversal Configuration ①

Parameter	Value	He
PCIe Controller A Lane Reversal Enabled	No	This setting allows the PCIe lanes on Contr
PCIe Controller B Lane Reversal Enabled	Yes	This setting allows the PCIe lanes on Contr

#	Parameter	Platform	Settings
①	**Flex I/O - PCIe Lane Reversal Configuration**		
	PCIe Controller A Lane Reversal Enabled **Values: Yes/ No** - This setting allows the PCIe lanes on Controller A to be reversed. **Note:** Refer to EDS for PCIe supported port configurations.	ICL-YN ICL-UN	No No
	PCIe Controller B Lane Reversal Enabled **Values: Yes/ No** - This setting allows the PCIe lanes on Controller B to be reversed. **Note:** Refer to EDS for PCIe supported port configurations.	ICL-YN ICL-UN	Yes Yes

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



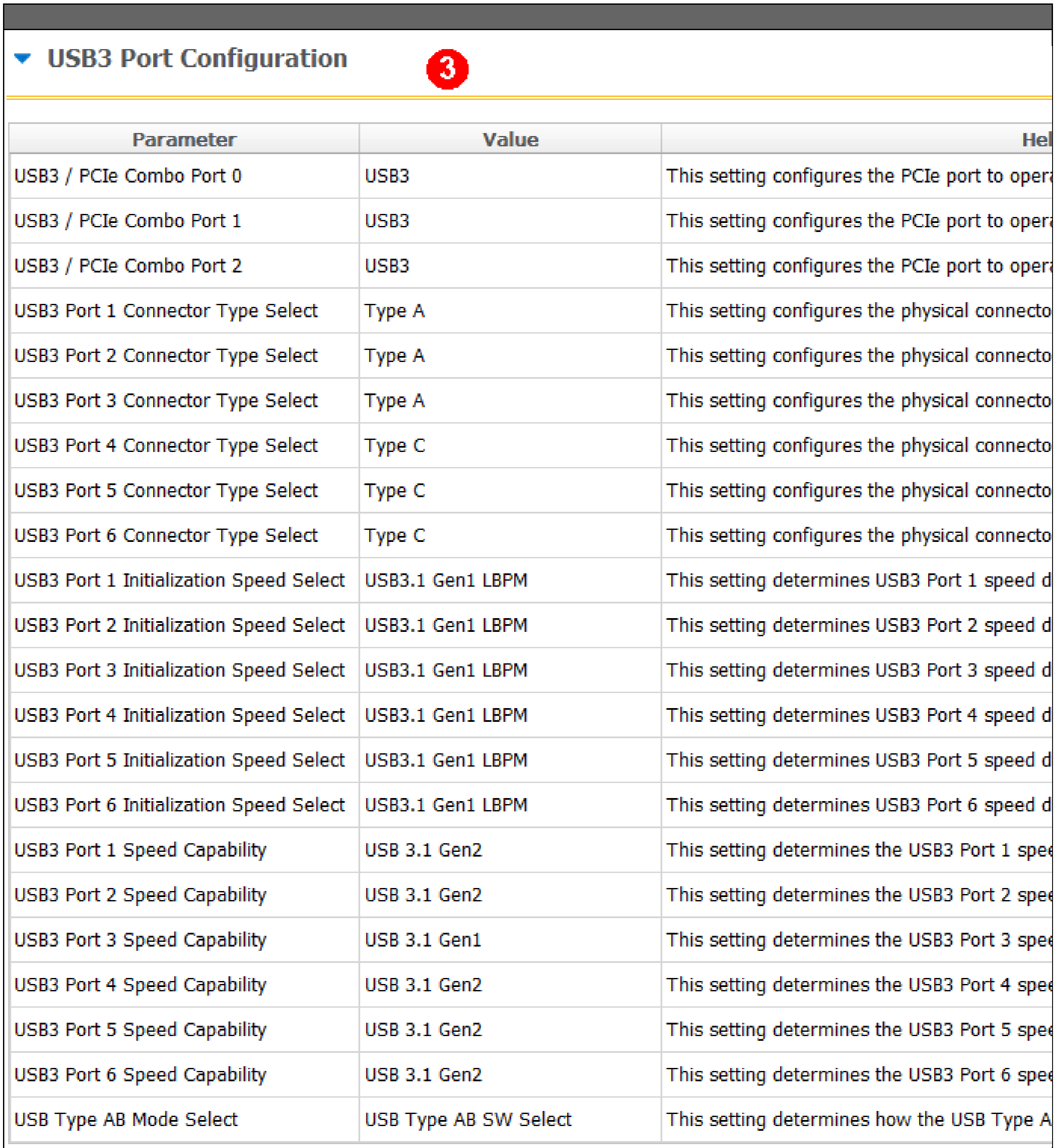
PCIe Port Configuration ②

Parameter	Value	He
PCIe Controller A (Port 5-8)	4x1	This setting controls PCIe Port configurations for
PCIe Controller B (Port 1-4)	1x4	This setting controls PCIe Port configurations for

#	Parameter	Platform	Settings
②	**Flex I/O - PCIe Port Configuration**		
	PCIe Controller A (Port 5-8) **Values: 4x1, (1x2, 2x1), 2x2** - This setting controls PCIe Port configurations for PCIe Controller 1. For further details see Ice Lake LP Platform Controller Hub EDS.	ICL-YN ICL-UN	4x1 4x1
	PCIe Controller B (Port 1-4) **Values: 4x1, (1x2, 2x1), 2x2, 1x4** - This setting controls PCIe Port configurations for PCIe Controller 2. For further details see Ice Lake LP Platform Controller Hub EDS.	ICL-YN ICL-UN	1x4 1x4

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

Table 2-15. - Flex I/O Straps (Sheet 2 of 14)



USB3 Port Configuration

Parameter	Value	Hel
USB3 / PCIe Combo Port 0	USB3	This setting configures the PCIe port to opera
USB3 / PCIe Combo Port 1	USB3	This setting configures the PCIe port to opera
USB3 / PCIe Combo Port 2	USB3	This setting configures the PCIe port to opera
USB3 Port 1 Connector Type Select	Type A	This setting configures the physical connecto
USB3 Port 2 Connector Type Select	Type A	This setting configures the physical connecto
USB3 Port 3 Connector Type Select	Type A	This setting configures the physical connecto
USB3 Port 4 Connector Type Select	Type C	This setting configures the physical connecto
USB3 Port 5 Connector Type Select	Type C	This setting configures the physical connecto
USB3 Port 6 Connector Type Select	Type C	This setting configures the physical connecto
USB3 Port 1 Initialization Speed Select	USB3.1 Gen1 LBPM	This setting determines USB3 Port 1 speed d
USB3 Port 2 Initialization Speed Select	USB3.1 Gen1 LBPM	This setting determines USB3 Port 2 speed d
USB3 Port 3 Initialization Speed Select	USB3.1 Gen1 LBPM	This setting determines USB3 Port 3 speed d
USB3 Port 4 Initialization Speed Select	USB3.1 Gen1 LBPM	This setting determines USB3 Port 4 speed d
USB3 Port 5 Initialization Speed Select	USB3.1 Gen1 LBPM	This setting determines USB3 Port 5 speed d
USB3 Port 6 Initialization Speed Select	USB3.1 Gen1 LBPM	This setting determines USB3 Port 6 speed d
USB3 Port 1 Speed Capability	USB 3.1 Gen2	This setting determines the USB3 Port 1 spee
USB3 Port 2 Speed Capability	USB 3.1 Gen2	This setting determines the USB3 Port 2 spee
USB3 Port 3 Speed Capability	USB 3.1 Gen1	This setting determines the USB3 Port 3 spee
USB3 Port 4 Speed Capability	USB 3.1 Gen2	This setting determines the USB3 Port 4 spee
USB3 Port 5 Speed Capability	USB 3.1 Gen2	This setting determines the USB3 Port 5 spee
USB3 Port 6 Speed Capability	USB 3.1 Gen2	This setting determines the USB3 Port 6 spee
USB Type AB Mode Select	USB Type AB SW Select	This setting determines how the USB Type A

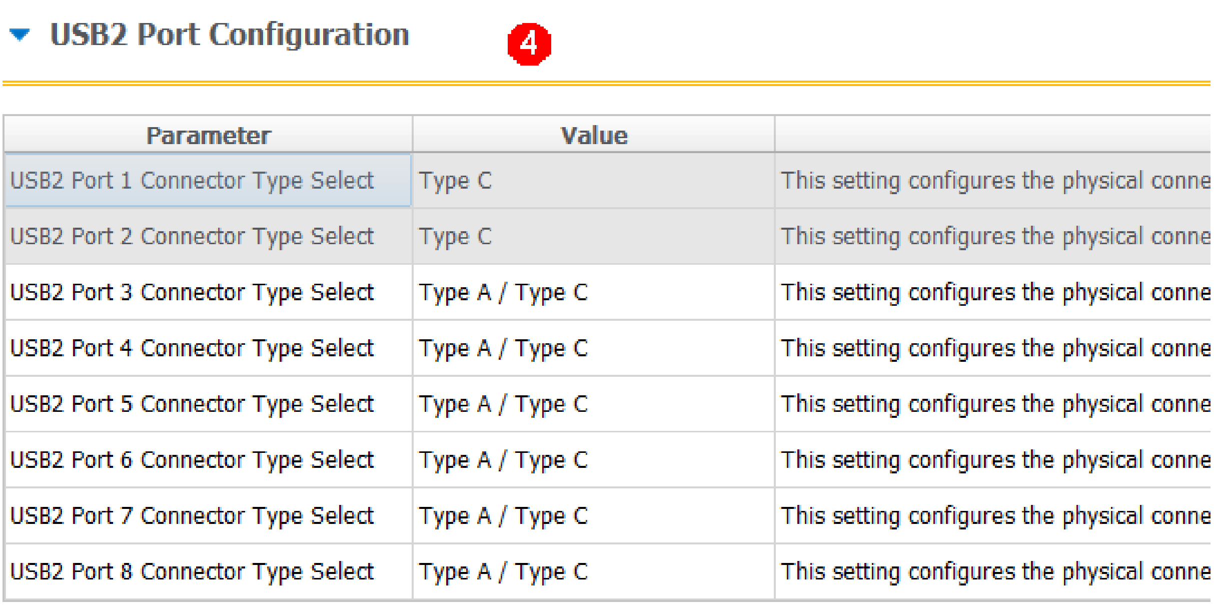
#	Parameter	Platform	Settings
③	**Flex I/O - USB3 Port Configuration**		

Table 2-15. - Flex I/O Straps (Sheet 3 of 14)

	USB3 / PCIe Combo Port 0 **Values: PCIe (or GbE), USB3 -** This setting configures the PCIe port to operate as either: PCIe Port 4 or USB3 Port 4 For further details on Flex I/O see Ice Lake LP Platform Controller Hub EDS. ***Note:*** If DCI BSSB for this USB3 Combo port it will be Grayed out.	ICL-YN ICL-UN	USB3 USB3
	USB3 / PCIe Combo Port 1 **Values: PCIe (or GbE), USB3 -** This setting configures the PCIe port to operate as either: PCIe Port 5 or USB3 Port 5 For further details on Flex I/O see Ice Lake LP Platform Controller Hub EDS. ***Note:*** If DCI BSSB for this USB3 Combo port it will be Grayed out.	ICL-YN ICL-UN	USB3 USB3
	USB3 / PCIe Combo Port 2 **Values: PCIe (or GbE), USB3** - This setting configures the PCIe port to operate as either: PCIe Port 6 or USB3 Port 6 For further details on Flex I/O see Ice Lake LP Platform Controller Hub EDS. ***Note:*** If DCI BSSB for this USB3 Combo port it will be Grayed out.	ICL-YN ICL-UN	USB3 USB3
	USB3 Port 1 Connector Type Select This setting configures the physical connector type to be used for USB 3.1 Port 1.	ICL-YN ICL-UN	Type-A Type-A
	USB3 Port 2 Connector Type Select This setting configures the physical connector type to be used for USB 3.1 Port 2.	ICL-YN ICL-UN	Type-A Type-A
	USB3 Port 3 Connector Type Select This setting configures the physical connector type to be used for USB 3.1 Port 3.	ICL-YN ICL-UN	Type-A Type-A
	USB3 Port 4 Connector Type Select This setting configures the physical connector type to be used for USB 3.1 Port 4.	ICL-YN ICL-UN	Type-A Type-A
	USB3 Port 5 Connector Type Select This setting configures the physical connector type to be used for USB 3.1 Port 5.	ICL-YN ICL-UN	Type-A Type-A
	USB3 Port 6 Connector Type Select This setting configures the physical connector type to be used for USB 3.1 Port 6.	ICL-YN ICL-UN	Type-A Type-A
	USB3 Port 1 Initialization Speed Select This setting determines USB3 Port 1 speed during platform power-up.	ICL-YN ICL-UN	USB3.1 Gen1 LBPM USB3.1 Gen1 LBPM
	USB3 Port 2 Initialization Speed Select This setting determines USB3 Port 2 speed during platform power-up.	ICL-YN ICL-UN	USB3.1 Gen1 LBPM USB3.1 Gen1 LBPM
	USB3 Port 3 Initialization Speed Select This setting determines USB3 Port 3 speed during platform power-up.	ICL-YN ICL-UN	USB3.1 Gen1 LBPM USB3.1 Gen1 LBPM
	USB3 Port 4 Initialization Speed Select This setting determines USB3 Port 4 speed during platform power-up.	ICL-YN ICL-UN	USB3.1 Gen1 LBPM USB3.1 Gen1 LBPM
	USB3 Port 5 Initialization Speed Select This setting determines USB3 Port 5 speed during platform power-up.	ICL-YN ICL-UN	USB3.1 Gen1 LBPM USB3.1 Gen1 LBPM
	USB3 Port 6 Initialization Speed Select This setting determines USB3 Port 6 speed during platform power-up.	ICL-YN ICL-UN	USB3.1 Gen1 LBPM USB3.1 Gen1 LBPM
	USB3 Port 1 Speed Capability This setting determines the USB3 Port 1 speed capabilities.	ICL-YN ICL-UN	USB 3.1 Gen2 USB 3.1 Gen2
	USB3 Port 2 Speed Capability This setting determines the USB3 Port 2 speed capabilities.	ICL-YN ICL-UN	USB 3.1 Gen2 USB 3.1 Gen2
	USB3 Port 3 Speed Capability This setting determines the USB3 Port 3 speed capabilities.	ICL-YN ICL-UN	USB 3.1 Gen2 USB 3.1 Gen2
	USB3 Port 4 Speed Capability This setting determines the USB3 Port 4 speed capabilities.	ICL-YN ICL-UN	USB 3.1 Gen2 USB 3.1 Gen2
	USB3 Port 5 Speed Capability This setting determines the USB3 Port 5 speed capabilities.	ICL-YN ICL-UN	USB 3.1 Gen2 USB 3.1 Gen2
	USB3 Port 6 Speed Capability This setting determines the USB3 Port 6 speed capabilities.	ICL-YN ICL-UN	USB 3.1 Gen2 USB 3.1 Gen2

Table 2-15. - Flex I/O Straps (Sheet 4 of 14)

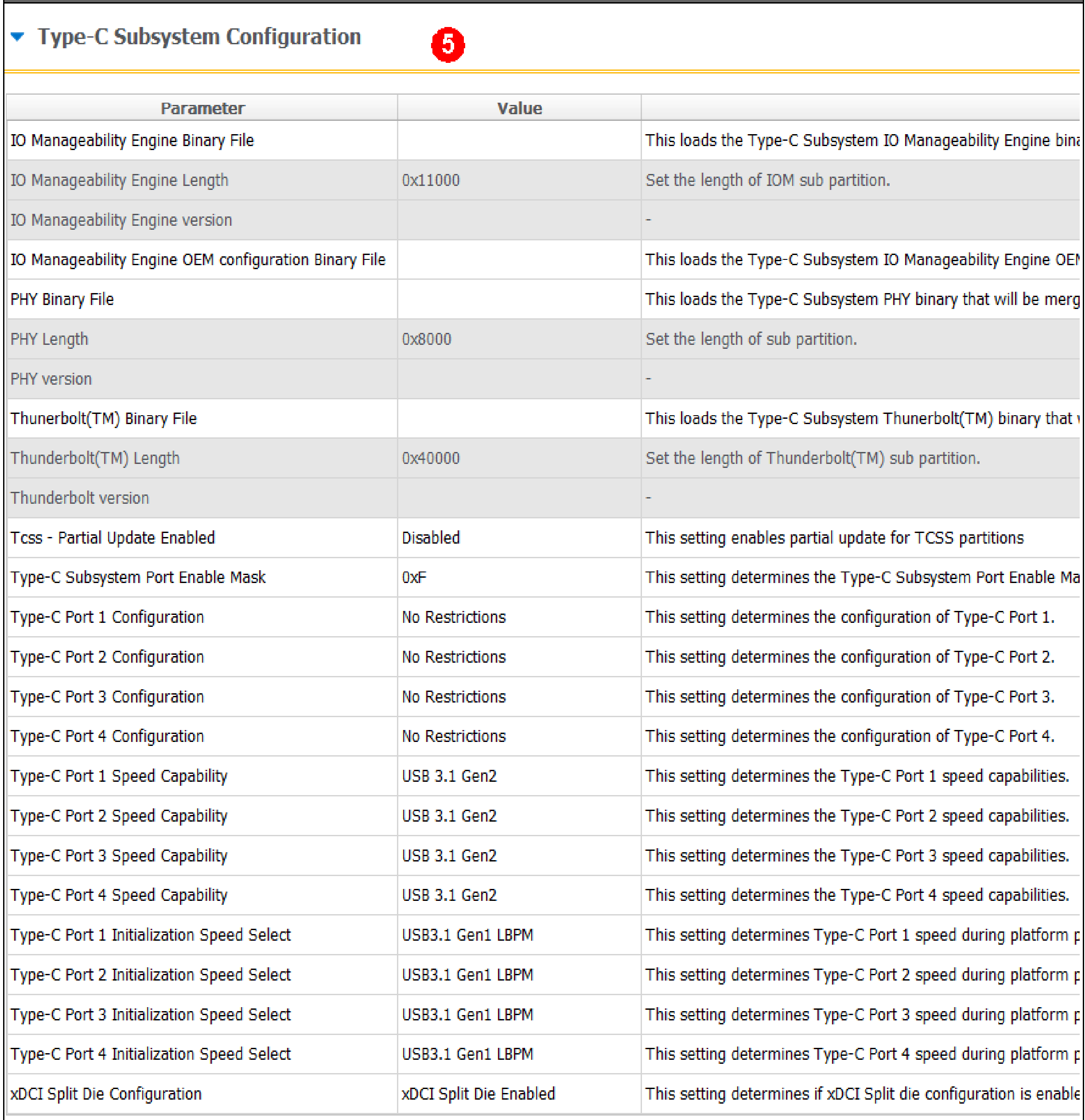
	USB Type AB Mode Select This setting determines how the USB Type AB connector switching is handled.	ICL-YN ICL-UN	USB Type AB SW Select USB Type AB SW Select
Click on Flex I/O in the left tabs menu> USB2 Port Configuration is expanded by default:			



Parameter	Value	
USB2 Port 1 Connector Type Select	Type C	This setting configures the physical conne
USB2 Port 2 Connector Type Select	Type C	This setting configures the physical conne
USB2 Port 3 Connector Type Select	Type A / Type C	This setting configures the physical conne
USB2 Port 4 Connector Type Select	Type A / Type C	This setting configures the physical conne
USB2 Port 5 Connector Type Select	Type A / Type C	This setting configures the physical conne
USB2 Port 6 Connector Type Select	Type A / Type C	This setting configures the physical conne
USB2 Port 7 Connector Type Select	Type A / Type C	This setting configures the physical conne
USB2 Port 8 Connector Type Select	Type A / Type C	This setting configures the physical conne

#	Parameter	Platform	Settings
④	**Flex I/O - USB2 Port Configuration**		
	USB2 Port 1 Connector Type This setting configures the physical connector type to be used for USB2 Port 1.	ICL-YN ICL-UN	Type-A Type-A
	USB2 Port 2 Connector Type This setting configures the physical connector type to be used for USB2 Port 2.	ICL-YN ICL-UN	Express Card / M.2 S2 Express Card / M.2 S2
	USB2 Port 3 Connector Type This setting configures the physical connector type to be used for USB2 Port 3.	ICL-YN ICL-UN	Express Card / M.2 S2 Express Card / M.2 S2
	USB2 Port 4 Connector Type This setting configures the physical connector type to be used for USB2 Port 4.	ICL-YN ICL-UN	Type-C Type-C
	USB2 Port 5 Connector Type This setting configures the physical connector type to be used for USB2 Port 5.	ICL-YN ICL-UN	Type-C Type-C
	USB2 Port 6 Connector Type This setting configures the physical connector type to be used for USB2 Port 6.	ICL-YN ICL-UN	Type-C Type-C
	USB2 Port 7 Connector Type This setting configures the physical connector type to be used for USB2 Port 7.	ICL-YN ICL-UN	Type-A / Type-C Type-C
	USB2 Port 8 Connector Type This setting configures the physical connector type to be used for USB2 Port 8.	ICL-YN ICL-UN	Type-A / Type-C Type-A / Type-C
Click on Flex I/O in the left tabs menu> Type-C Subsystem Configuration is expanded by default:			

Table 2-15. - Flex I/O Straps (Sheet 5 of 14)



Type-C Subsystem Configuration ⑤

Parameter	Value	
IO Manageability Engine Binary File		This loads the Type-C Subsystem IO Manageability Engine bina
IO Manageability Engine Length	0x11000	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 OE
PHY Binary File		This loads the Type-C Subsystem PHY binary that will be merg
PHY Length	0x8000	Set the length of sub partition.
PHY version		-
Thunerbolt(TM) Binary File		This loads the Type-C Subsystem Thunerbolt(TM) binary that
Thunderbolt(TM) Length	0x40000	Set the length of Thunderbolt(TM) sub partition.
Thunderbolt 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 Enable Ma
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 capabilities.
Type-C Port 2 Speed Capability	USB 3.1 Gen2	This setting determines the Type-C Port 2 speed capabilities.
Type-C Port 3 Speed Capability	USB 3.1 Gen2	This setting determines the Type-C Port 3 speed capabilities.
Type-C Port 4 Speed Capability	USB 3.1 Gen2	This setting determines the Type-C Port 4 speed capabilities.
Type-C Port 1 Initialization Speed Select	USB3.1 Gen1 LBPM	This setting determines Type-C Port 1 speed during platform p
Type-C Port 2 Initialization Speed Select	USB3.1 Gen1 LBPM	This setting determines Type-C Port 2 speed during platform p
Type-C Port 3 Initialization Speed Select	USB3.1 Gen1 LBPM	This setting determines Type-C Port 3 speed during platform p
Type-C Port 4 Initialization Speed Select	USB3.1 Gen1 LBPM	This setting determines Type-C Port 4 speed during platform p
xDCI Split Die Configuration	xDCI Split Die Enabled	This setting determines if xDCI Split die configuration is enable

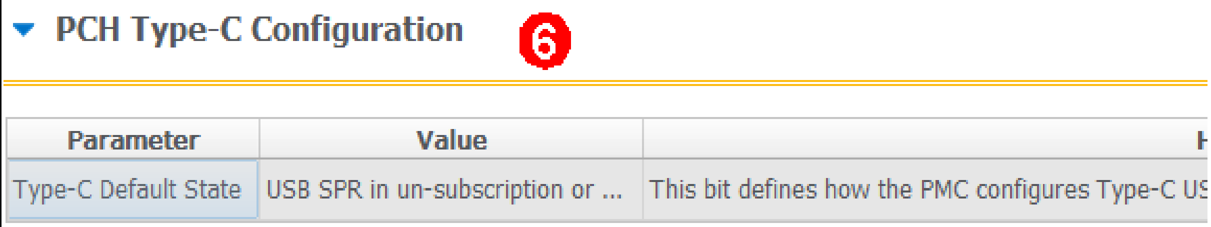
#	Parameter	Platform	Settings
⑤	**Type-C Subsystem Configuration**		
	IO Manageability Engine Binary File - This loads the IO Manageability binary that will be merged into the output image generated by the Intel® FIT.	ICL-YN ICL-UN	IOM Binary IOM Binary
	IO Manageability Engine Length		
	IO Manageability Engine version		

Table 2-15. - Flex I/O Straps (Sheet 6 of 14)

	IO Manageability Engine OEM configuration Binary File - This loads the Type-C Subsystem IO Manageability Engine OEM Configuration binary that will be written to the OEM config data section.	ICL-Y ICL-U	OEM Config Binary OEM Config Binary
	PHY Binary File - This loads the PHY binary that will be merged into the output image generated by the Intel® FIT.	ICL-YN ICL-UN	MG PHY Binary MG PHY Binary
	PHY Length		
	PHY Version		
	Thunderbolt$^{(TM)}$ Binary File **Values: Yes/No** This setting enables Anti-Roll back for the Type-C Subsystem Thunderbolt$^{(TM)}$ binary.	ICL-YN ICL-UN	TBT Binary TBT Binary
	Thunderbolt$^{(TM)}$ Length		
	Thunderbolt$^{(TM)}$ Version		
	Tcss - Partial Update Enabled **Values: Enabled/Disabled** This setting enabled partial firmware update of the TCSS partitions.	ICL-YN ICL-UN	Disabled Disabled
	Type-C Subsystem Port Enable Mask This setting determines the Type-C Subsystem Port Enable Mask	ICL-YN ICL-UN	0x3F 0x3F
	Type-C Subsystem Authentication Enabled **Values: Yes/No** This setting enables / disables firmware authentication for the Type-C Subsystem on power-up.	ICL-YN ICL-UN	Yes Yes
	Type-C Port 1 Configuration **Value: No Restrictions/DP Fixed Connection/No Thunderbolt** This setting determines the configuration for Type-C Port 1	ICL-YN ICL-UN	No Restrictions 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	ICL-YN ICL-UN	No Restrictions 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	ICL-YN ICL-UN	No Restrictions 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	ICL-YN ICL-UN	No Restrictions No Restrictions
	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	ICL-YN ICL-UN	USB 3.1 Gen2 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	ICL-YN ICL-UN	USB 3.1 Gen2 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	ICL-YN ICL-UN	USB 3.1 Gen2 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	ICL-YN ICL-UN	USB 3.1 Gen2 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.	ICL-YN ICL-UN	USB3.1 Gen1 LBPM 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.	ICL-YN ICL-UN	USB3.1 Gen1 LBPM 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.	ICL-YN ICL-UN	USB3.1 Gen1 LBPM USB3.1 Gen1 LBPM

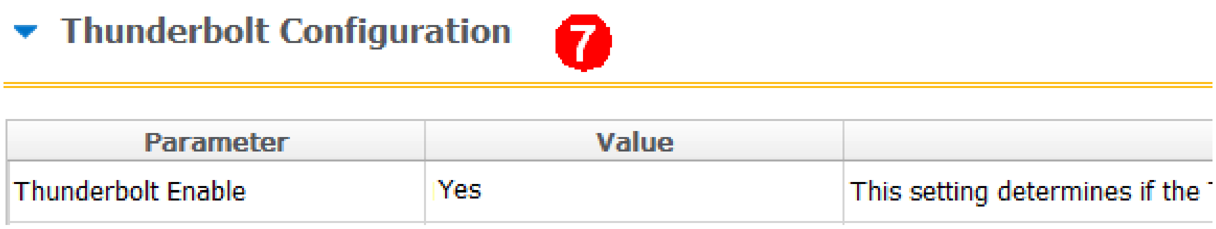
Table 2-15. - Flex I/O Straps (Sheet 7 of 14)

	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.	ICL-YN ICL-UN	USB3.1 Gen1 LBPM USB3.1 Gen1 LBPM
	xDCI Split Die Configuration **Values: xDCI Split Die Enabled / xDCI Split Die Disabled** This setting determines if xDCI Split Die Configuration is enabled / disabled on the platform.	ICL-YN ICL-UN	xDCI Split Die Enabled xDCI Split Die Enabled
Click on Flex I/O in the left tabs menu> PCH Type-C Configuration is expanded by default:			


PCH Type-C Configuration ⑥

Parameter	Value	
Type-C Default State	USB SPR in un-subscription or ...	This bit defines how the PMC configures Type-C U

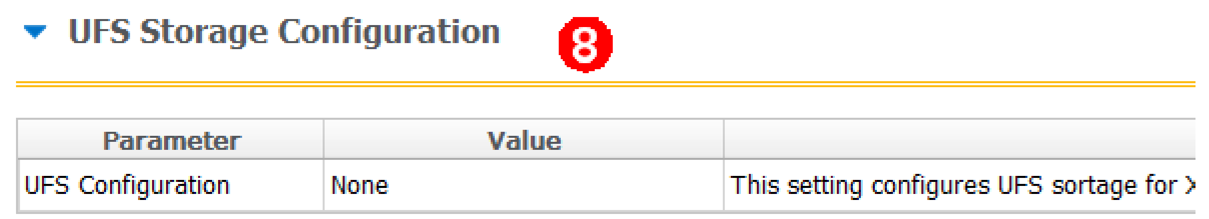
#	Parameter	Platform	Settings
⑥	**PCH Type-C Configuration**		
	Type-C Default State **Values: USB SPR in un-subscription or disconnected state by default / USB SPR in host subscription state by default** This bit defines how the PMC configures Type-C USB3 / USB2 SPR. ***Note:*** This setting will be greyed out when the PD Controller Type-C Port Enabled settings are set to 'Yes'.	ICL-YN ICL-UN	USB SPR in un-subscription or disconnected state by default USB SPR in un-subscription or disconnected state by default
Click on Flex I/O in the left tabs menu> Thunderbolt Configuration is expanded by default:			


Thunderbolt Configuration ⑦

Parameter	Value	
Thunderbolt Enable	Yes	This setting determines if the

#	Parameter	Platform	Settings
⑦	**Thunderbolt Configuration**		
	Thunderbolt Enable **Values: Yes/No** This setting determines if the Thunderbolt(tm) interface is enabled on the platform.	ICL-YN ICL-UN	Yes Yes
Click on Flex I/O in the left tabs menu> UFS Storage Configuration is expanded by default:			

Table 2-15. - Flex I/O Straps (Sheet 8 of 14)

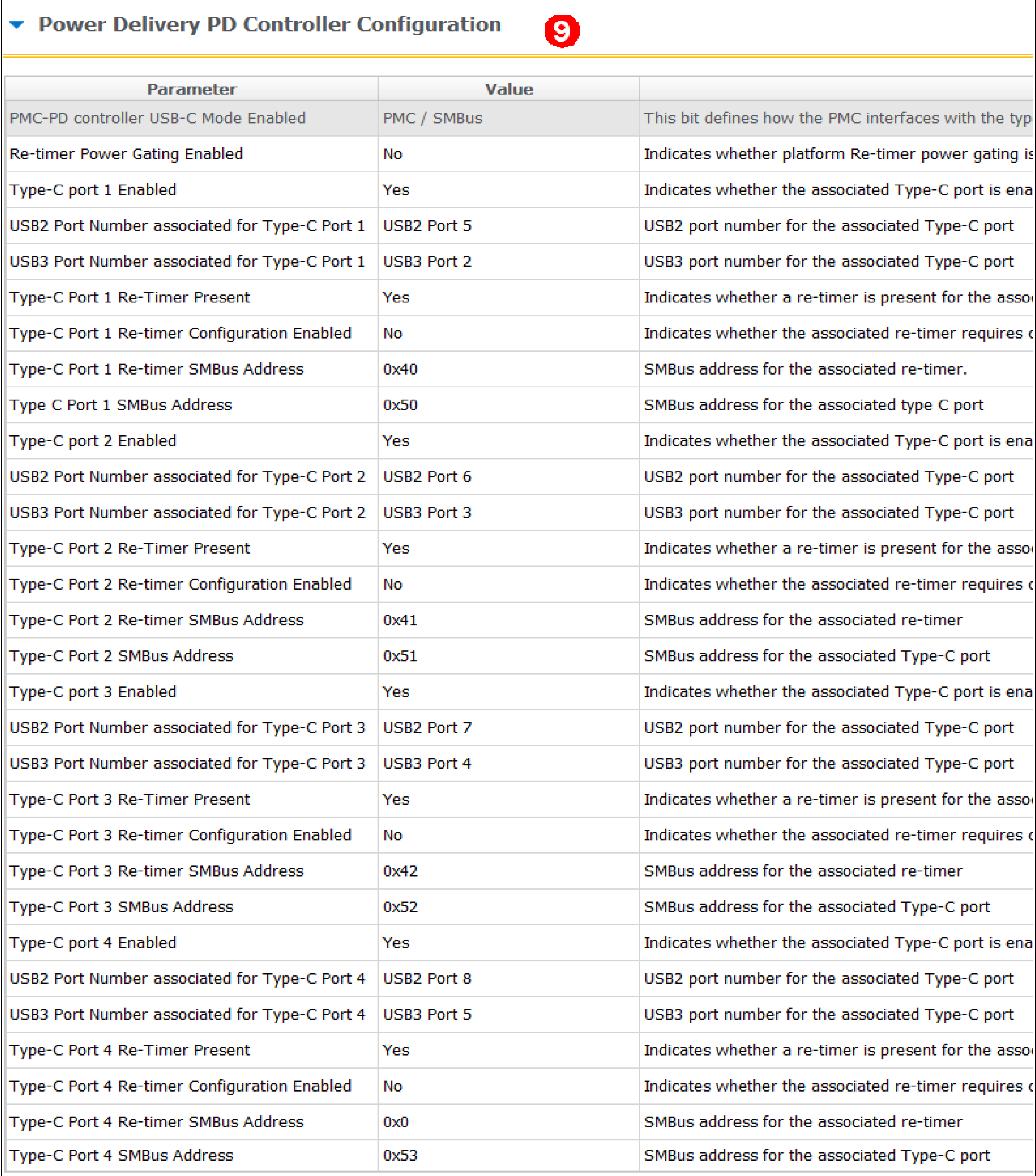


UFS Storage Configuration 8

Parameter	Value	
UFS Configuration	None	This setting configures UFS sortage for >

#	Parameter	Platform	Settings
8	**UFS Storage Configuration**		
	UFS Configuration **Leave settings at Intel® FIT default values**	ICL-YN ICL-UN	None None
Click on Flex I/O in the left tabs menu> Power Delivery PD Controller Configuration is expanded by default:			

Table 2-15. - Flex I/O Straps (Sheet 9 of 14)



Power Delivery PD Controller Configuration ⑨

Parameter	Value	
PMC-PD controller USB-C Mode Enabled	PMC / SMBus	This bit defines how the PMC interfaces with the typ
Re-timer Power Gating Enabled	No	Indicates whether platform Re-timer power gating is
Type-C port 1 Enabled	Yes	Indicates whether the associated Type-C port is ena
USB2 Port Number associated for Type-C Port 1	USB2 Port 5	USB2 port number for the associated Type-C port
USB3 Port Number associated for Type-C Port 1	USB3 Port 2	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 asso
Type-C Port 1 Re-timer Configuration Enabled	No	Indicates whether the associated re-timer requires
Type-C Port 1 Re-timer SMBus Address	0x40	SMBus address for the associated re-timer.
Type C Port 1 SMBus Address	0x50	SMBus address for the associated type C port
Type-C port 2 Enabled	Yes	Indicates whether the associated Type-C port is ena
USB2 Port Number associated for Type-C Port 2	USB2 Port 6	USB2 port number for the associated Type-C port
USB3 Port Number associated for Type-C Port 2	USB3 Port 3	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 asso
Type-C Port 2 Re-timer Configuration Enabled	No	Indicates whether the associated re-timer requires
Type-C Port 2 Re-timer SMBus Address	0x41	SMBus address for the associated re-timer
Type-C Port 2 SMBus Address	0x51	SMBus address for the associated Type-C port
Type-C port 3 Enabled	Yes	Indicates whether the associated Type-C port is ena
USB2 Port Number associated for Type-C Port 3	USB2 Port 7	USB2 port number for the associated Type-C port
USB3 Port Number associated for Type-C Port 3	USB3 Port 4	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 asso
Type-C Port 3 Re-timer Configuration Enabled	No	Indicates whether the associated re-timer requires
Type-C Port 3 Re-timer SMBus Address	0x42	SMBus address for the associated re-timer
Type-C Port 3 SMBus Address	0x52	SMBus address for the associated Type-C port
Type-C port 4 Enabled	Yes	Indicates whether the associated Type-C port is ena
USB2 Port Number associated for Type-C Port 4	USB2 Port 8	USB2 port number for the associated Type-C port
USB3 Port Number associated for Type-C Port 4	USB3 Port 5	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 asso
Type-C Port 4 Re-timer Configuration Enabled	No	Indicates whether the associated re-timer requires
Type-C Port 4 Re-timer SMBus Address	0x0	SMBus address for the associated re-timer
Type-C Port 4 SMBus Address	0x53	SMBus address for the associated Type-C port

⑨	**Power Delivery PD Controller Configuration**		

Table 2-15. - Flex I/O Straps (Sheet 10 of 14)

	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.	ICL-YN ICL-UN	PMC / SMBus PMC / SMBus
	Re-timer Power Gating Enabled **Values: Yes / No** This setting indicates whether platform Re-timer power gating is enabled.	ICL-YN ICL-UN	No 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.	ICL-YN ICL-UN	Yes 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)	ICL-YN ICL-UN	USB2 Port 1 USB2 Port 1
	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)	ICL-YN ICL-UN	Type-C Port 1 Type-C Port 1
	Type-C Port 1 Re-timer Present **Values: Yes / No** This indicates whether a re-timer is present for the associated Type-C port.	ICL-YN ICL-UN	Yes Yes

Table 2-15. - Flex I/O Straps (Sheet 11 of 14)

	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.	ICL-YN ICL-UN	No No
	Type-C Port 1 Re-timer SMBus Address **Value: Hex** This indicates the SMBus address for the associated re-timer.	ICL-YN ICL-UN	0x38 0x38
	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.	ICL-YN ICL-UN	0x38 0x38
	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.	ICL-YN ICL-UN	Yes 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)	ICL-YN ICL-UN	USB2 Port 2 USB2 Port 2
	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)	ICL-YN ICL-UN	Type-C Port 2 Type-C 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.	ICL-YN ICL-UN	Yes Yes
	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.	ICL-YN ICL-UN	No No

Table 2-15. - Flex I/O Straps (Sheet 12 of 14)

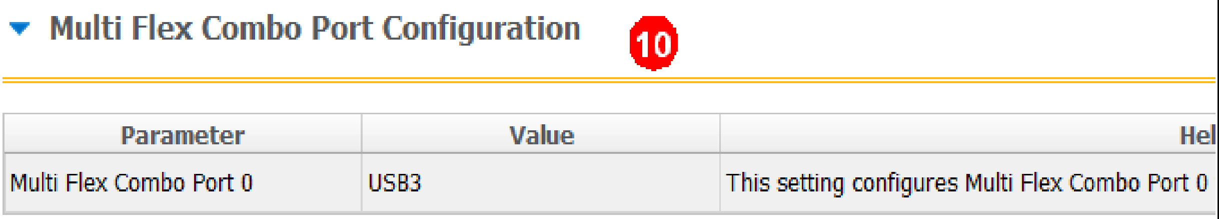
	Type-C Port 2 Re-timer SMBus Address **Value: Hex** This indicates the SMBus address for the associated re-timer.	ICL-YN ICL-UN	0x3F 0x3F
	Type-C Port 2 SMBus Address **Value: Hex** This indicates the SMBus address for the associated Type-C port. ***Note:*** OEMs are recommended to set unique SMBus address allocation for Type-C port and Re-timer associated.	ICL-YN ICL-UN	0x3F 0x3F
	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.	ICL-YN ICL-UN	No 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)	ICL-YN ICL-UN	USB2 Port 3 USB2 Port 3
	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)	ICL-YN ICL-UN	Type-C Port 3 Type-C 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.	ICL-YN ICL-UN	No 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.	ICL-YN ICL-UN	No No
	Type-C Port 3 Re-timer SMBus Address **Value: Hex** This indicates the SMBus address for the associated re-timer.	ICL-YN ICL-UN	0x42 0x3B

Table 2-15. - Flex I/O Straps (Sheet 13 of 14)

	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.	ICL-YN ICL-UN	0x21 0x3B
	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.	ICL-YN ICL-UN	No 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)	ICL-YN ICL-UN	USB2 Port 4 USB2 Port 4
	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)	ICL-YN ICL-UN	Type-C Port 4 Type-C 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.	ICL-YN ICL-UN	No 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.	ICL-YN ICL-UN	No No
	Type-C Port 4 Re-timer SMBus Address **Value: Hex** This indicates the SMBus address for the associated re-timer.	ICL-YN ICL-UN	0x43 0x3C
	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.	ICL-YN ICL-UN	0x53 0x3C

Table 2-15. - Flex I/O Straps (Sheet 14 of 14)

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



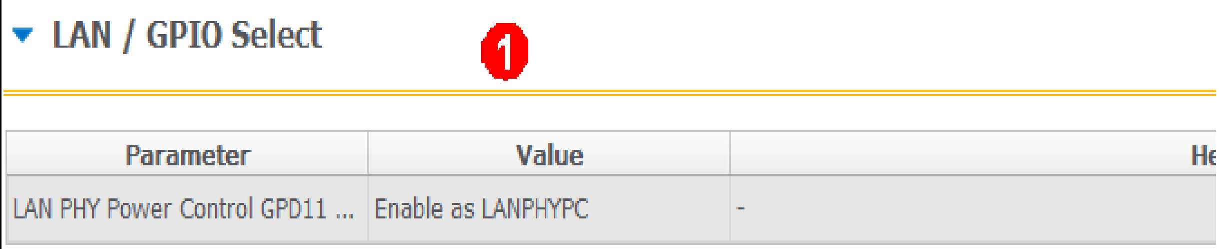
Multi Flex Combo Port Configuration 10

Parameter	Value	Hel
Multi Flex Combo Port 0	USB3	This setting configures Multi Flex Combo Port 0

#	Parameter	Platform	Settings
10	**Multi Flex Combo Port**		
	Multi Flex Combo Port 0 **Values: USB3/PCIe** This setting configures Multi Flex Combo Port 0 to operates as either USB3 Port 6, PCIe Port 8, SATA 1 or UFS 1. For further details on Flex I/O see Ice Lake N Platform Controller Hub EDS. ***Note:*** This setting will be grayed out if DCI BSSB over USB3 Port6 Enabled is set to 'yes'	ICL-YN ICL-UN	USB3 USB3

Table 2-16. - GPIO (Sheet 1 of 17)

Click on GPIO in the left tabs menu> LAN / GPIO Select is expanded by default:

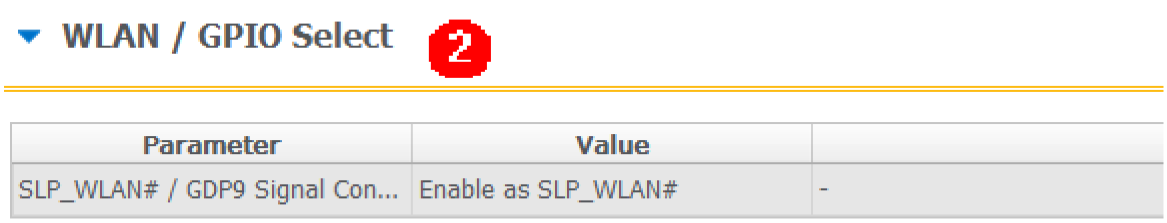


LAN / GPIO Select

Parameter	Value	He
LAN PHY Power Control GPD11 ...	Enable as LANPHYPC	-

#	Parameter	Platform	Settings
①	**GPIO - LAN / GPIO Select**		
	LAN PHY Power Control GPD11 Signal Configuration	ICL-YN ICL-UN	LANPHYPC LANPHYPC

Click on GPIO in the left tabs menu> WLAN / GPIO Select is expanded by default:

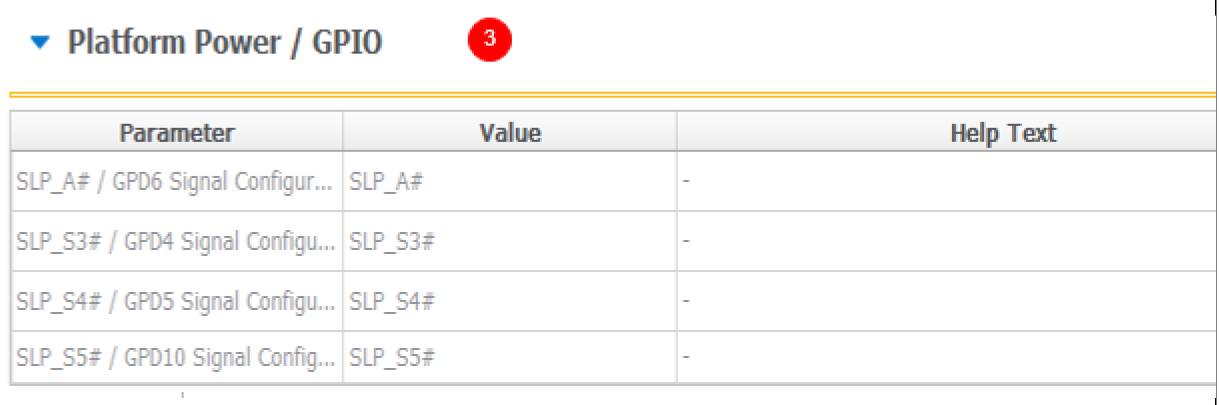


WLAN / GPIO Select

Parameter	Value	
SLP_WLAN# / GDP9 Signal Con...	Enable as SLP_WLAN#	-

#	Parameter	Platform	Settings
②	**GPIO - WLAN / GPIO Select**		
	SLP_WLAN# / GPD9 Signal Configuration	ICL-YN ICL-UN	SLP_WLAN# SLP_WLAN#

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



Platform Power / GPIO

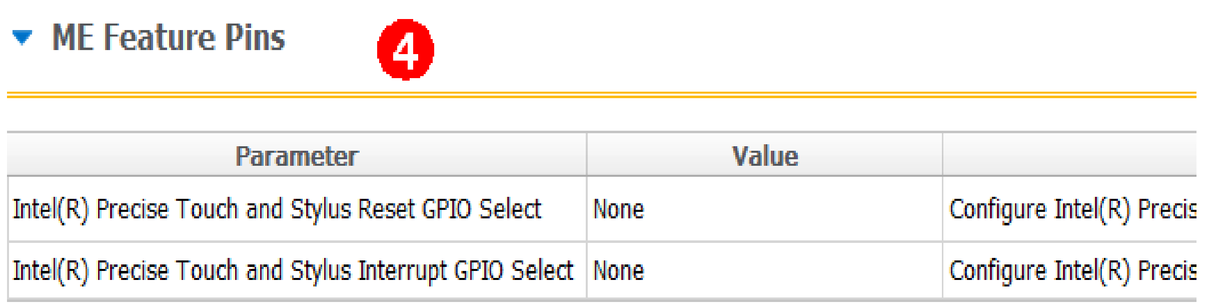
Parameter	Value	Help Text
SLP_A# / GPD6 Signal Configur...	SLP_A#	-
SLP_S3# / GPD4 Signal Configu...	SLP_S3#	-
SLP_S4# / GPD5 Signal Configu...	SLP_S4#	-
SLP_S5# / GPD10 Signal Config...	SLP_S5#	-

#	Parameter	Platform	Settings

Table 2-16. - GPIO (Sheet 2 of 17)

③	**GPIO - Platform Power / GPIO**		
	SLP_A# / GPD6 Signal Configuration	ICL-YN ICL-UN	SLP_A# SLP_A#
	SLP_S3# / GPD4 Signal Configuration	ICL-YN ICL-UN	SLP_S3# SLP_S3#
	SLP_S4# / GPD5 Signal Configuration	ICL-YN ICL-UN	SLP_S4# SLP_S4#
	SLP_S5# / GPD10 Signal Configuration	ICL-YN ICL-UN	SLP_S5# SLP_S5#

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

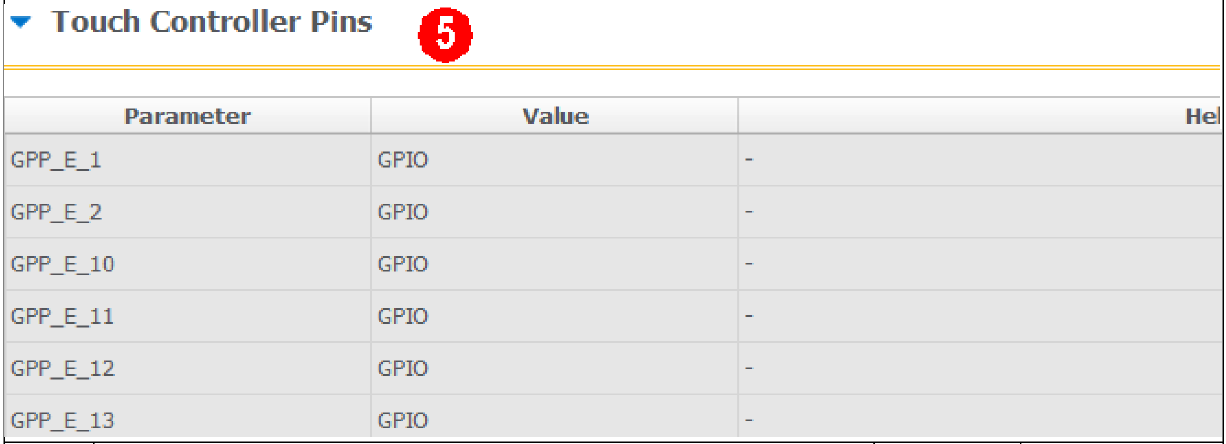


ME Feature Pins ④

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

#	Parameter	Platform	Settings
④	**GPIO - ME Feature Pins**		
	Intel® Precise Touch and Stylus Reset GPIO Select Configure Intel® Precise Touch and Stylus Reset GPIO.	ICL-YN ICL-UN	None None
	Intel® Precise Touch and Stylus Interrupt GPIO Select Configure Intel® Precise Touch and Stylus Interrupt GPIO.	ICL-YN ICL-UN	None None

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



Touch Controller Pins ⑤

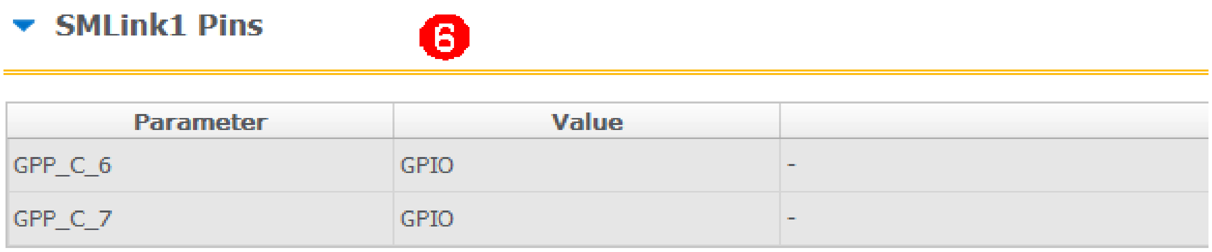
Parameter	Value	Hel
GPP_E_1	GPIO	-
GPP_E_2	GPIO	-
GPP_E_10	GPIO	-
GPP_E_11	GPIO	-
GPP_E_12	GPIO	-
GPP_E_13	GPIO	-

#	Parameter	Platform	Settings

Table 2-16. - GPIO (Sheet 3 of 17)

⑤	**GPIO - Touch Controller Pins**		
	GPP_E_1	ICL-YN ICL-UN	GPIO GPIO
	GPP_E_2	ICL-YN ICL-UN	GPIO GPIO
	GPP_E_10	ICL-YN ICL-UN	GPIO GPIO
	GPP_E_11	ICL-YN ICL-UN	GPIO GPIO
	GPP_E_12	ICL-YN ICL-UN	GPIO GPIO
	GPP_E_13	ICL-YN ICL-UN	GPIO GPIO

Click on GPIO in the left tabs menu> SMLink1 Pins is expanded by default:



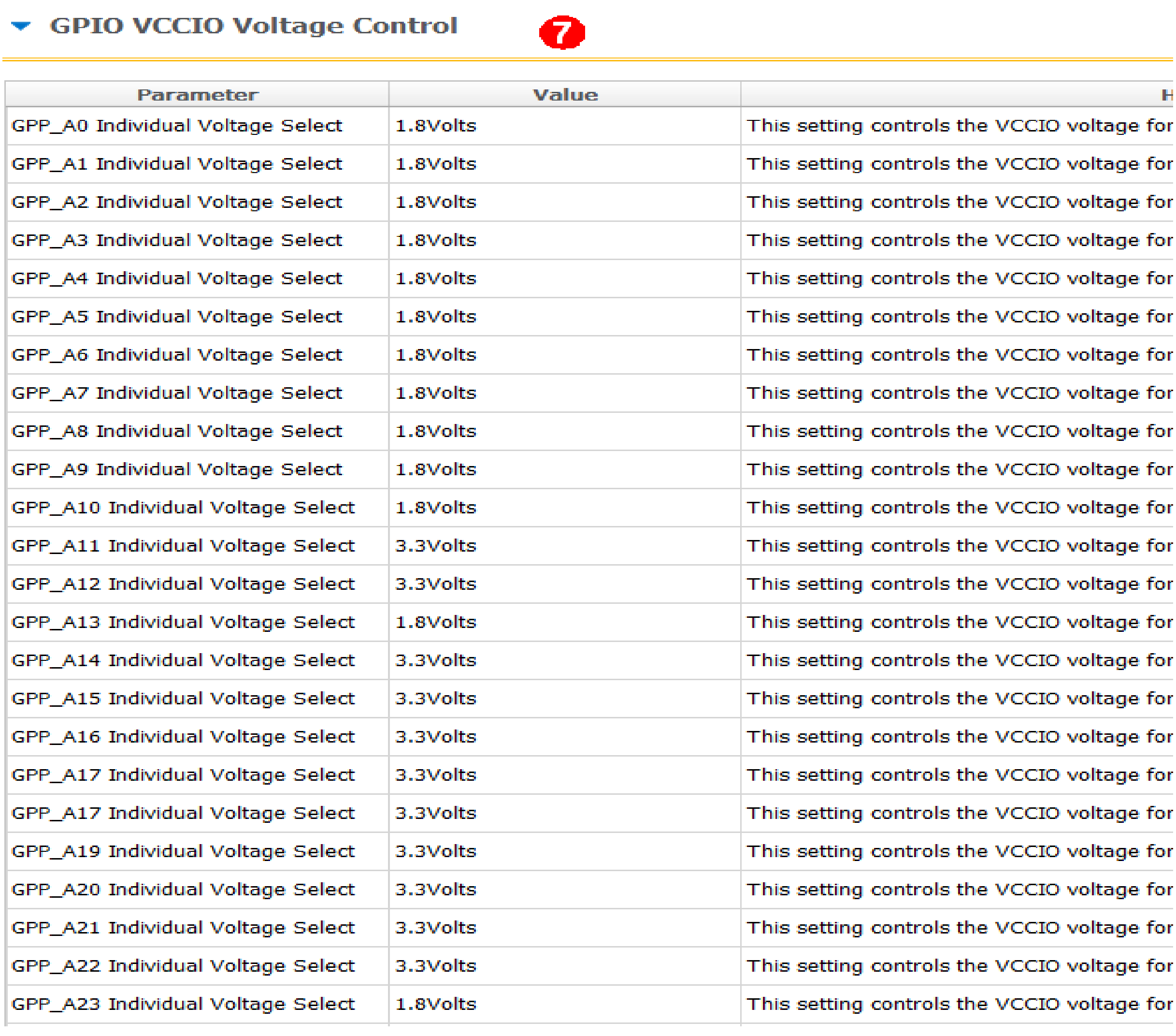
SMLink1 Pins ⑥

Parameter	Value	
GPP_C_6	GPIO	-
GPP_C_7	GPIO	-

#	Parameter	Platform	Settings
⑥	**GPIO - SMLink1 Pins**		
	GPP_C_6	ICL-YN ICL-UN	GPIO GPIO
	GPP_C_7	ICL-YN ICL-UN	GPIO GPIO

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

Table 2-16. - GPIO (Sheet 4 of 17)



GPIO VCCIO Voltage Control ⑦

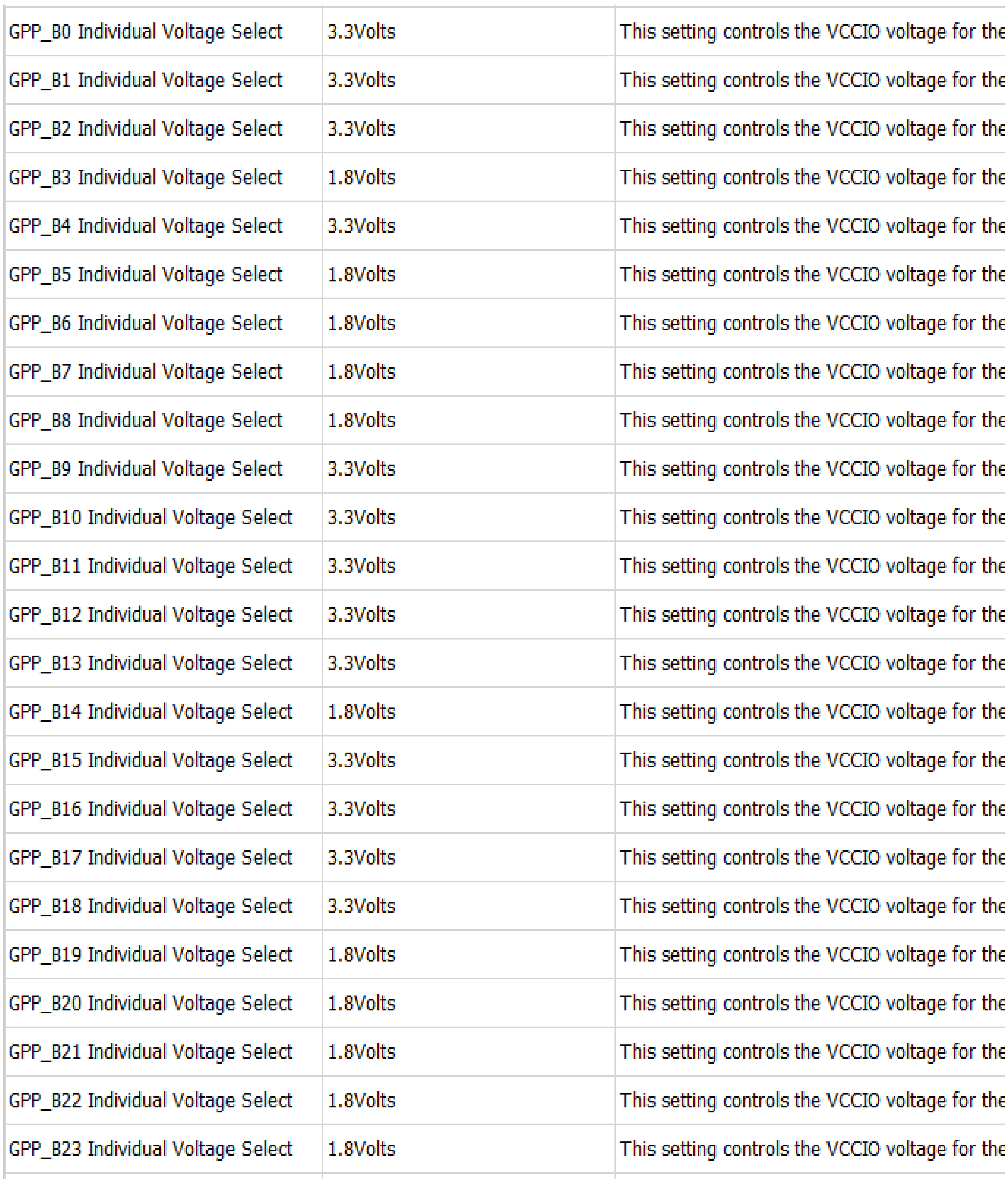
Parameter	Value	H
GPP_A0 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage for
GPP_A1 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage for
GPP_A2 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage for
GPP_A3 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage for
GPP_A4 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage for
GPP_A5 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage for
GPP_A6 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage for
GPP_A7 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage for
GPP_A8 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage for
GPP_A9 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage for
GPP_A10 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage for
GPP_A11 Individual Voltage Select	3.3Volts	This setting controls the VCCIO voltage for
GPP_A12 Individual Voltage Select	3.3Volts	This setting controls the VCCIO voltage for
GPP_A13 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage for
GPP_A14 Individual Voltage Select	3.3Volts	This setting controls the VCCIO voltage for
GPP_A15 Individual Voltage Select	3.3Volts	This setting controls the VCCIO voltage for
GPP_A16 Individual Voltage Select	3.3Volts	This setting controls the VCCIO voltage for
GPP_A17 Individual Voltage Select	3.3Volts	This setting controls the VCCIO voltage for
GPP_A17 Individual Voltage Select	3.3Volts	This setting controls the VCCIO voltage for
GPP_A19 Individual Voltage Select	3.3Volts	This setting controls the VCCIO voltage for
GPP_A20 Individual Voltage Select	3.3Volts	This setting controls the VCCIO voltage for
GPP_A21 Individual Voltage Select	3.3Volts	This setting controls the VCCIO voltage for
GPP_A22 Individual Voltage Select	3.3Volts	This setting controls the VCCIO voltage for
GPP_A23 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage for

#	Parameter	Platform	Settings
⑦	**GPIO - GPIO VCCIO Voltage Control** ***Warning:*** Incorrectly configuring GPIO voltages may result in MCP damage.		
	GPP_A0 Individual Voltage Select	ICL-YN ICL-UN	1.8 Volts 1.8 Volts
	GPP_A1 Individual Voltage Select	ICL-YN ICL-UN	1.8 Volts 1.8 Volts
	GPP_A2 Individual Voltage Select	ICL-YN ICL-UN	1.8 Volts 1.8 Volts
	GPP_A3 Individual Voltage Select	ICL-YN ICL-UN	1.8 Volts 1.8 Volts
	GPP_A4 Individual Voltage Select	ICL-YN ICL-UN	1.8 Volts 1.8 Volts

Table 2-16. - GPIO (Sheet 5 of 17)

	GPP_A5 Individual Voltage Select	ICL-YN ICL-UN	1.8 Volts 1.8 Volts
	GPP_A6 Individual Voltage Select	ICL-YN ICL-UN	1.8 Volts 1.8 Volts
	GPP_A7 Individual Voltage Select	ICL-YN ICL-UN	1.8 Volts 3.3 Volts
	GPP_A8 Individual Voltage Select	ICL-YN ICL-UN	1.8 Volts 1.8 Volts
	GPP_A9 Individual Voltage Select	ICL-YN ICL-UN	1.8 Volts 1.8 Volts
	GPP_A10 Individual Voltage Select	ICL-YN ICL-UN	1.8 Volts 1.8 Volts
	GPP_A11 Individual Voltage Select	ICL-YN ICL-UN	3.3 Volts 3.3 Volts
	GPP_A12 Individual Voltage Select	ICL-YN ICL-UN	3.3 Volts 3.3 Volts
	GPP_A13 Individual Voltage Select	ICL-YN ICL-UN	1.8 Volts 1.8 Volts
	GPP_A14 Individual Voltage Select	ICL-YN ICL-UN	3.3 Volts 3.3 Volts
	GPP_A15 Individual Voltage Select	ICL-YN ICL-UN	3.3 Volts 3.3 Volts
	GPP_A16 Individual Voltage Select	ICL-YN ICL-UN	3.3 Volts 3.3 Volts
	GPP_A17 Individual Voltage Select	ICL-YN ICL-UN	3.3 Volts 3.3 Volts
	GPP_A18 Individual Voltage Select	ICL-YN ICL-UN	3.3 Volts 3.3 Volts
	GPP_A19 Individual Voltage Select	ICL-YN ICL-UN	3.3 Volts 3.3 Volts
	GPP_A20 Individual Voltage Select	ICL-YN ICL-UN	3.3 Volts 3.3 Volts
	GPP_A21 Individual Voltage Select	ICL-YN ICL-UN	3.3 Volts 3.3 Volts
	GPP_A22 Individual Voltage Select	ICL-YN ICL-UN	3.3 Volts 3.3 Volts
	GPP_A23 Individual Voltage Select	ICL-YN ICL-UN	1.8 Volts 1.8 Volts

Table 2-16. - GPIO (Sheet 6 of 17)



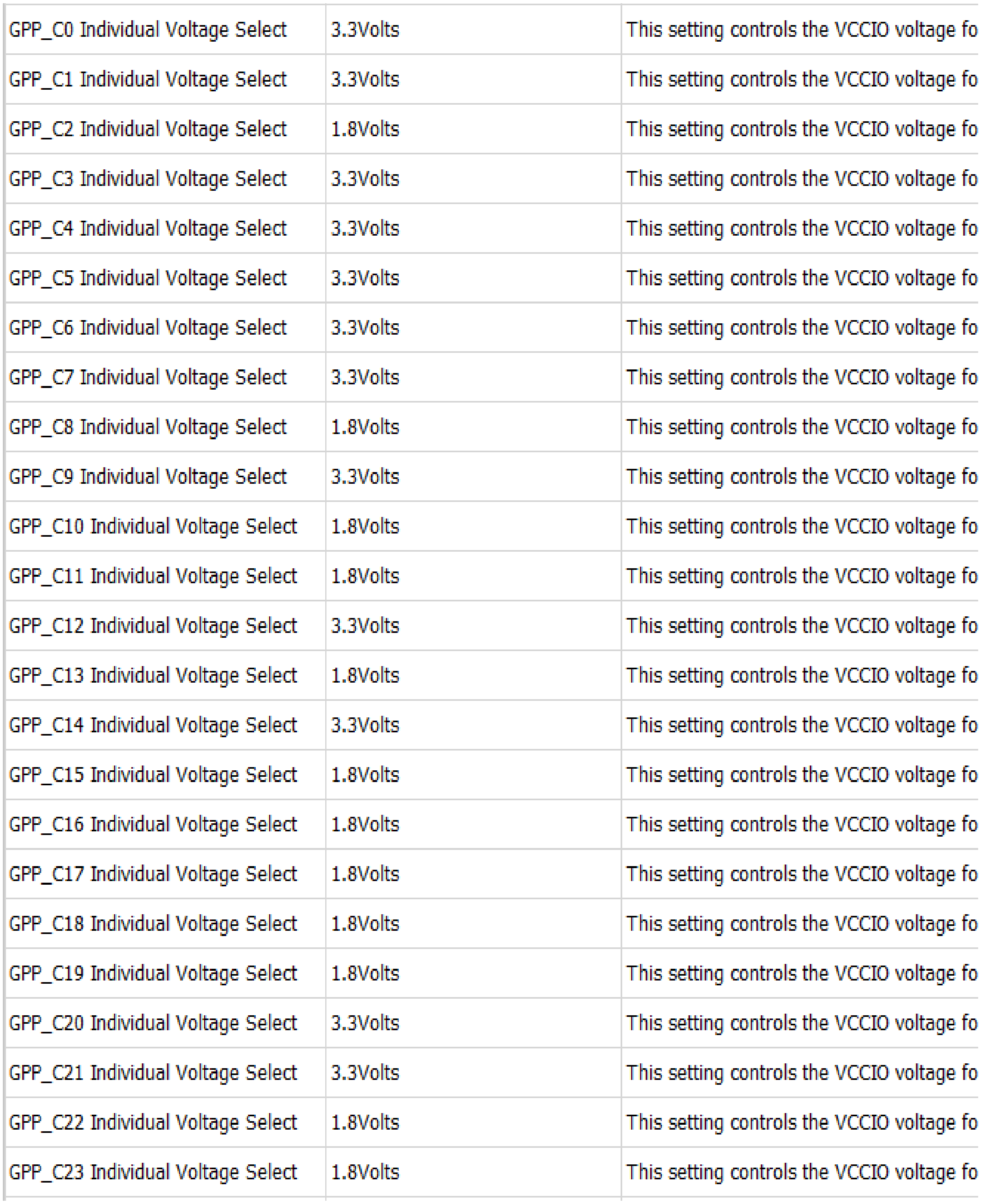
GPP_B0 Individual Voltage Select	3.3Volts	This setting controls the VCCIO voltage for the
GPP_B1 Individual Voltage Select	3.3Volts	This setting controls the VCCIO voltage for the
GPP_B2 Individual Voltage Select	3.3Volts	This setting controls the VCCIO voltage for the
GPP_B3 Individual Voltage Select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

#	Parameter	Platform	Settings
	GPP_B0 Individual Voltage Select	ICL-YN ICL-UN	3.3 Volts 3.3 Volts

Table 2-16. - GPIO (Sheet 7 of 17)

	GPP_B1 Individual Voltage Select	ICL-YN	3.3 Volts
		ICL-UN	3.3 Volts
	GPP_B2 Individual Voltage Select	ICL-YN	3.3 Volts
		ICL-UN	3.3 Volts
	GPP_B3 Individual Voltage Select	ICL-YN	1.8 Volts
		ICL-UN	1.8 Volts
	GPP_B4 Individual Voltage Select	ICL-YN	3.3 Volts
		ICL-UN	3.3 Volts
	GPP_B5 Individual Voltage Select	ICL-YN	1.8 Volts
		ICL-UN	1.8 Volts
	GPP_B6 Individual Voltage Select	ICL-YN	1.8 Volts
		ICL-UN	1.8 Volts
	GPP_B7 Individual Voltage Select	ICL-YN	1.8 Volts
		ICL-UN	1.8 Volts
	GPP_B8 Individual Voltage Select	ICL-YN	1.8 Volts
		ICL-UN	1.8 Volts
	GPP_B9 Individual Voltage Select	ICL-YN	3.3 Volts
		ICL-UN	3.3 Volts
	GPP_B10 Individual Voltage Select	ICL-YN	3.3 Volts
		ICL-UN	3.3 Volts
	GPP_B11 Individual Voltage Select	ICL-YN	3.3 Volts
		ICL-UN	3.3 Volts
	GPP_B12 Individual Voltage Select	ICL-YN	3.3 Volts
		ICL-UN	3.3 Volts
	GPP_B13 Individual Voltage Select	ICL-YN	3.3 Volts
		ICL-UN	3.3 Volts
	GPP_B14 Individual Voltage Select	ICL-YN	1.8 Volts
		ICL-UN	1.8 Volts
	GPP_B15 Individual Voltage Select	ICL-YN	3.3 Volts
		ICL-UN	3.3 Volts
	GPP_B16 Individual Voltage Select	ICL-YN	3.3 Volts
		ICL-UN	3.3 Volts
	GPP_B17 Individual Voltage Select	ICL-YN	3.3 Volts
		ICL-UN	3.3 Volts
	GPP_B18 Individual Voltage Select	ICL-YN	3.3 Volts
		ICL-UN	3.3 Volts
	GPP_B19 Individual Voltage Select	ICL-YN	1.8 Volts
		ICL-UN	1.8 Volts
	GPP_B20 Individual Voltage Select	ICL-YN	1.8 Volts
		ICL-UN	1.8 Volts
	GPP_B21 Individual Voltage Select	ICL-YN	1.8 Volts
		ICL-UN	1.8 Volts
	GPP_B22 Individual Voltage Select	ICL-YN	1.8 Volts
		ICL-UN	1.8 Volts
	GPP_B23 Individual Voltage Select	ICL-YN	1.8 Volts
		ICL-UN	1.8 Volts

Table 2-16. - GPIO (Sheet 8 of 17)

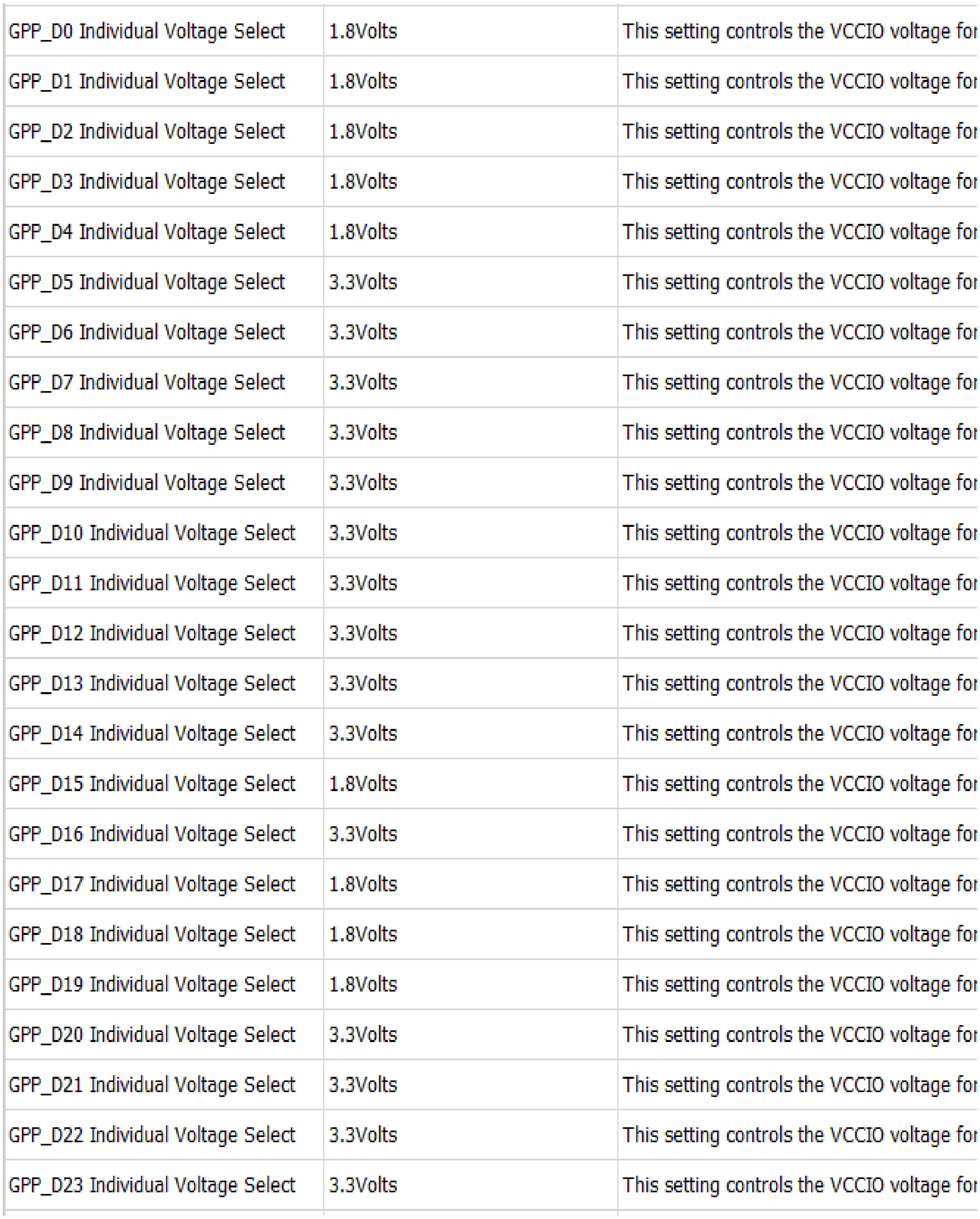


GPP_C0 Individual Voltage Select	3.3Volts	This setting controls the VCCIO voltage fo
GPP_C1 Individual Voltage Select	3.3Volts	This setting controls the VCCIO voltage fo
GPP_C2 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage fo
GPP_C3 Individual Voltage Select	3.3Volts	This setting controls the VCCIO voltage fo
GPP_C4 Individual Voltage Select	3.3Volts	This setting controls the VCCIO voltage fo
GPP_C5 Individual Voltage Select	3.3Volts	This setting controls the VCCIO voltage fo
GPP_C6 Individual Voltage Select	3.3Volts	This setting controls the VCCIO voltage fo
GPP_C7 Individual Voltage Select	3.3Volts	This setting controls the VCCIO voltage fo
GPP_C8 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage fo
GPP_C9 Individual Voltage Select	3.3Volts	This setting controls the VCCIO voltage fo
GPP_C10 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage fo
GPP_C11 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage fo
GPP_C12 Individual Voltage Select	3.3Volts	This setting controls the VCCIO voltage fo
GPP_C13 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage fo
GPP_C14 Individual Voltage Select	3.3Volts	This setting controls the VCCIO voltage fo
GPP_C15 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage fo
GPP_C16 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage fo
GPP_C17 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage fo
GPP_C18 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage fo
GPP_C19 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage fo
GPP_C20 Individual Voltage Select	3.3Volts	This setting controls the VCCIO voltage fo
GPP_C21 Individual Voltage Select	3.3Volts	This setting controls the VCCIO voltage fo
GPP_C22 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage fo
GPP_C23 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage fo

Table 2-16. - GPIO (Sheet 9 of 17)

#	Parameter	Platform	Settings
	GPP_C0 Individual Voltage Select	ICL-YN	3.3 Volts
		ICL-UN	3.3 Volts
	GPP_C1 Individual Voltage Select	ICL-YN	3.3 Volts
		ICL-UN	3.3 Volts
	GPP_C2 Individual Voltage Select	ICL-YN	1.8 Volts
		ICL-UN	1.8 Volts
	GPP_C3 Individual Voltage Select	ICL-YN	3.3 Volts
		ICL-UN	3.3 Volts
	GPP_C4 Individual Voltage Select	ICL-YN	3.3 Volts
		ICL-UN	3.3 Volts
	GPP_C5 Individual Voltage Select	ICL-YN	3.3 Volts
		ICL-UN	3.3 Volts
	GPP_C6 Individual Voltage Select	ICL-YN	3.3 Volts
		ICL-UN	3.3 Volts
	GPP_C7 Individual Voltage Select	ICL-YN	3.3 Volts
		ICL-UN	3.3 Volts
	GPP_C8 Individual Voltage Select	ICL-YN	1.8 Volts
		ICL-UN	1.8 Volts
	GPP_C9 Individual Voltage Select	ICL-YN	3.3 Volts
		ICL-UN	3.3 Volts
	GPP_C10 Individual Voltage Select	ICL-YN	1.8 Volts
		ICL-UN	1.8 Volts
	GPP_C11 Individual Voltage Select	ICL-YN	1.8 Volts
		ICL-UN	1.8 Volts
	GPP_C12 Individual Voltage Select	ICL-YN	3.3 Volts
		ICL-UN	3.3 Volts
	GPP_C13 Individual Voltage Select	ICL-YN	1.8 Volts
		ICL-UN	1.8 Volts
	GPP_C14 Individual Voltage Select	ICL-YN	3.3 Volts
		ICL-UN	3.3 Volts
	GPP_C15 Individual Voltage Select	ICL-YN	1.8 Volts
		ICL-UN	1.8 Volts
	GPP_C16 Individual Voltage Select	ICL-YN	1.8 Volts
		ICL-UN	1.8 Volts
	GPP_C17 Individual Voltage Select	ICL-YN	1.8 Volts
		ICL-UN	1.8 Volts
	GPP_C18 Individual Voltage Select	ICL-YN	1.8 Volts
		ICL-UN	1.8 Volts
	GPP_C19 Individual Voltage Select	ICL-YN	1.8 Volts
		ICL-UN	1.8 Volts
	GPP_C20 Individual Voltage Select	ICL-YN	3.3 Volts
		ICL-UN	3.3 Volts
	GPP_C21 Individual Voltage Select	ICL-YN	3.3 Volts
		ICL-UN	3.3 Volts
	GPP_C22 Individual Voltage Select	ICL-YN	1.8 Volts
		ICL-UN	1.8 Volts
	GPP_C23 Individual Voltage Select	ICL-YN	1.8 Volts
		ICL-UN	1.8 Volts

Table 2-16. - GPIO (Sheet 10 of 17)

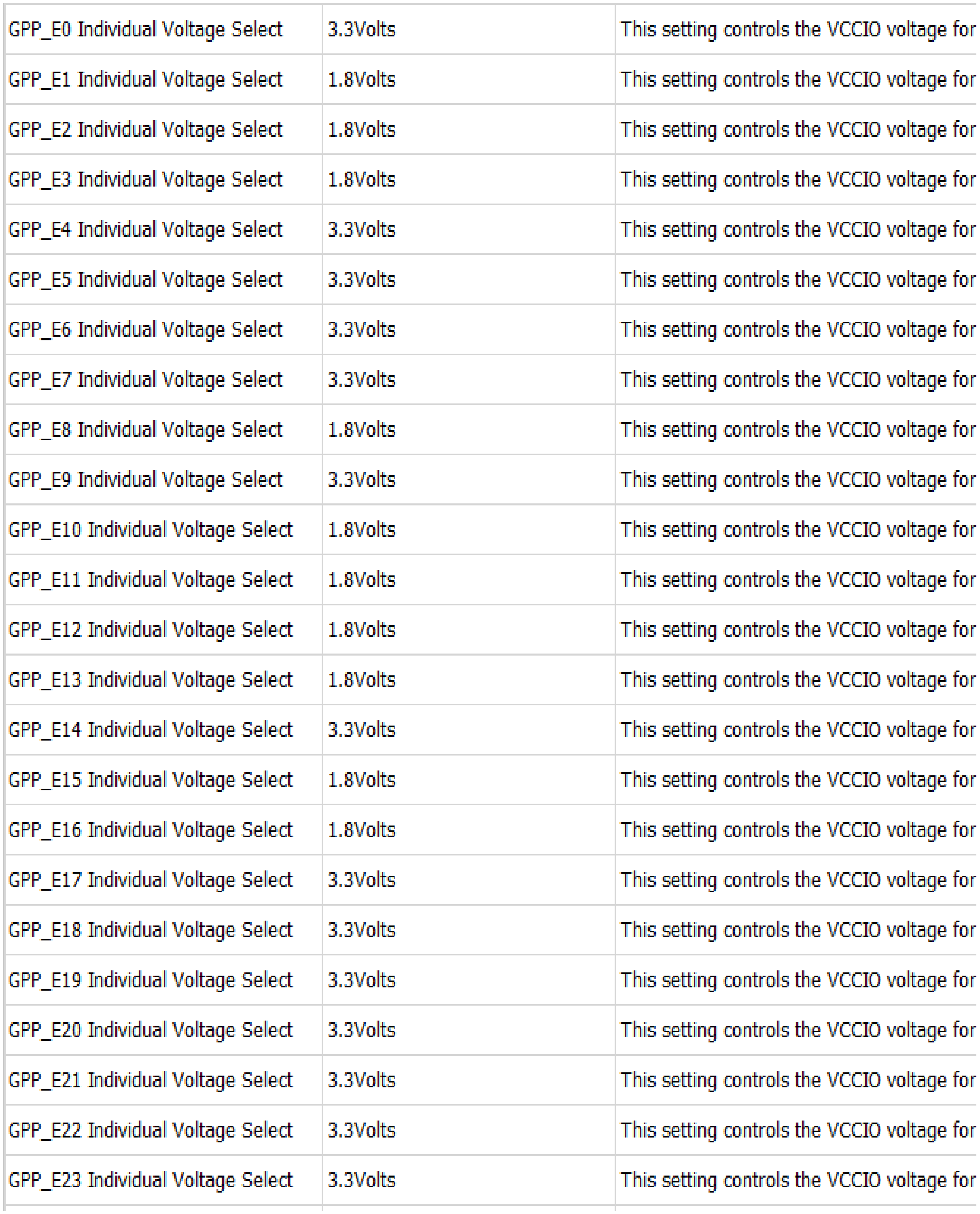


GPP_D0 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage for
GPP_D1 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage for
GPP_D2 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage for
GPP_D3 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage for
GPP_D4 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage for
GPP_D5 Individual Voltage Select	3.3Volts	This setting controls the VCCIO voltage for
GPP_D6 Individual Voltage Select	3.3Volts	This setting controls the VCCIO voltage for
GPP_D7 Individual Voltage Select	3.3Volts	This setting controls the VCCIO voltage for
GPP_D8 Individual Voltage Select	3.3Volts	This setting controls the VCCIO voltage for
GPP_D9 Individual Voltage Select	3.3Volts	This setting controls the VCCIO voltage for
GPP_D10 Individual Voltage Select	3.3Volts	This setting controls the VCCIO voltage for
GPP_D11 Individual Voltage Select	3.3Volts	This setting controls the VCCIO voltage for
GPP_D12 Individual Voltage Select	3.3Volts	This setting controls the VCCIO voltage for
GPP_D13 Individual Voltage Select	3.3Volts	This setting controls the VCCIO voltage for
GPP_D14 Individual Voltage Select	3.3Volts	This setting controls the VCCIO voltage for
GPP_D15 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage for
GPP_D16 Individual Voltage Select	3.3Volts	This setting controls the VCCIO voltage for
GPP_D17 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage for
GPP_D18 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage for
GPP_D19 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage for
GPP_D20 Individual Voltage Select	3.3Volts	This setting controls the VCCIO voltage for
GPP_D21 Individual Voltage Select	3.3Volts	This setting controls the VCCIO voltage for
GPP_D22 Individual Voltage Select	3.3Volts	This setting controls the VCCIO voltage for
GPP_D23 Individual Voltage Select	3.3Volts	This setting controls the VCCIO voltage for

Table 2-16. - GPIO (Sheet 11 of 17)

#	Parameter	Platform	Settings
	GPP_D0 Individual Voltage Select	ICL-YN ICL-UN	1.8 Volts 1.8 Volts
	GPP_D1 Individual Voltage Select	ICL-YN ICL-UN	1.8 Volts 1.8 Volts
	GPP_D2 Individual Voltage Select	ICL-YN ICL-UN	1.8 Volts 1.8 Volts
	GPP_D3 Individual Voltage Select	ICL-YN ICL-UN	1.8 Volts 1.8 Volts
	GPP_D4 Individual Voltage Select	ICL-YN ICL-UN	1.8 Volts 1.8 Volts
	GPP_D5 Individual Voltage Select	ICL-YN ICL-UN	3.3 Volts 3.3 Volts
	GPP_D6 Individual Voltage Select	ICL-YN ICL-UN	3.3 Volts 3.3 Volts
	GPP_D7 Individual Voltage Select	ICL-YN ICL-UN	3.3 Volts 3.3 Volts
	GPP_D8 Individual Voltage Select	ICL-YN ICL-UN	3.3 Volts 3.3 Volts
	GPP_D9 Individual Voltage Select	ICL-YN ICL-UN	3.3 Volts 3.3 Volts
	GPP_D10 Individual Voltage Select	ICL-YN ICL-UN	3.3 Volts 3.3 Volts
	GPP_D11 Individual Voltage Select	ICL-YN ICL-UN	3.3 Volts 3.3 Volts
	GPP_D12 Individual Voltage Select	ICL-YN ICL-UN	3.3 Volts 3.3 Volts
	GPP_D13 Individual Voltage Select	ICL-YN ICL-UN	3.3 Volts 3.3 Volts
	GPP_D14 Individual Voltage Select	ICL-YN ICL-UN	3.3 Volts 3.3 Volts
	GPP_D15 Individual Voltage Select	ICL-YN ICL-UN	1.8 Volts 1.8 Volts
	GPP_D16 Individual Voltage Select	ICL-YN ICL-UN	3.3 Volts 3.3 Volts
	GPP_D17 Individual Voltage Select	ICL-YN ICL-UN	1.8 Volts 1.8 Volts
	GPP_D18 Individual Voltage Select	ICL-YN ICL-UN	1.8 Volts 1.8 Volts
	GPP_D19 Individual Voltage Select	ICL-YN ICL-UN	1.8 Volts 1.8 Volts
	GPP_D20 Individual Voltage Select	ICL-YN ICL-UN	3.3 Volts 3.3 Volts
	GPP_D21 Individual Voltage Select	ICL-YN ICL-UN	3.3 Volts 3.3 Volts
	GPP_D22 Individual Voltage Select	ICL-YN ICL-UN	3.3 Volts 3.3 Volts
	GPP_D23 Individual Voltage Select	ICL-YN ICL-UN	3.3 Volts 3.3 Volts

Table 2-16. - GPIO (Sheet 12 of 17)

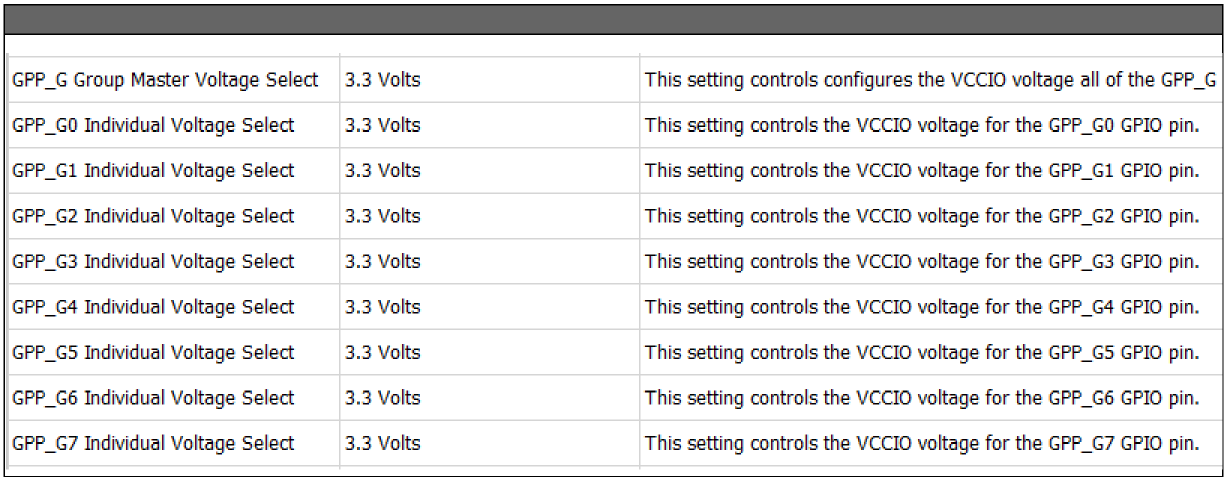


GPP_E0 Individual Voltage Select	3.3Volts	This setting controls the VCCIO voltage for
GPP_E1 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage for
GPP_E2 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage for
GPP_E3 Individual Voltage Select	1.8Volts	This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

Table 2-16. - GPIO (Sheet 13 of 17)

#	Parameter	Platform	Settings
	GPP_E0 Individual Voltage Select	ICL-YN	3.3 Volts
		ICL-UN	3.3 Volts
	GPP_E1 Individual Voltage Select	ICL-YN	1.8 Volts
		ICL-UN	1.8 Volts
	GPP_E2 Individual Voltage Select	ICL-YN	1.8 Volts
		ICL-UN	1.8 Volts
	GPP_E3 Individual Voltage Select	ICL-YN	1.8 Volts
		ICL-UN	1.8 Volts
	GPP_E4 Individual Voltage Select	ICL-YN	3.3 Volts
		ICL-UN	3.3 Volts
	GPP_E5 Individual Voltage Select	ICL-YN	3.3 Volts
		ICL-UN	3.3 Volts
	GPP_E6 Individual Voltage Select	ICL-YN	3.3 Volts
		ICL-UN	3.3 Volts
	GPP_E7 Individual Voltage Select	ICL-YN	3.3 Volts
		ICL-UN	3.3 Volts
	GPP_E8 Individual Voltage Select	ICL-YN	1.8 Volts
		ICL-UN	1.8 Volts
	GPP_E9 Individual Voltage Select	ICL-YN	3.3 Volts
		ICL-UN	3.3 Volts
	GPP_E10 Individual Voltage Select	ICL-YN	1.8 Volts
		ICL-UN	1.8 Volts
	GPP_E11 Individual Voltage Select	ICL-YN	1.8 Volts
		ICL-UN	1.8 Volts
	GPP_E12 Individual Voltage Select	ICL-YN	1.8 Volts
		ICL-UN	1.8 Volts
	GPP_E13 Individual Voltage Select	ICL-YN	1.8 Volts
		ICL-UN	1.8 Volts
	GPP_E14 Individual Voltage Select	ICL-YN	3.3 Volts
		ICL-UN	3.3 Volts
	GPP_E15 Individual Voltage Select	ICL-YN	1.8 Volts
		ICL-UN	1.8 Volts
	GPP_E16 Individual Voltage Select	ICL-YN	1.8 Volts
		ICL-UN	1.8 Volts
	GPP_E17 Individual Voltage Select	ICL-YN	3.3 Volts
		ICL-UN	3.3 Volts
	GPP_E18 Individual Voltage Select	ICL-YN	3.3 Volts
		ICL-UN	3.3 Volts
	GPP_E19 Individual Voltage Select	ICL-YN	3.3 Volts
		ICL-UN	3.3 Volts
	GPP_E20 Individual Voltage Select	ICL-YN	3.3 Volts
		ICL-UN	3.3 Volts
	GPP_E21 Individual Voltage Select	ICL-YN	3.3 Volts
		ICL-UN	3.3 Volts
	GPP_E22 Individual Voltage Select	ICL-YN	3.3 Volts
		ICL-UN	3.3 Volts
	GPP_E23 Individual Voltage Select	ICL-YN	3.3 Volts
		ICL-UN	3.3 Volts

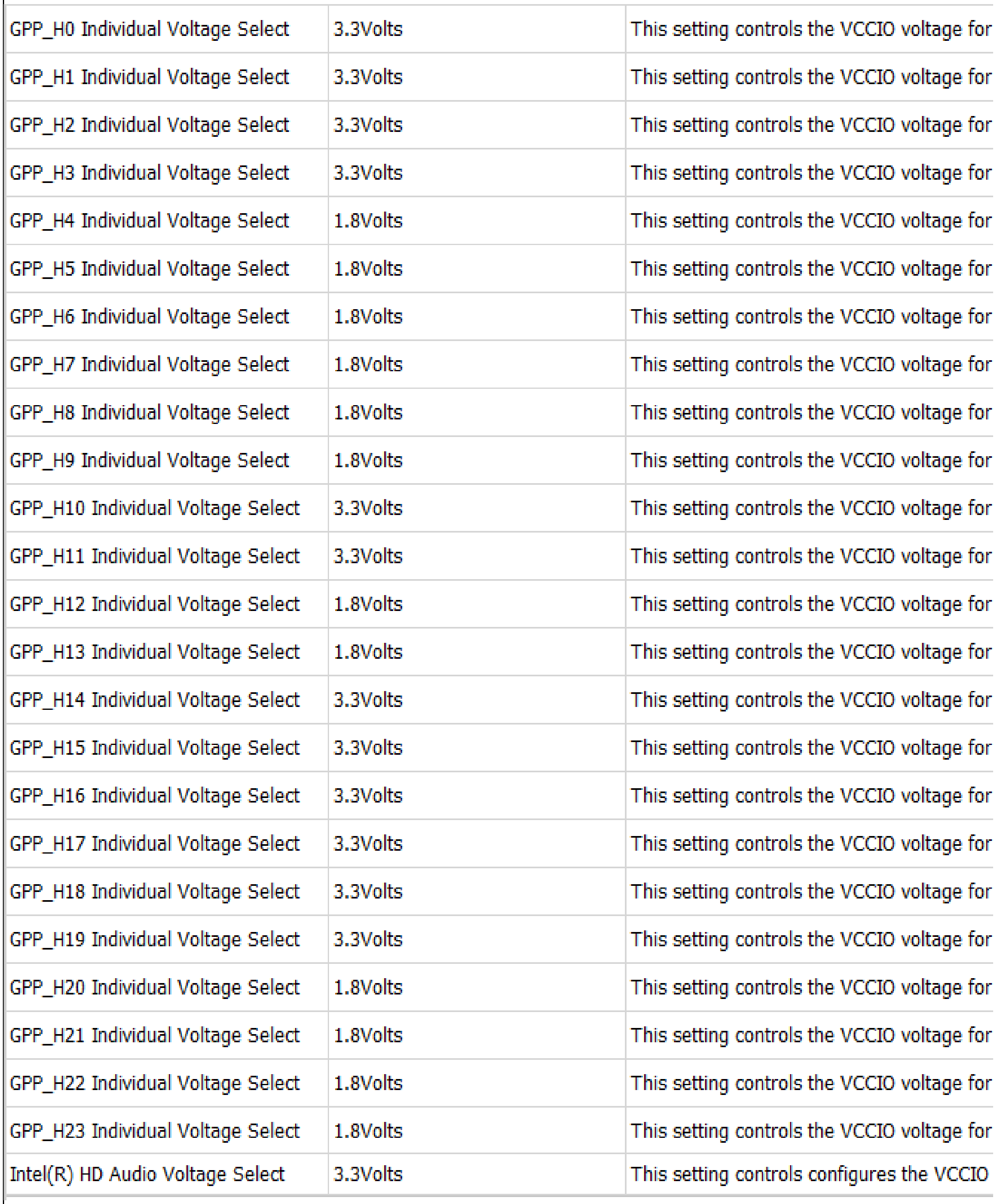
Table 2-16. - GPIO (Sheet 14 of 17)



GPP_G Group Master Voltage Select	3.3 Volts	This setting controls configures the VCCIO voltage all of the GPP_G
GPP_G0 Individual Voltage Select	3.3 Volts	This setting controls the VCCIO voltage for the GPP_G0 GPIO pin.
GPP_G1 Individual Voltage Select	3.3 Volts	This setting controls the VCCIO voltage for the GPP_G1 GPIO pin.
GPP_G2 Individual Voltage Select	3.3 Volts	This setting controls the VCCIO voltage for the GPP_G2 GPIO pin.
GPP_G3 Individual Voltage Select	3.3 Volts	This setting controls the VCCIO voltage for the GPP_G3 GPIO pin.
GPP_G4 Individual Voltage Select	3.3 Volts	This setting controls the VCCIO voltage for the GPP_G4 GPIO pin.
GPP_G5 Individual Voltage Select	3.3 Volts	This setting controls the VCCIO voltage for the GPP_G5 GPIO pin.
GPP_G6 Individual Voltage Select	3.3 Volts	This setting controls the VCCIO voltage for the GPP_G6 GPIO pin.
GPP_G7 Individual Voltage Select	3.3 Volts	This setting controls the VCCIO voltage for the GPP_G7 GPIO pin.

#	Parameter	Platform	Settings
	GPP_G0 Individual Voltage Select	ICL-YN ICL-UN	3.3 Volts 3.3 Volts
	GPP_G1 Individual Voltage Select	ICL-YN ICL-UN	3.3 Volts 3.3 Volts
	GPP_G2 Individual Voltage Select	ICL-YN ICL-UN	3.3 Volts 3.3 Volts
	GPP_G3 Individual Voltage Select	ICL-YN ICL-UN	3.3 Volts 3.3 Volts
	GPP_G4 Individual Voltage Select	ICL-YN ICL-UN	3.3 Volts 3.3 Volts
	GPP_G5 Individual Voltage Select	ICL-YN ICL-UN	3.3 Volts 3.3 Volts
	GPP_G6 Individual Voltage Select	ICL-YN ICL-UN	3.3 Volts 3.3 Volts
	GPP_G7 Individual Voltage Select	ICL-YN ICL-UN	3.3 Volts 3.3 Volts

Table 2-16. - GPIO (Sheet 15 of 17)



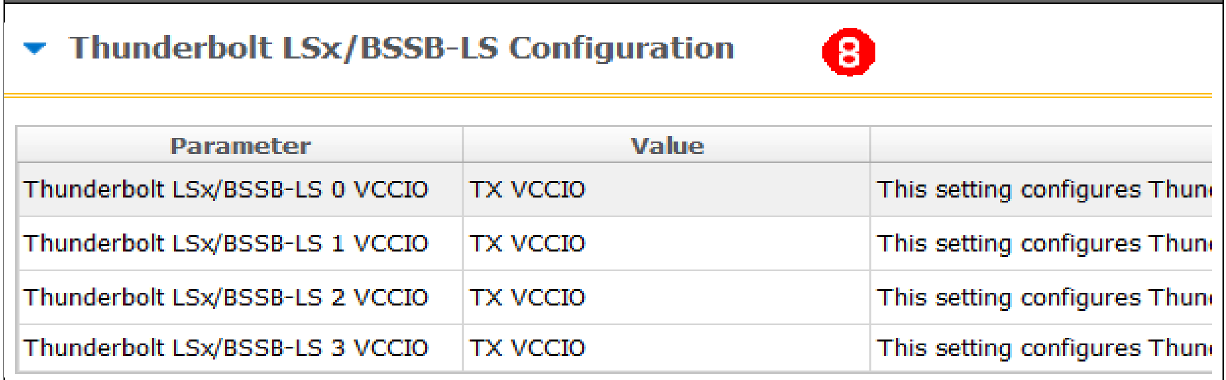
GPP_H0 Individual Voltage Select	3.3Volts	This setting controls the VCCIO voltage for
GPP_H1 Individual Voltage Select	3.3Volts	This setting controls the VCCIO voltage for
GPP_H2 Individual Voltage Select	3.3Volts	This setting controls the VCCIO voltage for
GPP_H3 Individual Voltage Select	3.3Volts	This setting controls the VCCIO voltage for
GPP_H4 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage for
GPP_H5 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage for
GPP_H6 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage for
GPP_H7 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage for
GPP_H8 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage for
GPP_H9 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage for
GPP_H10 Individual Voltage Select	3.3Volts	This setting controls the VCCIO voltage for
GPP_H11 Individual Voltage Select	3.3Volts	This setting controls the VCCIO voltage for
GPP_H12 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage for
GPP_H13 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage for
GPP_H14 Individual Voltage Select	3.3Volts	This setting controls the VCCIO voltage for
GPP_H15 Individual Voltage Select	3.3Volts	This setting controls the VCCIO voltage for
GPP_H16 Individual Voltage Select	3.3Volts	This setting controls the VCCIO voltage for
GPP_H17 Individual Voltage Select	3.3Volts	This setting controls the VCCIO voltage for
GPP_H18 Individual Voltage Select	3.3Volts	This setting controls the VCCIO voltage for
GPP_H19 Individual Voltage Select	3.3Volts	This setting controls the VCCIO voltage for
GPP_H20 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage for
GPP_H21 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage for
GPP_H22 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage for
GPP_H23 Individual Voltage Select	1.8Volts	This setting controls the VCCIO voltage for
Intel(R) HD Audio Voltage Select	3.3Volts	This setting controls configures the VCCIO

#	Parameter	Platform	Settings

Table 2-16. - GPIO (Sheet 16 of 17)

	GPP_H0 Individual Voltage Select	ICL-YN	3.3 Volts
		ICL-UN	3.3 Volts
	GPP_H1 Individual Voltage Select	ICL-YN	3.3 Volts
		ICL-UN	3.3 Volts
	GPP_H2 Individual Voltage Select	ICL-YN	3.3 Volts
		ICL-UN	3.3 Volts
	GPP_H3 Individual Voltage Select	ICL-YN	3.3 Volts
		ICL-UN	3.3 Volts
	GPP_H4 Individual Voltage Select	ICL-YN	1.8 Volts
		ICL-UN	1.8 Volts
	GPP_H5 Individual Voltage Select	ICL-YN	1.8 Volts
		ICL-UN	1.8 Volts
	GPP_H6 Individual Voltage Select	ICL-YN	1.8 Volts
		ICL-UN	1.8 Volts
	GPP_H7 Individual Voltage Select	ICL-YN	1.8 Volts
		ICL-UN	1.8 Volts
	GPP_H8 Individual Voltage Select	ICL-YN	1.8 Volts
		ICL-UN	1.8 Volts
	GPP_H9 Individual Voltage Select	ICL-YN	1.8 Volts
		ICL-UN	1.8 Volts
	GPP_H10 Individual Voltage Select	ICL-YN	3.3 Volts
		ICL-UN	3.3 Volts
	GPP_H11 Individual Voltage Select	ICL-YN	3.3 Volts
		ICL-UN	3.3 Volts
	GPP_H12 Individual Voltage Select	ICL-YN	1.8 Volts
		ICL-UN	1.8 Volts
	GPP_H13 Individual Voltage Select	ICL-YN	1.8 Volts
		ICL-UN	1.8 Volts
	GPP_H14 Individual Voltage Select	ICL-YN	3.3 Volts
		ICL-UN	3.3 Volts
	GPP_H15 Individual Voltage Select	ICL-YN	3.3 Volts
		ICL-UN	3.3 Volts
	GPP_H16 Individual Voltage Select	ICL-YN	3.3 Volts
		ICL-UN	3.3 Volts
	GPP_H17 Individual Voltage Select	ICL-YN	3.3 Volts
		ICL-UN	3.3 Volts
	GPP_H18 Individual Voltage Select	ICL-YN	3.3 Volts
		ICL-UN	3.3 Volts
	GPP_H19 Individual Voltage Select	ICL-YN	3.3 Volts
		ICL-UN	3.3 Volts
	GPP_H20 Individual Voltage Select	ICL-YN	1.8 Volts
		ICL-UN	1.8 Volts
	GPP_H21 Individual Voltage Select	ICL-YN	1.8 Volts
		ICL-UN	1.8 Volts
	GPP_H22 Individual Voltage Select	ICL-YN	1.8 Volts
		ICL-UN	1.8 Volts
	GPP_H23 Individual Voltage Select	ICL-YN	1.8 Volts
		ICL-UN	1.8 Volts
	Intel® HD Audio Voltage Select	ICL-YN	1.8 Volts
		ICL-UN	1.8 Volts

Table 2-16. - GPIO (Sheet 17 of 17)



Thunderbolt LSx/BSSB-LS Configuration ⑧

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
⑧	**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.	ICL-YN ICL-UN	TX VCCIO TX VCCIO
	Thunderbolt LSx/BSSB-LS 1 VCCIO **Values: TX VCCIO / Legacy VCCIO** This setting configured Thunderbolt LSx/BSSB-LS 0 VCCIO.	ICL-YN ICL-UN	TX VCCIO TX VCCIO
	Thunderbolt LSx/BSSB-LS 2 VCCIO **Values: TX VCCIO / Legacy VCCIO** This setting configured Thunderbolt LSx/BSSB-LS 0 VCCIO.	ICL-YN ICL-UN	TX VCCIO TX VCCIO
	Thunderbolt LSx/BSSB-LS 3 VCCIO **Values: TX VCCIO / Legacy VCCIO** This setting configured Thunderbolt LSx/BSSB-LS 0 VCCIO.	ICL-YN ICL-UN	TX VCCIO TX VCCIO

Table 2-17. - Intel® Precise Touch and Stylus

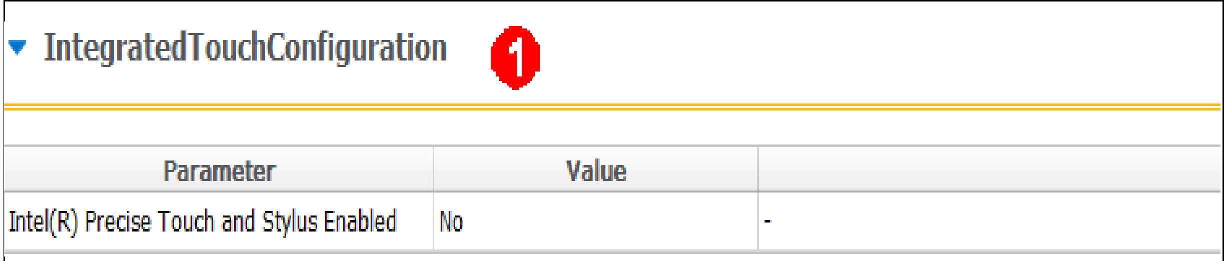
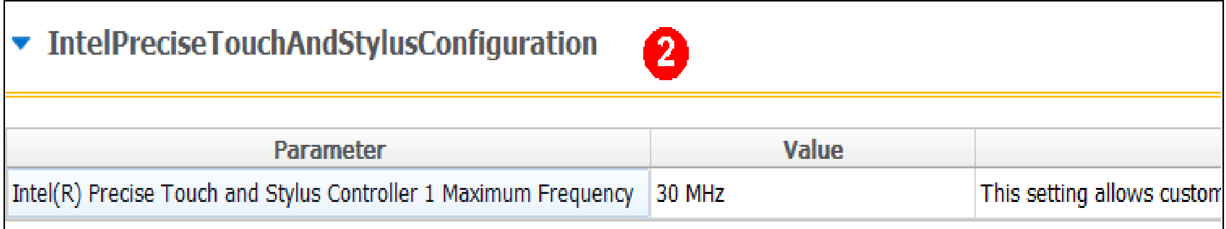
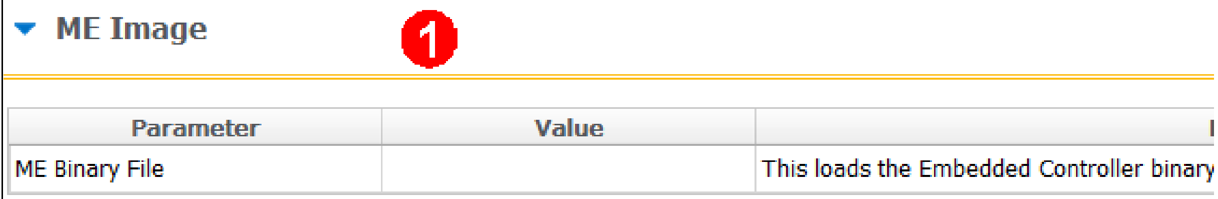
<table>
<tr><th colspan="4"></th></tr>
<tr><td colspan="4"><b>Click on Intel® Precise Touch and Stylus in the left tabs menu> IntegratedTouchConfiguration is expanded by default:</b></td></tr>
<tr><td colspan="4">
▼ IntegratedTouchConfiguration ①
<table>
<tr><th>Parameter</th><th>Value</th><th></th></tr>
<tr><td>Intel(R) Precise Touch and Stylus Enabled</td><td>No</td><td>-</td></tr>
</table></td></tr>
<tr><th>#</th><th>Parameter</th><th>Platform</th><th>Settings</th></tr>
<tr><td>①</td><td><b>Intel® Precise Touch and Stylus - IntegratedTouchConfiguration</b></td><td></td><td></td></tr>
<tr><td></td><td><b>Intel® Precise Touch and Stylus Enabled</b></td><td>ICL-YN
ICL-UN</td><td>No
No</td></tr>
<tr><td colspan="4"><b>Click on Intel® Precise Touch and Stylus in the left tabs menu> IntegratedTouchAndStylusConfiguration is expanded by default:</b></td></tr>
<tr><td colspan="4">
▼ IntelPreciseTouchAndStylusConfiguration ②
<table>
<tr><th>Parameter</th><th>Value</th><th></th></tr>
<tr><td>Intel(R) Precise Touch and Stylus Controller 1 Maximum Frequency</td><td>30 MHz</td><td>This setting allows custom</td></tr>
</table></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td>②</td><td><b>Intel® Precise Touch and Stylus - IntelPerciseTouchandStylusConfiguration</b></td><td></td><td></td></tr>
<tr><td></td><td><b>Intel® Precise Touch and Stylus Controller 1 Maximum Frequency</b></td><td>ICL-YN
ICL-UN</td><td>30MHz
30MHz</td></tr>
</table>

Table 2-18. - FW Update Image Build

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

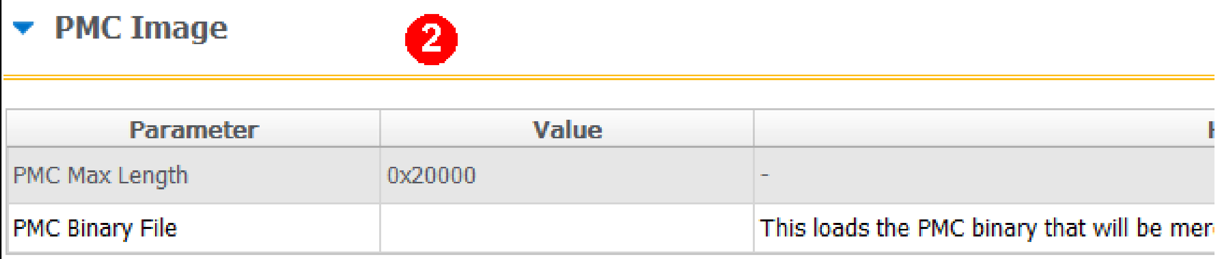


ME Image

Parameter	Value	
ME Binary File		This loads the Embedded Controller binary

#	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**		
①	**FW Update Image - 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.	ICL-YN ICL-UN	ME Binary ME Binary

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

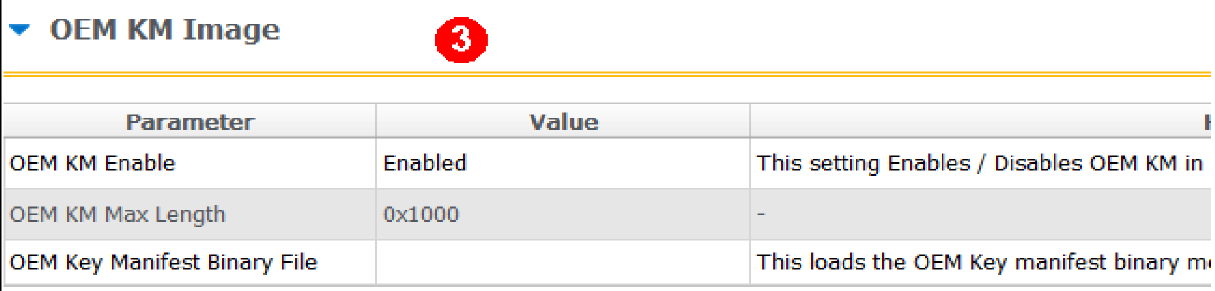


PMC Image

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

#	Parameter	Platform	Settings
②	**FW Update Image - 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.	ICL-YN ICL-UN	PMC Binary PMC Binary

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



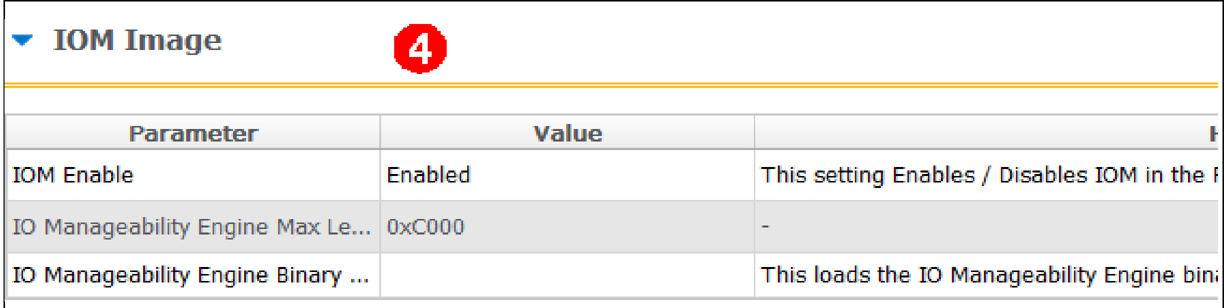
OEM KM Image

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

Table 2-18. - FW Update Image Build

#	Parameter	Platform	Settings
③	**FW Update Image - OEM KM Image**		
	OEM KM Enable **Values: Enabled / Disabled** This setting Enables / Disables OEM KM in the FWUpdate image.	ICL-YN ICL-UN	Enabled 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.	ICL-YN ICL-UN	OEM KM Binary OEM KM Binary

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

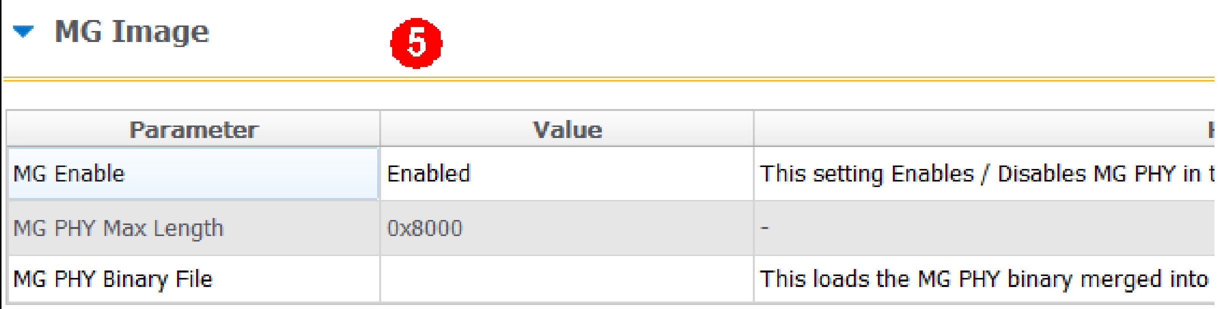

IOM Image

④

Parameter	Value	
IOM Enable	Enabled	This setting Enables / Disables IOM in the
IO Manageability Engine Max Le...	0xC000	-
IO Manageability Engine Binary ...		This loads the IO Manageability Engine bin

#	Parameter	Platform	Settings
④	**FW Update Image - IOM Image**		
	IOM Enable **Values: Enabled / Disabled** This setting Enables / Disables IOM in the FWUpdate image.	ICL-YN ICL-UN	Enabled 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.	ICL-YN ICL-UN	IOM Binary IOM Binary

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


MG Image

⑤

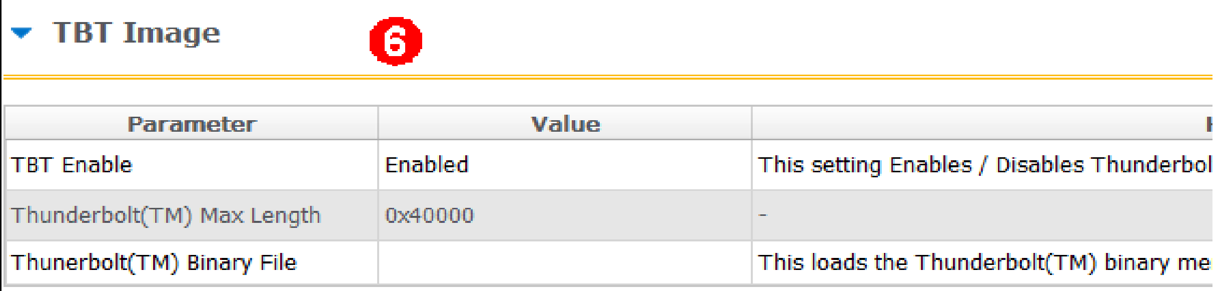
Parameter	Value	
MG Enable	Enabled	This setting Enables / Disables MG PHY in
MG PHY Max Length	0x8000	-
MG PHY Binary File		This loads the MG PHY binary merged into

#	Parameter	Platform	Settings

Table 2-18. - FW Update Image Build

⑤	**FW Update Image - MG Image**		
	MG Enable **Values: Enabled/Disabled** This setting Enables / Disables MG PHY in the FWUpdate image.	ICL-YN ICL-UN	Enabled Enabled
	MG PHY Max Length		
	MG PHY Binary File **Values: Binary File** This loads the MG PHY binary merged into the output image generated by the Intel® FIT tool.	ICL-YN ICL-UN	MG PHY Binary MG PHY Binary

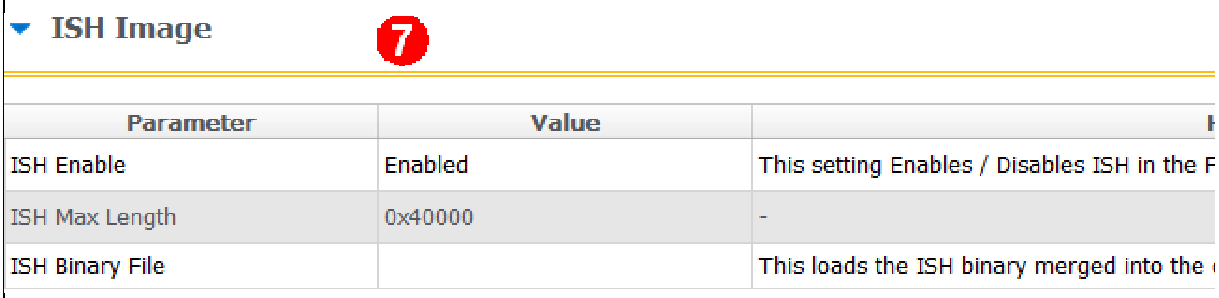
Click on FW Update Image Build in the left tabs menu> TBT Image is expanded by default:



Parameter	Value	
TBT Enable	Enabled	This setting Enables / Disables Thunderbol
Thunderbolt(TM) Max Length	0x40000	-
Thunerbolt(TM) Binary File		This loads the Thunderbolt(TM) binary me

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

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

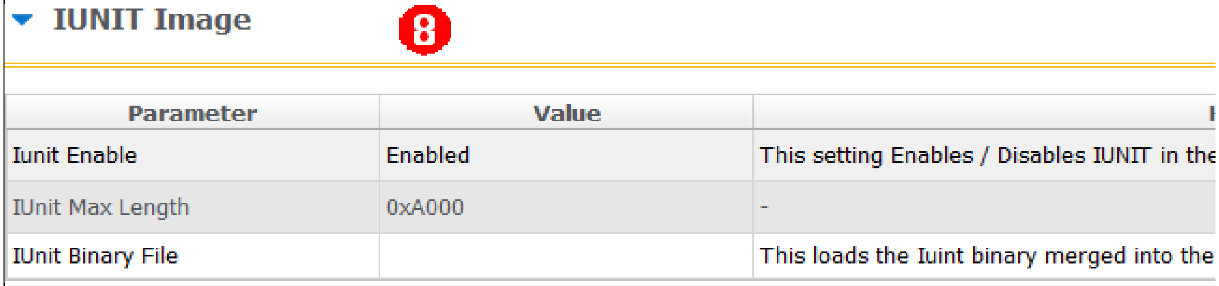


Parameter	Value	
ISH Enable	Enabled	This setting Enables / Disables ISH in the F
ISH Max Length	0x40000	-
ISH Binary File		This loads the ISH binary merged into the

#	Parameter	Platform	Settings
⑦	**FW Update Image - ISH Image**		

Table 2-18. - FW Update Image Build

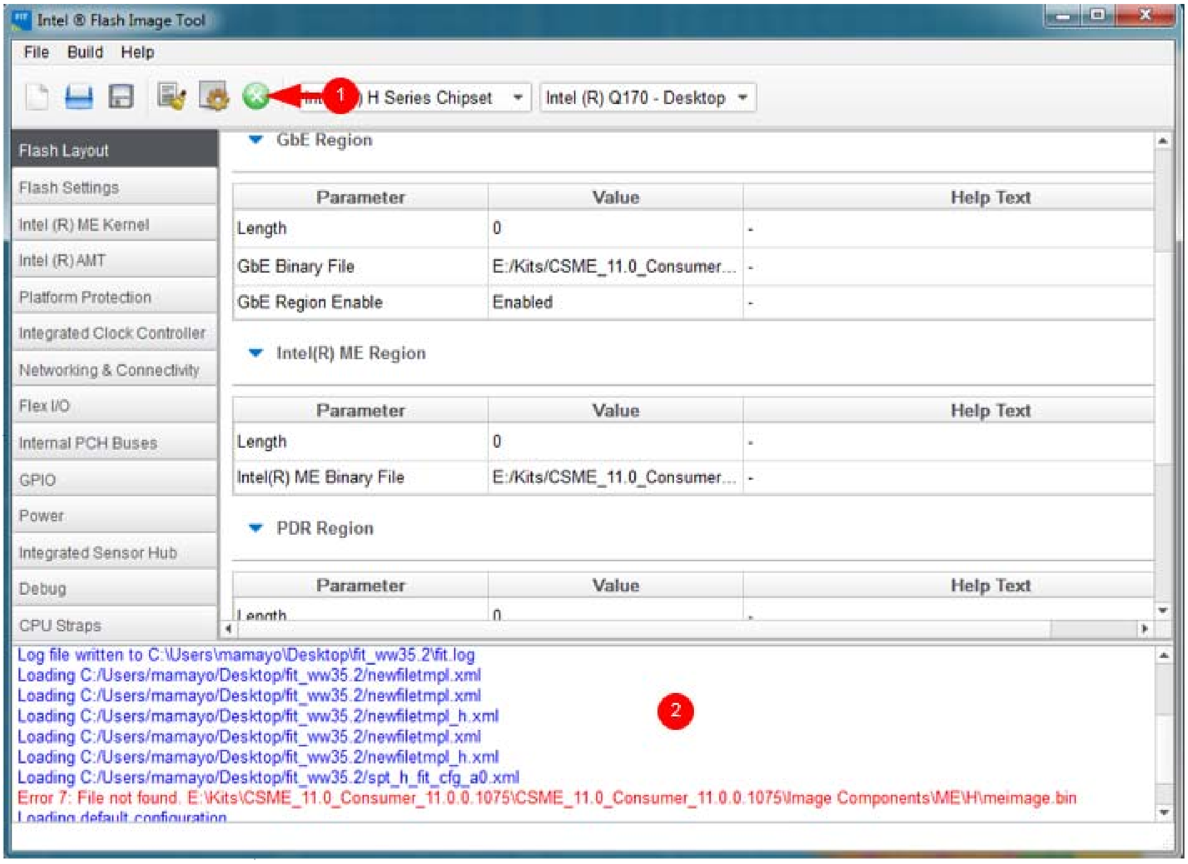
	ISH Enable **Values: Enabled / Disabled** This setting Enables / Disables ISH in the FWUpdate image.	ICL-YN ICL-UN	Enabled Enabled
	ISH Max Length		
	ISH Binary File **Values: Binary File** This loads the ISH binary merged into the output image generated by the Intel® FIT tool.	ICL-YN ICL-UN	ISH Binary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



Parameter	Value	
Iunit Enable	Enabled	This setting Enables / Disables IUNIT in the
IUnit Max Length	0xA000	-
IUnit Binary File		This loads the Iuint binary merged into the

#	Parameter	Platform	Settings
⑧	**FW Update Image - IUNIT Image**		
	IUnit Enable **Values: Enabled / Disabled** This setting Enables / Disables IUNIT in the FWUpdate image.	ICL-YN ICL-UN	Enabled 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.	ICL-YN ICL-UN	IUnit Binary IUnit Binary

Table 2-20. - Intel® FIT - Build Image

#	Parameter	CRB	Values
			
①	**Green Build button**		Can also select CTRL+B, or Build> Build Image from the menu bar along the top of the screen
②	**Console shows status of build and path where saved**		

GbE Region

Parameter	Value	Help Text
Length	0	-
GbE Binary File	E:/Kits/CSME_11.0_Consumer...	-
GbE Region Enable	Enabled	-

Intel(R) ME Region

Parameter	Value	Help Text
Length	0	-
Intel(R) ME Binary File	E:/Kits/CSME_11.0_Consumer...	-

PDR Region

Parameter	Value	Help Text
Length	0	-

```
Log file written to C:\Users\mamayo\Desktop\fit_ww35.2\fit.log
Loading C:/Users/mamayo/Desktop/fit_ww35.2/newfiletmpl.xml
Loading C:/Users/mamayo/Desktop/fit_ww35.2/newfiletmpl.xml
Loading C:/Users/mamayo/Desktop/fit_ww35.2/newfiletmpl_h.xml
Loading C:/Users/mamayo/Desktop/fit_ww35.2/newfiletmpl.xml
Loading C:/Users/mamayo/Desktop/fit_ww35.2/newfiletmpl_h.xml
Loading C:/Users/mamayo/Desktop/fit_ww35.2/spt_h_fit_cfg_a0.xml
Error 7: File not found. E:\Kits\CSME_11.0_Consumer_11.0.0.1075\CSME_11.0_Consumer_11.0.0.1075\Image Components\ME\H\meimage.bin
Loading default configuration
```

3 Programming SPI Flash Devices and Checking Firmware Status

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

3.1 Flash Burner/Programmer

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

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

   If two total SPI Flash devices were specified during the build process, then additional image files will be saved, one for each SPI Flash device. These files are assumed to be named **outimage(1).bin** and **outimage(2).bin**.
2. Utilize a Flash burner/programmer to program the image(s). For multiple SPI Flash devices, the images are numbered sequentially to correspond to the first and second SPI Flash device accordingly.

3.1.1 In-Circuit SPI Flash Programming for CRB

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

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

3.2 Flash Programming Tool (Intel® FPT)

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

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

Intel® FPT DOS Version

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

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

```
fpt.exe -i
```

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

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

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

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

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

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

```
FPT Operation Passed
```

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

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

3.2.1 Intel® FPT Windows* Version

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

Use the following steps to program the SPI Flash devices,

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

```
fptw.exe -i
```

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

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

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

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

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

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

```
FPT Operation Passed
```

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

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

3.3 Checking Intel® ME Firmware Status

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

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

```
MEInfo.exe -fwsts
```

The system should respond with a message similar to below.

```
Intel® MEInfo Version: 13.0.0.xxxx

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

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

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

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

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

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

3.4 Common Bring Up Issues and Troubleshooting Table

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

Problem / Issue	Solution / Workaround
System does not boot to DOS	By default, the system will boot to EFI Shell. To boot to DOS, 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® *Ice 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

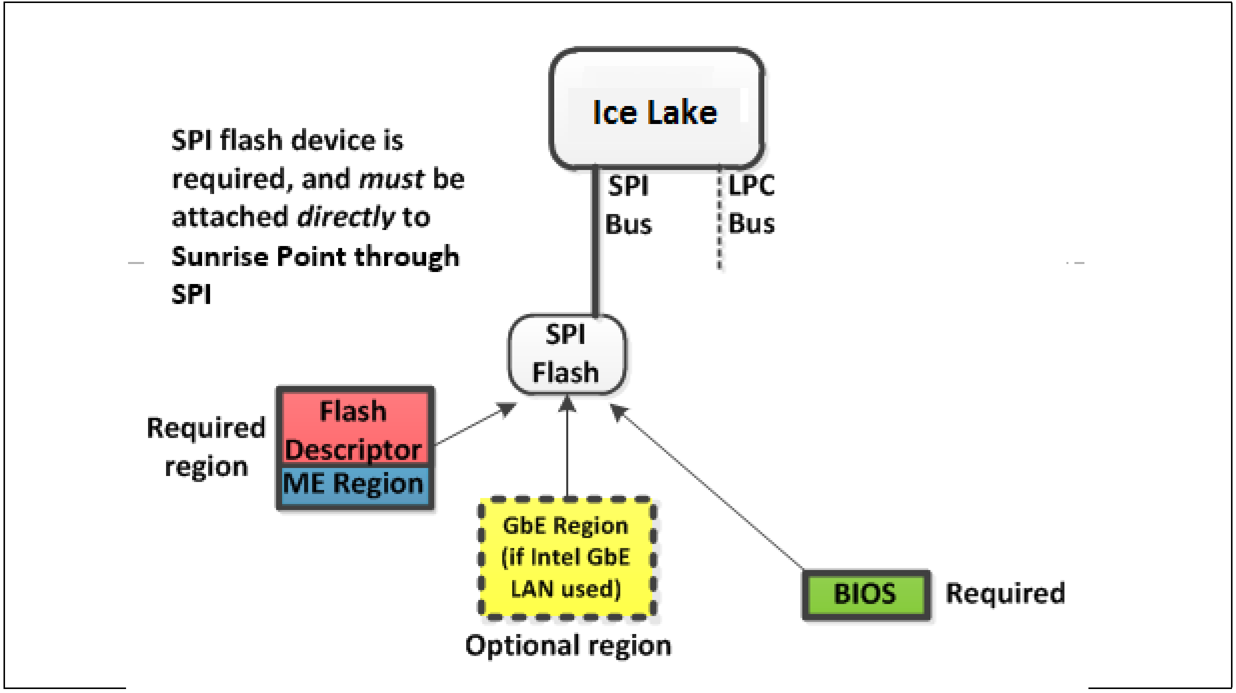

SPI flash device is required, and *must* be attached *directly* to Sunrise Point through SPI
Ice Lake
SPI Bus
LPC Bus
SPI Flash
Required region
Flash Descriptor
ME Region
GbE Region (if Intel GbE LAN used)
Optional region
BIOS
Required

Figure A-2. Configuration "B" — Mobile Only

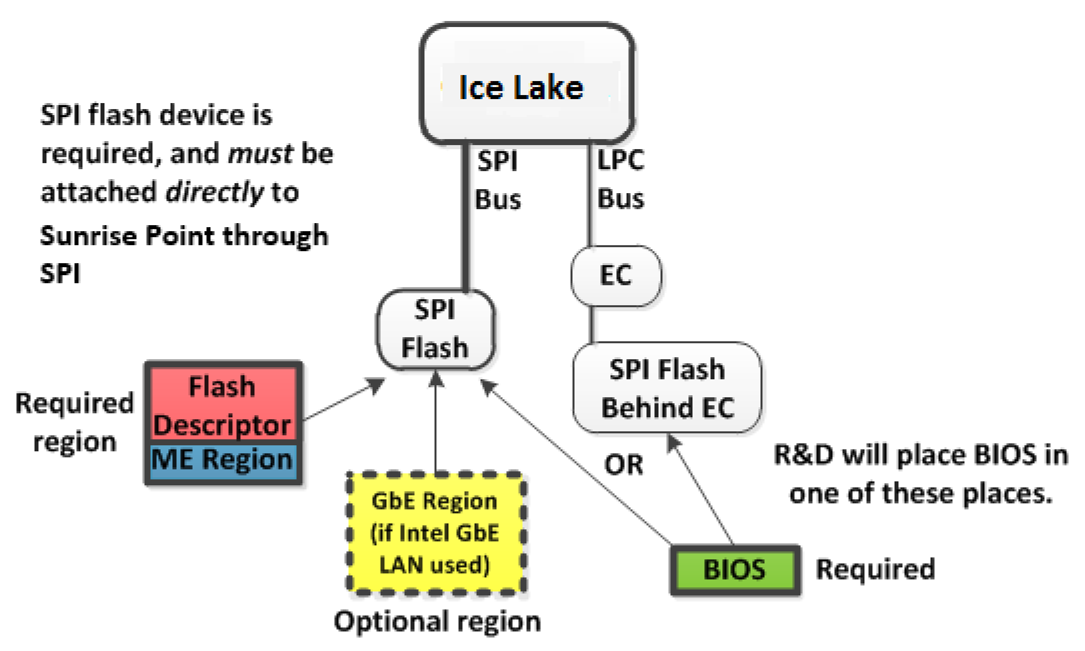

Ice Lake
SPI flash device is required, and *must* be attached *directly* to Sunrise Point through SPI
SPI Bus
LPC Bus
EC
SPI Flash
SPI Flash Behind EC
Required region
Flash Descriptor
ME Region
OR
R&D will place BIOS in one of these places.
GbE Region (if Intel GbE LAN used)
BIOS
Required
Optional region

Figure A-3. Configuration "C" — Desktop / Server / Workstation Only

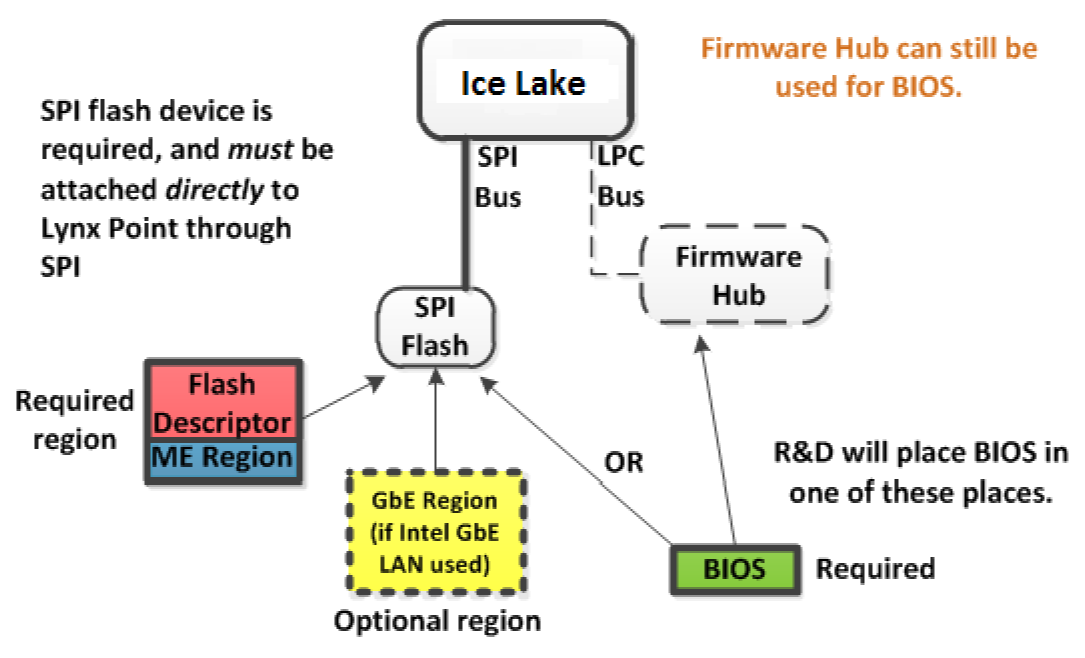
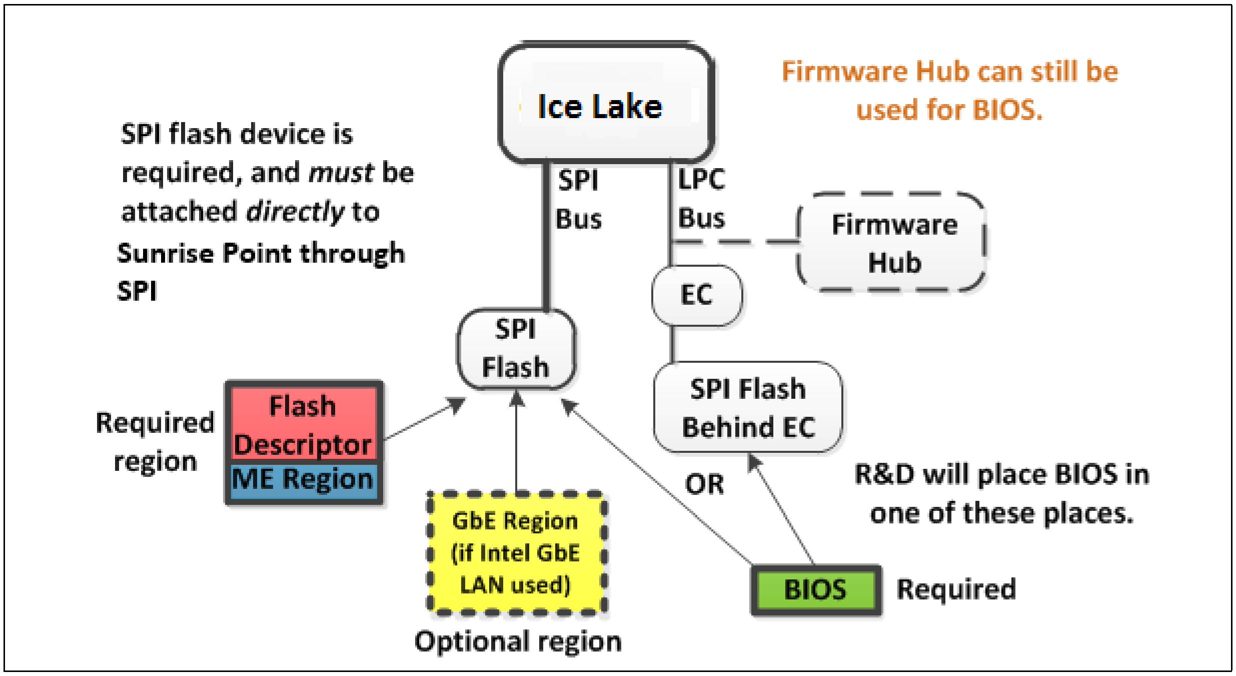

Ice Lake
Firmware Hub can still be used for BIOS.
SPI flash device is required, and *must* be attached *directly* to Lynx Point through SPI
SPI Bus
LPC Bus
Firmware Hub
SPI Flash
Required region
Flash Descriptor
ME Region
OR
R&D will place BIOS in one of these places.
GbE Region (if Intel GbE LAN used)
BIOS
Required
Optional region

Figure A-4. Configuration “D” — Mobile Only


Ice Lake
Firmware Hub can still be used for BIOS.
SPI flash device is required, and *must* be attached *directly* to Sunrise Point through SPI
SPI Bus
LPC Bus
Firmware Hub
EC
SPI Flash
SPI Flash Behind EC
Required region
Flash Descriptor
ME Region
GbE Region (if Intel GbE LAN used)
Optional region
OR
R&D will place BIOS in one of these places.
BIOS
Required

§ §

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 Ice Lake-N SKUs.

Note: Please refer to Ice Lake-H/LP Platform Controller Hub (PCH) External Design Specification (EDS) for details about Ice 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 - ICP-LP

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 - ICP-LP

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 Intel® 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.
1	**Boot Guard VE**	0	1	0	01	1	When Verification is desired but if verification fails the platform will continue to boot with the unverified IBB for a short period, to allow remediation.
2	**Boot Guard VME**	0	1	1	01	1	When Verification and Measured are desired and the asset protection is provided by both TPM protection and a timed remediation period.
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.

Note: Intel® Platform Trust Technology does not support the full TPM functionality requirements and should not be used for Intel® vPro™ based platforms.

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® CSME) Firmware 12 and Intel® Integrated Sensor Solution on Ice Lake Mobile, Ice Lake Desktop, (CDI # WIP) for additional details.

CLSMNF = Close Manufacturing switch used with 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.