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

## Consumer Firmware Bring Up Guide

*February 2020*

**Revision 1.2**

**Intel Confidential**

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

INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH Intel® PRODUCTS. NO LTigerNSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN INTEL'S TERMS AND CONDITIONS OF SALE FOR SUCH PRODUCTS, INTEL ASSUMES NO LIABILITY WHATSOEVER, AND INTL DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF INTEL PRODUCTS INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT.

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

Intel may make changes to specifications and product descriptions at any time, without notTiger. Designers must not rely on the absence or characteristics of any features or instructions marked "reserved" or "undefined". Intel reserves these for future definition and shall have no responsibility whatsoever for conflicts or incompatibilities arising from future changes to them. The information here is subject to change without notTiger.

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

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

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

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

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

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

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

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

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

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

Copyright © 2014-2020, Intel Corporation. All rights reserved.

# Contents


**1 Introduction** ..... 6
- 1.1 Related Documentation ..... 6
- 1.2 Prerequisites ..... 6
- 1.3 Acronyms and Definitions ..... 7
  - 1.3.1 General ..... 7
  - 1.3.2 Intel® Converged Security and Management Engine ..... 8
  - 1.3.3 System States and Power Management ..... 9
- 1.4 Reference Documents ..... 10
- 1.5 Format and Notation ..... 10
- 1.6 Kit Contents ..... 11
- 1.7 External Hardware Requirements for Bring Up ..... 20

**2 Image Creation: Intel® Flash Image Tool** ..... 21
- 2.1 Start Intel®FIT ..... 21
- 2.2 Step-by-Step Guide to Build SPI Flash Image with Intel® FIT Interface ..... 21

**3 Programming SPI Flash Devices and Checking Firmware Status** ..... 139
- 3.1 Flash Burner/Programmer ..... 139
  - 3.1.1 In-Circuit SPI Flash Programming for CRB ..... 139
- 3.2 Flash Programming Tool (Intel® FPT) ..... 139
  - 3.2.1 Intel® FPT Windows* Version ..... 140
- 3.3 Checking Intel® ME Firmware Status ..... 140
- 3.4 Common Bring Up Issues and Troubleshooting Table ..... 142

**A Appendix — Flash Configurations** ..... 143

**B Appendix — Intel® ICCS SKU Support Matrix** ..... 144

**C Appendix — Boot Guard Configuration** ..... 145

**D Appendix — Intel® Platform Trust Technology** ..... 147

**E Appendix — Integrated Sensor Hub (ISH) Public Key Settings** ..... 148

**F Appendix — RVP Platform Specific Settings** ..... 150

## Figures

## Tables


1-1 Number Format Notation ..... 10
1-2 Data Format Notation ..... 10
1-3 Kit Contents ..... 11
2-1 - Initial Screen Layout ..... 22
2-2 - Build Settings ..... 31
2-3 - Flash Layout ..... 33
2-4 - Flash Settings ..... 39
2-5 - Intel® ME Kernel ..... 49
2-6 - Intel® AMT ..... 53
2-7 - Platform Protection ..... 61
2-8 - Integrated Clock Controller ..... 67
2-9 - Networking & Connectivity ..... 73
2-10- Internal PCH Buses ..... 78
2-11- Power ..... 83
2-12- Integrated Sensor Hub ..... 85
2-13- Camera ..... 87
2-14- Debug ..... 88
2-15- CPU Straps ..... 93
2-16- Flex I/O Straps ..... 95
2-17- GPIO ..... 110
2-18- Intel® Precise Touch and Stylus ..... 130
2-19- Download and Execute ..... 131
2-20- FW Update Image Build ..... 133
2-21- Intel® FIT - Build Image ..... 138
3-1 Common Bring Up Issues and Troubleshooting Table ..... 142

# Revision History

| Document Number | Revision Number | Description | Revision Date |
|---|---|---|---|
| | 0.5 | Initial Release | March 2018 |
| | 0.51 | Updated Tiger Lake and Intel®CSME references | February 2019 |
| | 0.7 | Synced to the latest FIT UI layout | February 2019 |
| | 0.71 | Updated to latest RVP defaults | June 2019 |
| | 0.8 | Updated for Alpha release | August 2019 |
| | 0.81 | Added GBST settings | September 2019 |
| | 0.82 | Added Version to IUNIT, PCHC and GBST entries in Flash Layout<br>eSPI / EC Bus Frequency listed 40MHz should have been 48MHz<br>Updated USB2 Port Configuration screen capture<br>Updated OPI Link volt recommended default | October 2019 |
| | 0.83 | Added missing 1.05v value to OPI Link Voltage | November 2019 |
| | 1.0 | Updated to revision 1.0 | December 2019 |
| | 1.1 | Updated screen capture and settings information to latest UI layout<br>Added Platform Appendix section | February 2020 |
| | 1.2 | Added note to USB3 Port Speed Capability settings. | February 2020 |

§ §

# 1 Introduction

This document covers the Intel® Converged Security and Management Engine Firmware (Intel® ME) 15.0 - Consumer / Consumer Firmware bring up procedure. Intel® ME is tied to essential platform functionality — this dependency cannot be avoided for engineering reasons.

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

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

For more details on SPI Flash layout, see the document **Tiger Lake-H / LP SPI Programming Guide** SPI Programming Guide and Appendix A. Once the SPI Flash image is built, it will be programmed to the target based platform and the platform will be booted. This document also covers any tests and checks required to ensure that this boot process is successful and that Intel® ME Consumer FW is operating as expected.

## 1.1 Related Documentation

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

CDI # WIP Intel® Ethernet Connection i2xx

Intel® CSME FW Features

This firmware release includes the following applications:

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

## 1.2 Prerequisites

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

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

This document makes only the following limited assumptions regarding hardware:

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

## 1.3 Acronyms and Definitions

### 1.3.1 General

| Acronym or Term | Definition |
|---|---|
| BIOS | Basic Input Output System |
| DIMM | Dual In-line Memory Module |
| DMI | Direct Media Interface |
| EC | Embedded Controller |
| FPF | Field Programmable Fuses |
| FW | Firmware |
| GbE | Gigabit Ethernet |
| HECI | Host Embedded Controller Interface (aka Intel® MEI) |
| Intel® ICCS | Intel® Integrated Clock Controller Service |
| Intel® CSME | Intel® Converged Security and Management Engine (Intel®ME) |
| Intel® MEI | Intel® Converged Security and Management Engine Interface (Intel® MEI) (renamed from HECI) |
| Intel® PTT | Intel® Platform Trusted Technology (Intel® PPT) |
| Intel® MSS | Intel® Management and Security Status Application |
| KVM | Keyboard, Video, Mouse |
| LAN | Local Area Network |
| MCP | Multi-Chip Package (Central Processing Unit / Platform Controller Hub) |
| NVM | Non-Volatile Memory |
| OOB | Out-of-Band |
| OS | Operating System |
| PAVP | Protected Audio and Video Path |
| PCI | Peripheral Component Interconnect |
| PCIe* | Peripheral Component Interconnect Express |
| PHY | Physical Layer (Networking) |
| RTC | Real Time Clock |
| SBT | Intel® Small Business Technology |
| SMBus | System Management Bus |

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

## 1.3.2 Intel® Converged Security and Management Engine

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

### 1.3.3 System States and Power Management

| Acronym or Term | Definition |
|---|---|
| G3 | A system state of Mechanical Off where all power is disconnected from the system. G3 power state does not necessarily indicate that RTC power is removed. |
| CM0 | Intel® Converged Security and Management Engine firmware power state where all hardware power planes are activated. The host power state is S0. |
| CM3 | Intel® Converged Security and Management Engine power state where the host is in Sx. The processor DRAM Controller is turned off and DRAM power stays in off/self refresh mode. There is no UMA usage in CM3 state. Less than 1MB of SRAM used for code and data. Code is executed off of flash takes ~1mS. |
| CM0-PG | Core Well Powered; Intel® ME Well Powered; (Intel® ME core not consuming power) DRAM available. |
| CM3-PG | An Intel® ME Firmware power state where no power is applied to the Converged Security and Management Engine subsystem. (Intel® ME firmware is shut down). |
| OS Hibernate | System state where the OS state is saved on the hard drive. |
| S0 | A system state where power is applied to all HW devices and the system is running normally. |
| S1, S2, S3 | A system state where the host CPU is halted but power remains available to the memory system (memory is in self-refresh mode). |
| S4 | A system state where the host CPU and memory are not active. |
| S5 | A system state where all power to the host system is off, however the power cord (and/or battery in mobile designs) is still connected. |
| Shut Down | Equivalent to the S5 state. |
| Snooze Mode | Intel® Converged Security and Management Engine activities are mostly suspended to save power. The Intel® Converged Security and Management Engine monitors HW activities and can restore its activities depending on the HW event. |
| Standby | System state where the OS state is saved in memory and resumed from the memory when mouse/keyboard is clicked. |
| Sx | All S states which are different than S0. |

## 1.4 Reference Documents

| Document | Doc Number/ Location* |
|---|---|
| *Tiger Lake Intel® Converged Security and Management Engine (Intel® CSME) and Embedded Controller Interaction Product Specification Revision 0.5* | 549024 / CDI |
| *Intel® Converged Security and Management Engine BIOS Writers Guide* | TBD / * |
| *Intel® Converged Security and Management Engine (Intel® CSME) 15 SKU Firmware* Consumer *Compliance Guide for Tiger Lake PCH-H/LP Chipset Family - Tiger Lake Platform Compliancy and Testing Guide - Revision x.x* | TBD / CDI |

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

## 1.5 Format and Notation

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

### Table 1-1. Number Format Notation

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

### Table 1-2. Data Format Notation

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

## 1.6 Kit Contents

The Intel® CSME 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 8)

| File or [Directory] | Content Description |
|---|---|
| [root] | Root directory |
| [Installers] | |
| [3rd party Licenses in Security SW] | |
| ACE-TAO-CIAO.pdf | Copyright and Licensing Information for ACE(TM), TAO(TM), and CIAO(TM) |
| Apache-Xerces-C++-XML-Parser.txt | Apache license for C++ XML parser |
| Inno Setup License.txt | Inno Setup License |
| LICENSE.libmei | libmei BSD License |
| Microsoft Windows Classic Samples.txt | Microsoft Windows Classic Samples License |
| Microsoft winfile MIT.txt | Microsoft winfile MIT License |
| openwsman.pdf | Intel openwsman License |
| Windows driver samples.txt | Microsoft driver samples License |
| WixLicenseNote.txt | Microsoft Wix License |
| [ME_SW_DCH] | |
| IntelMEFWVer.dll | DLL file containing software version information |
| mup.xml | XML file containing software version and driver information |
| SetupME.exe | DCH software installer executable |
| [ME_SW_MSI] | |
| IntelMEFWVer.dll | DLL file containing software version information |
| mup.xml | XML file containing software version and driver information |
| SetupME.exe | MSI software installer executable |
| [MEI-Only Installer MSI] | |
| IntelMEFWVer.dll | DLL file containing MEI version information |
| mup.xml | XML file containing MEI software version and driver information |
| SetupME.exe | Intel® MEI software installer executable |
| [WindowsDriverPackages] | |
| [ICLS] | Intel® Capability Licensing Service folder |
| iclsClient.cat | iCLS CAT file |
| iclsClient.inf | UWD iCLS Client INF |
| [JHI] | |
| [IotCorePackages] | |
| Intel.Drivers.DAL.cab | Intel® Dynamic Application Loader CAB file |
| [Win10] | |
| DAL.cat | Intel® Dynamic Application Loader CAT file |

## Table 1-3. Kit Contents (Sheet 2 of 8)

| File or [Directory] | Content Description |
|---|---|
| DAL.inf | Intel® Dynamic Application Loader INF file |
| JHI.dll | Intel® Dynamic Application Loader 32bit DLL file |
| jhi_service.exe | Intel® Dynamic Application Loader Windows Services executable file |
| JHI64.dll | Intel® Dynamic Application Loader 64bit DLL file |
| SpoolerApplet.dalp | Intel® Dynamic Application Loader Spooler Applet |
| TEEManagement.dll | Intel® Dynamic Application Loader TEE Management 32bit DLL |
| TEEManagement64.dll | Intel® Dynamic Application Loader TEE Management 64bit DLL |
| [LMS] | |
| [Certificates] | |
| B2C067A6568D27791074C3F5C5A58966D6F12E36.cer | LMS Certificates files |
| BBAF7E023DFAA6F13C848EADEE3898ECD93232D4.cer | |
| BF4E419CC0A20D33947C2A04867B27DE63A2174F.cer | |
| SFIP Production SHA256.cer | |
| [Templates] | |
| 5710ABF3E156BFE90FD5C8E21606788DA4D69ADD.data | LMS Template file |

## Table 1-3. Kit Contents (Sheet 3 of 8)

| File or [Directory] | Content Description |
|---|---|
| 1200_PD_PFU.BIN | Intel® CSME 12.x Firmware Update binaries |
| 1200_PP_PFU.BIN | |
| 1300_PD_PFU.BIN | Intel® CSME 13.x Firmware Update binaries |
| 1300_PP_PFU.BIN | |
| 1400_PD_PFU.BIN | Intel® CSME 14.x Firmware Update binaries |
| 1400_PP_PFU.BIN | |
| 1500_PD_PFU.BIN | Intel® CSME 15.x Firmware Update binaries |
| 1500_PP_PFU.BIN | |
| ACE.dll | ADAPTIVE Communication Environment(TM) DLL |
| ComEventHandler.dll | COM Event Handler DLL |
| Common.dll | Common DLL |
| Configurator.dll | Configurator DLL |
| EventManager.dll | Windows Event Manager DLL |
| FWUpdateLib_10.dll | Firmware Update Library DLL for Intel® ME 10.x |
| FWUpdateLib_11.dll | Firmware Update Library DLL for Intel® ME 11.x |
| FWUpdateLib_12.dll | Firmware Update Library DLL for Intel® ME 12.x - 15.x |
| GmsCommon.dll | GMS Common DLL |
| HistoryEventHandler.dll | History Event Handler DLL |
| HostChangesNotificationService.dll | Host Changes Notification Service DLL |
| IPRefreshService.dll | IP Refresh Service DLL |
| LMS.cat | LMS CAT file |
| LMS.exe | LMS Service executable |
| LMS.inf | LMS INF file |
| Log.txt | LMS Log file |
| PartialFWUpdateService.dll | Partial Firmware Update Service DLL |
| PortForwardingService.dll | Port Forwarding Service DLL |
| PowerOperationsService.dll | Power Operation Service DLL |
| SharedStaticIPService.dll | Shared Static IP Service DLL |
| SoapServerService.dll | Soap Server Service DLL |
| StatusEventHandler.dll | Status Event Handler DLL |
| TimeSyncService.dll | Time Sync Service DLL |
| WiFiProfileSyncService.dll | WiFi Profile Sync Server DLL |
| WinLogEventHandler.dll | Windows Log Event Handler DLL |
| WMIEventHandler.dll | WMI Event Handler DLL |
| WsmanClient.dll | WSMAN Client DLL |
| [MEI] | |
| [Win7] | |
| [x64] | |
| TeeDriverx64.sys | Windows 7 64bit MEI TeeDriver file |
| [x86] | |

## Table 1-3. Kit Contents (Sheet 4 of 8)

| File or [Directory] | Content Description |
|---|---|
| TeeDriver.sys | Windows 7 32bit MEI TeeDriver file |
| heci.cat | Windows 7 MEI TeeDriver CAT file |
| heci.inf | Windows 7 MEI TeeDriver INF file |
| [Win8] | |
| [x64] | |
| TeeDriverW8x64.sys | Windows 8 64bit MEI TeeDriver file |
| [x86] | |
| TeeDriverW8.sys | Windows 8 32bit MEI TeeDriver file |
| heci.cat | Windows 8 MEI TeeDriver CAT file |
| heci.inf | Windows 8 MEI TeeDriver INF file |
| [Win10] | |
| [x64] | |
| TeeDriverW10x64.sys | Windows 10 64bit MEI TeeDriver file |
| [x86] | |
| TeeDriverW10.sys | Windows 10 32bit MEI TeeDriver file |
| heci.cat | Windows 10 MEI TeeDriver CAT file |
| heci.inf | Windows 10 MEI TeeDriver INF file |
| [MEI_iCLS] | |
| ReleaseNotes.txt | iCLS Client release notes |
| [SOL] | |
| mesrl.cat | Serial Over LAN CAT file |
| mesrl.inf | Serial Over LAN INF file |
| [TGP-LP] | |
| [3rd party Licenses in Security FW] | |
| Apache Harmony Apache Version 2.0, January 2004 w header.txt | Apache Harmony Apache Version 2.0 License |
| Apache-Xerces-Java-XML-Parser.txt | Apache Xerces Java XML Parser License |
| ConvertUTF unicode license.txt | Convert UTF Unicode License |
| CxImage license complete.txt | CxImage License |
| HTTP Client C MIT license.txt | HTTP Client MIT License |
| llvm.org University of Illinois_NCSA.txt | Compiler_RT MIT License |
| Microsoft TPM 2.0 BSD Two Clause License.txt | TPM 2.0 BSD Two Clause Microsoft License |
| Minix 3.pdf | Minix 3 operating system License |
| MIT Kerberos for Windows.pdf | Kerberos for Windows MIT License |
| newlib_licenses.txt | Newlib License |
| Synopsys UFS Host Controller OS.pdf | Synopsys UFS Host Controller OS License |
| wpa supplicant license.txt | WPA Supplicant License |
| zlib license.txt | Zlib compression library License |
| [FWU_Prestitched] | |
| Cons_Prestitched_FWUpdate.bin | Consumer Firmware Updated Pre-stitched binary |
| Corp_Prestitched_FWUpdate.bin | Corporate Firmware Updated Pre-stitched binary |

## Table 1-3. Kit Contents (Sheet 5 of 8)

| File or [Directory] | Content Description |
|---|---|
| [Image Components] | |
| [CSME] | |
| [Silicon] | |
| [LP] | |
| [A0] | |
| [PreProduction] | |
| CSME_FW_Consumer_TGP-LP_A0.bin | Intel® CSME firmware image (**Non-Production FW**) - supports **un-fused** Tiger Lake PCH-LP Platform I/O MCP stepping:<br>• Un-fused (Super SKU)<br>***Note:*** For PAVP Testing, you must match Production FW with Production Part and Non-Production FW with Non-Production Parts. |
| [PCHC] | |
| pchc_TGL_PCHC_15.0.0.xxxx.bin | Un-signed PCH Configuration binary |
| pchc_TGL_PCHC_15.0.0.xxxx_signed.bin | Signed PCH Configuration binary |
| [PMC] | |
| TGPLP_Z0_PMC_FW_150.01.00.xxxx.bin | PMC firmware binary |
| [TCSS] | |
| [IOM] | |
| iomfw_v10.000c.0.0_signed.bin | IOM firmware binary |
| [PHY] | |
| TcssPartition_v2.1017.bin | PHY firmware binary |
| [Retimer] | |
| BBR_CDR_A1_TGL_PORTS_0_1_rev2_2_sign.bin | Retimer firmware binary for TCSS Ports 0 and 1 |
| BBR_CDR_A1_TGL_PORTS_2_3_rev2_2_sign.bin | Retimer firmware binary for TCSS Ports 2 and 3 |
| [TBT] | |
| TBT_TGL_A0_REV1_PRE16_signed.bin | Thunderbolt™ firmware binary |
| TGL-LP Consumer Bring Up Guide.pdf | This document |
| TGL-LP Corporate Bring Up Guide.pdf | |
| Tigerlake-LP Client SPI Programming Guide.pdf | |
| [Tools] | |
| [ICC Tools] | |
| [ICC SDK] | |
| [Windows64] | |
| icc_sdk_api.h | Integrated Clock Controller SDK API .H file |
| sdkLib.lib | Integrated Clock Controller SDK Library file |
| [WDT Driver] | |
| [ICCWDT_11.7.0.1000_19H1_Cert] | |
| [Win7] | |
| [ICCWDT.Dev.Install] | |

## Table 1-3. Kit Contents (Sheet 6 of 8)

| File or [Directory] | Content Description |
|---|---|
| [ICCWDT_Driver] | |
| [x64] | |
| iccwdt.sys | |
| WdfCoInstaller01009.dll | |
| iccwdt.cat | |
| iccwdt.inf | |
| iccwdt.sys | |
| WdfCoInstaller01009.dll | |
| [x64] | |
| DIFxAPI.dll | ICC Watch Dog Timer 64bit driver install frameworks API DLL |
| Drv64.exe | |
| DIFxAPI.dll | ICC Watch Dog Timer 32bit driver install frameworks API DLL |
| license.txt | ICC Watch Dog Timer SDK License |
| Readme.txt | ICC Watch Dog Timer Readme file |
| Setup.cfg | ICC Watch Dog Timer Setup configuration file |
| setup.exe | ICC Watch Dog Timer Setup executable |
| Setup.if2 | ICC Watch Dog Timer IF2 file |
| [ICCWDT.Install] | |
| [Win10] | |
| [ICCWDT.Dev.Install] | |
| [ICCWDT.Install] | |
| Intel(R) ME Firmware ICC Tools User Guide.pdf | Integrated Clock Controller Tools User guide |
| [System Tools] | |
| [Documentation] | |
| Signing and Manifesting User Guide.pdf | Signing and Manifest Users Guide |
| SLA_TOOLS.PDF | MEInfo and FWUpdLcl Redistribution License |
| TGL_System_Tools_UG.pdf | System Tools User guide |
| VSCCommn_bin Content.pdf | List of supported SPI Flash devices with specific Flash parameters. |
| [FIT] | |
| Windows32] | |
| fit.exe | Intel® Flash Image Tool |
| vsccommn.bin | Binary containing the supported SPI parts. |
| [FPT] | |
| [Efi64] | |
| Fpt.efi | 64bit uEFI Intel® Flash Programming Tool executable. |
| [Windows64] | |
| FPTW64.exe | Windows 64bit Intel® Flash Programming Tool executable. |

## Table 1-3. Kit Contents (Sheet 7 of 8)

| File or [Directory] | Content Description |
|---|---|
| Idrvdll32e.dll | Windows DLL files for Intel® Flash Programming Tool. |
| Pmxdll32e.dll | |
| [FWUpdate] | |
| [Efi64] | |
| errorlist.c | 64bit uEFI C Source and Library files for Firmware Update. |
| errorlist.h | |
| fwudef.h | |
| FwUpdateEfiLib.lib | |
| fwupdatelib.h | |
| fwupdatelibdeprecated.h | |
| FWUpdLcl.efi | 64bit uEFI Firmware Update executable. |
| [Windows64] | |
| errorlist.c | Windows 64bit C Source and Library and Sample code files for Firmware Update. |
| errorlist.h | |
| fwudef.h | |
| FwUpdateEfiLib.lib | |
| fwupdatelib.h | |
| fwupdatelibdeprecated.h | |
| FWUpdateSample.c | |
| FWUpdLcl64.exe | Windows 64bit Firmware Update executable. |
| [FWUpdate_RS] | |
| [Efi64] | |
| errorlist.c | Reduced size 64bit uEFI C Source and Library files for Firmware Update. |
| errorlist.h | |
| fwudef.h | |
| FwUpdateEfiLib.lib | |
| fwupdatelib.h | |
| fwupdatelibdeprecated.h | |
| FWUpdLcl.efi | Reduced size 64bit uEFI Firmware Update executable. |
| FWUpdLclApp.c | Reduced size 64bit uEFI Firmware Update Application sample. |
| FWUpdLclAppDeprecated.c | |
| [MEInfo] | |
| [Efi64] | |
| MEInfo.efi | 64bit uEFI Intel® ME Information executable. |
| [Windows64] | |
| MEInfoWin64.exe | Window 64bit Intel® ME Information executable. |
| Idrvdll32e.dll | Windows DLL files for Intel® ME Information Tool. |
| Pmxdll32e.dll | |
| [MEManuf] | |
| [Efi64] | |

### Table 1-3. Kit Contents (Sheet 8 of 8)

| File or [Directory] | Content Description |
|---|---|
| MEManuf.efi | 64bit uEFI Intel® ME Manufacturing test tool executable. |
| [Windows64] | |
| MEManufWin64.exe | Windows 64bit Intel® ME Manufacturing test tool executable. |
| Idrvdll32e.dll | Windows DLL files for Intel® ME Information Tool. |
| Pmxdll32e.dll | |
| [MEU] | |
| [Windows32] | |
| meu.exe | Windows 32bit Intel® Manifest Extension Utility executable. |

## 1.7 External Hardware Requirements for Bring Up

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

| Windows* OS System | Flash Burner | DOS Bootable USB Key |
|---|---|---|
| | | |
| **Equipment:**<br>• Laptop or desktop that supports win32 applications<br><br>**Purpose:**<br>• Will run firmware image assembly and build process software. | **Equipment:**<br>• (Optional) For platforms that don't boot, a Flash Chip Programmer will be required<br>• For platforms that can boot to DOS or Windows*, a Intel® FPT is provided in this kit<br><br>**Purpose:**<br>• Will burn firmware images onto the target system Flash device(s). | **Equipment:**<br>• A DOS Bootable USB Key (Size > 512 MB)<br><br>**Purpose:**<br>• 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.<br>• Or will be used to transfer a firmware image onto a Flash burner. |

§ §

# 2 Image Creation: Intel® Flash Image Tool

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

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

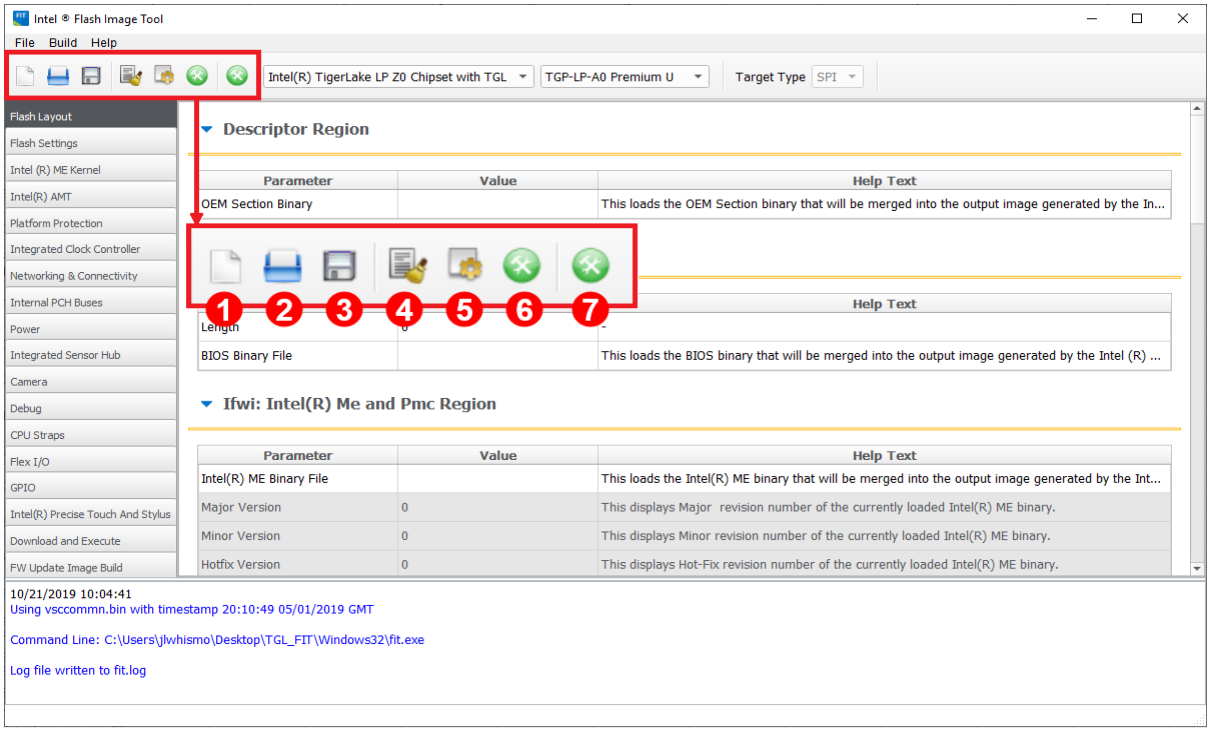
***Note:*** The Flash Image Tool may be updated throughout the release cycles. As a general rule, please ensure you use the tools, images and other content from the same kit and refrain from using different version tools.

## 2.1 Start Intel®FIT

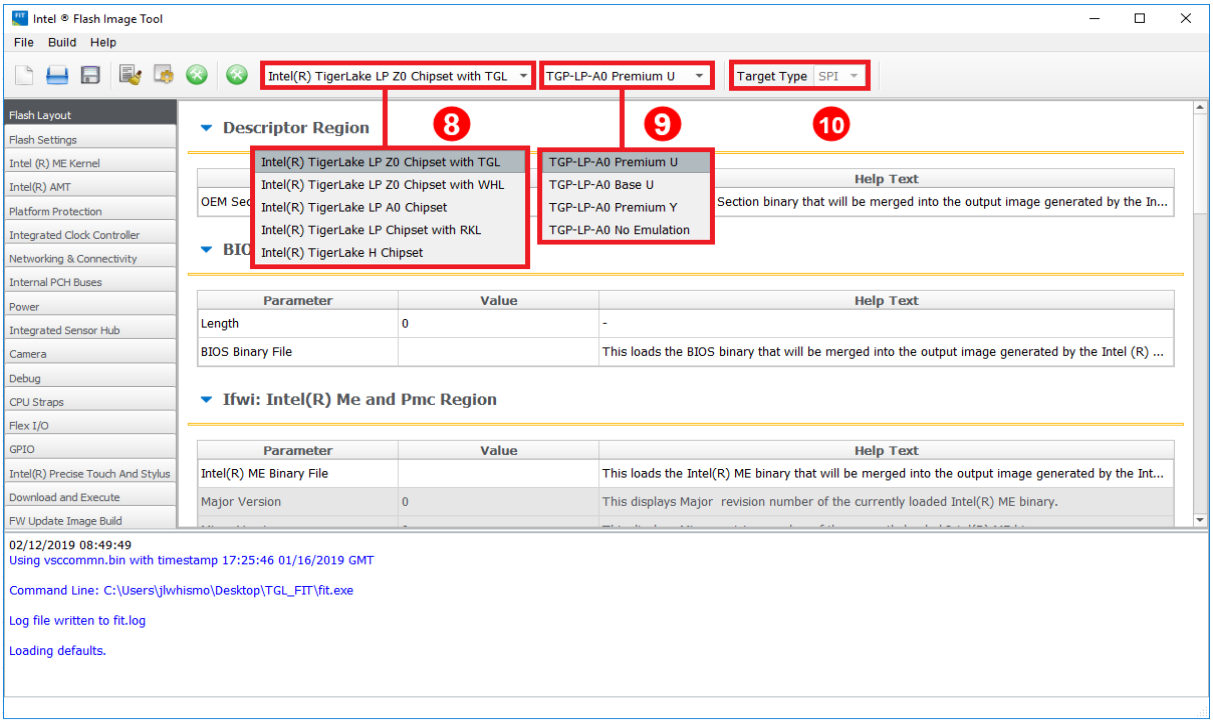
1. Invoke Intel® Flash Image Tool. Using Explorer*, navigate to **[root]\Tools\System Tools\Flash Image Tool**. Verify that the directory contents are correct (see Section 1.6). Double-click **FIT.exe**.
2. **NOTE:** In the tables below, where default settings are listed for TGL LP/H, if the value is the same one value will be listed. If there is a different default value when the program loads with either platform, both values will be listed to show the difference.

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

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

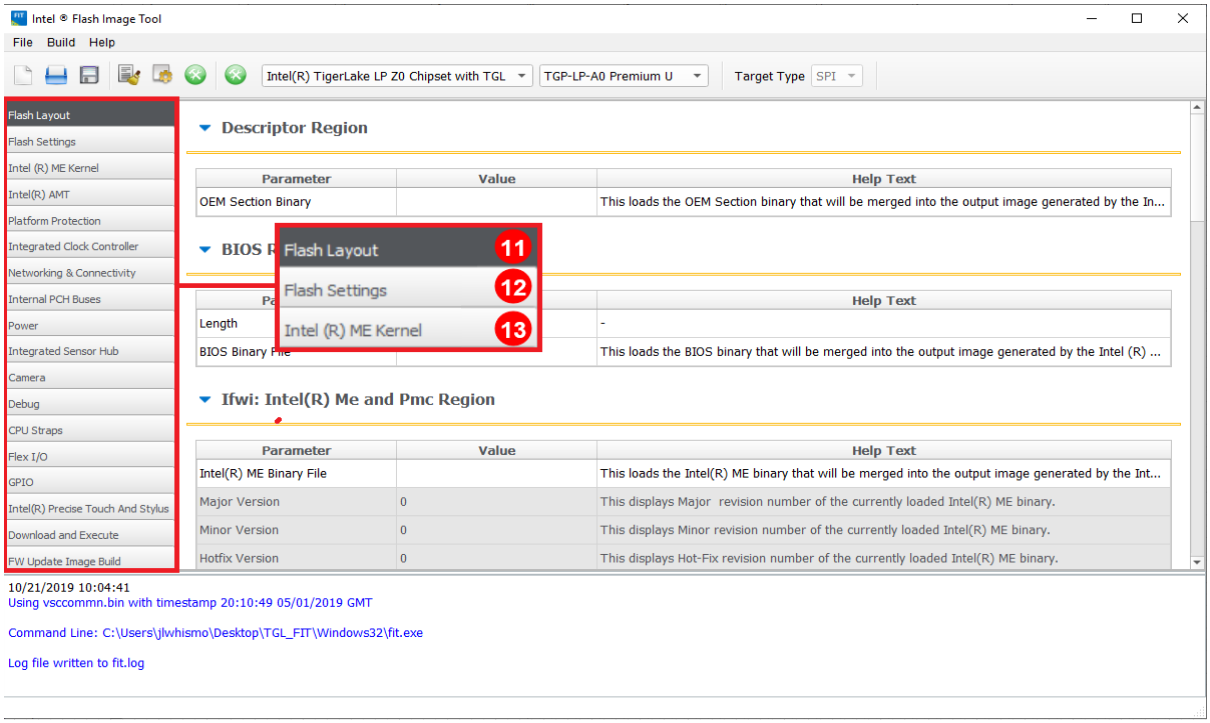
| # | Label | Contents |
|---|---|---|
|  | | |
| 1 | **New** | This button labeled 'New' on rollover allows opening of a new session with default values |
| 2 | **Open** | This button labeled 'Open' on rollover allows opening of an xml or bin file |
| 3 | **Save** | This button labeled 'Save' on rollover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

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

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

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

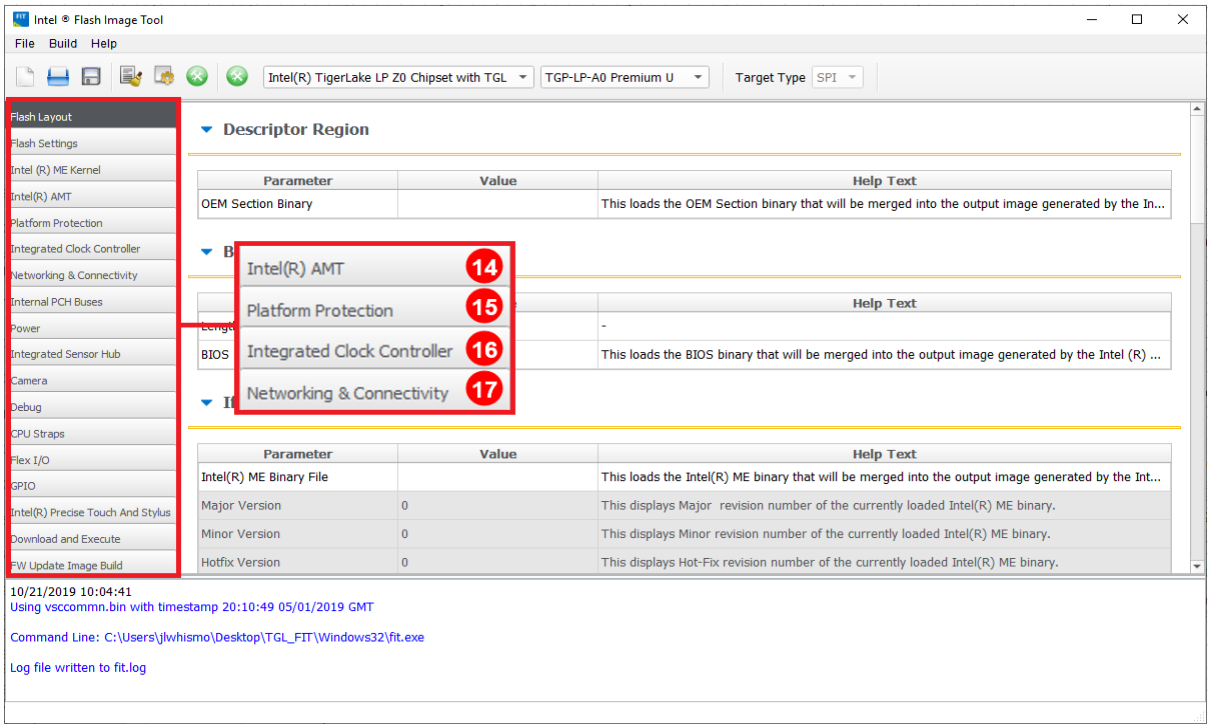
| # | Label | Contents |
|---|---|---|



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

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

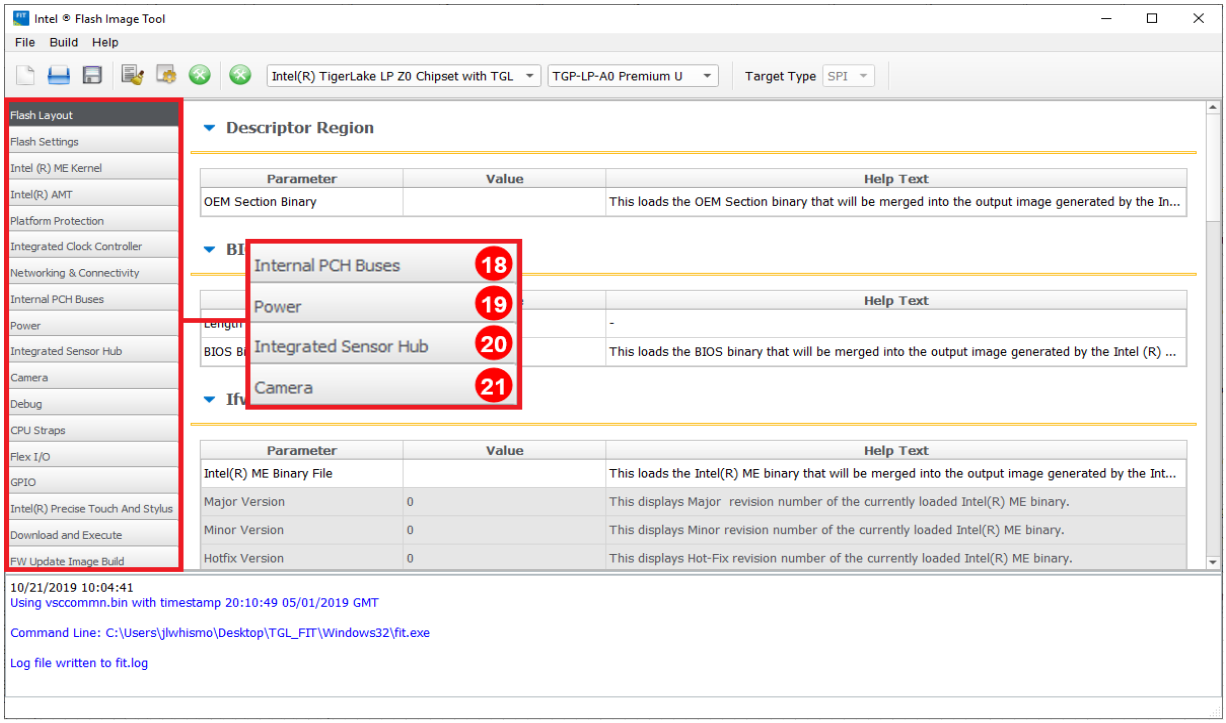
## Table 2-1. - Initial Screen Layout (Sheet 5 of 9)

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

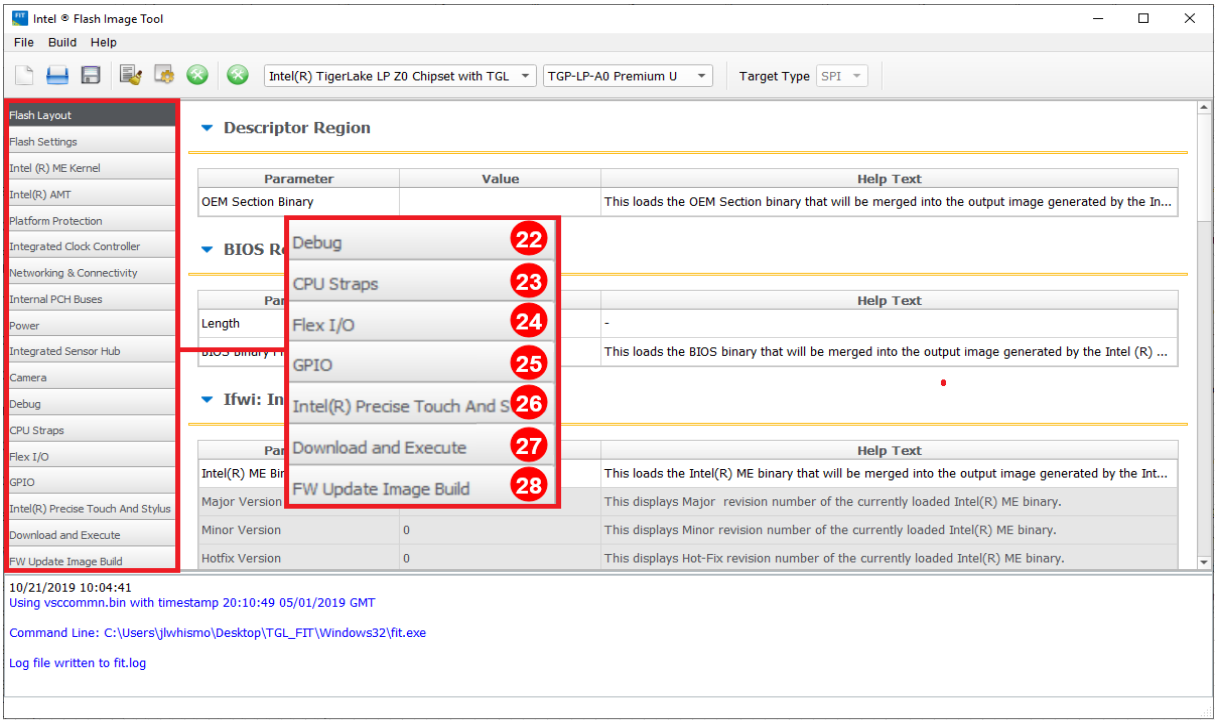
## Table 2-1. - Initial Screen Layout (Sheet 6 of 9)

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

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

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

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

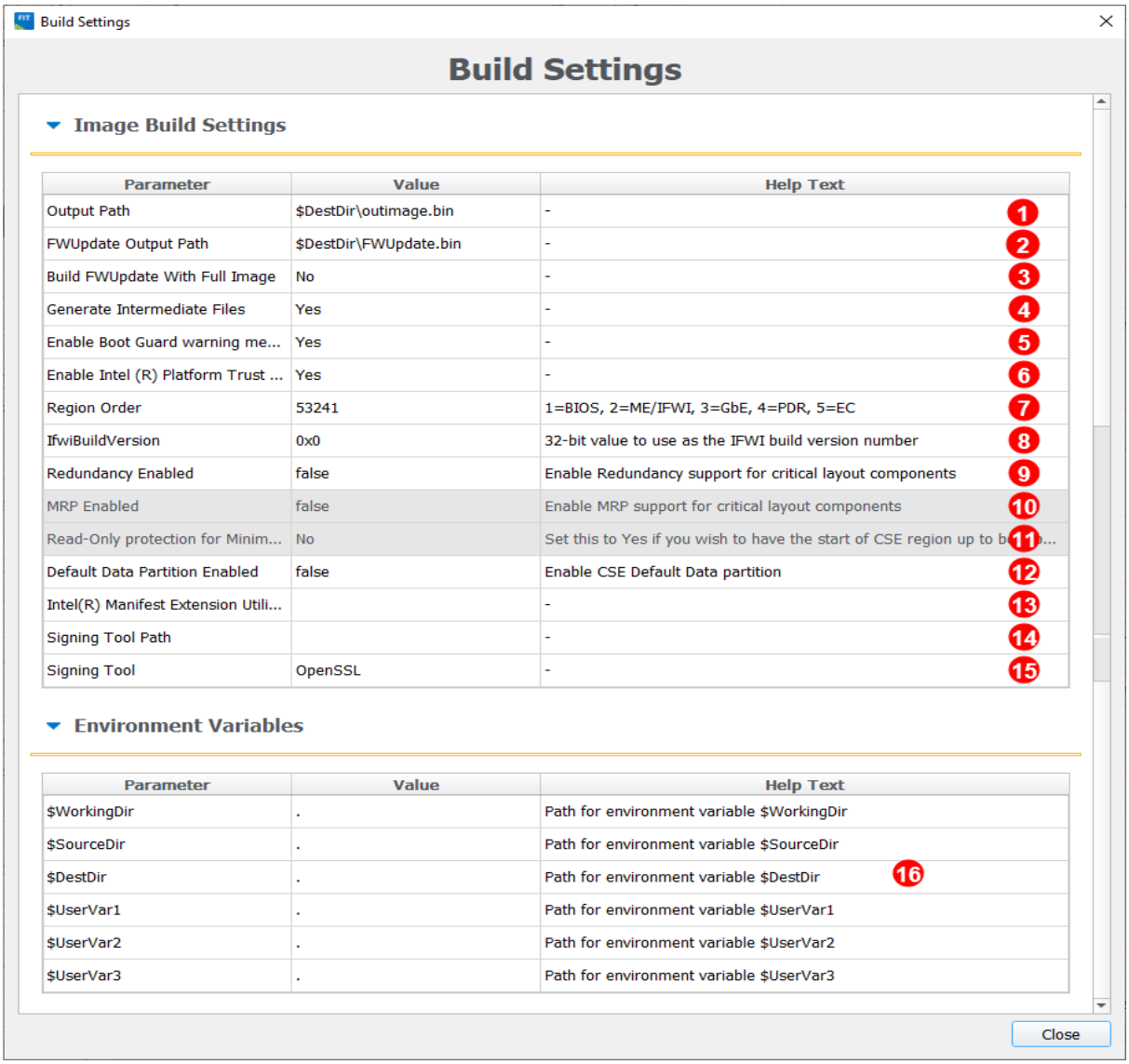
| # | Label | Contents |
|---|---|---|
|  | | |
| 22 | **Debug Tab** | Debug which contains (see Table 2-14):<br>• IDLM<br>• Delayed Authentication Mode Configuration<br>• Intel® Trace Hub Technology<br>• Intel® ME Firmware Debugging Overrides<br>• Direct Connection Interface Configuration<br>• eSPI Freature Overrides<br>• Early USB DBC over Type-A Configuration<br>• TRC Emulation |
| 23 | **CPU Straps Tab** | CPU Straps which contain a detailed list of parameters (see Table 2-15)<br>• CPU Straps |
| 24 | **Flex I/O Tab** | Flex I/O which contains (see Table 2-16):<br>• PCIe Lane Reversal Configuration<br>• PCIe Port Configuration<br>• SATA / PCIe Combo Port Configuration<br>• USB3 Port Configuration<br>• USB2 Port Configuration<br>• Type-C Subsystem Configuration<br>• Thunderbolt Configuration |
| 25 | **GPIO Tab** | GPIO which contains (see Table 2-17):<br>• ME Feature Pins<br>• Touch Controller Pins<br>• GPIO VCCIO Voltage Control<br>• Thunderbolt LSx/BSSB-LS Configuration |

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

| # | Label | Contents |
|---|---|---|
| 26 | **Intel® Precise Touch and Stylus** | Intel® Precise Touch and Stylus which contains (see Table 2-18):<br>• Integrated Touch Configuration<br>• Intel® Integrated Touch and Stylus Configuration |
| 27 | **Download and Execute** | Download and Execute which contains (see Table 2-19):<br>• DnX Configuration<br>• USB Descriptor |
| 28 | **FW Update Image Build** | FW Update Image Build which contains (see Table 2-20):<br>• ME Image<br>• PMC Image<br>• OEM KM Image<br>• IOM Image<br>• NPHY Image<br>• TBT Image<br>• ISH Image<br>• INUIT Image<br>• PCHC Image |
| | **Console Window Area** | Displays opening messages, log file entries, and build activity messages |

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

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




| Parameter | 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 |
| Redundancy Enabled | false | Enable Redundancy support for critical layout components | 9 |
| MRP Enabled | false | Enable MRP support for critical layout components | 10 |
| Read-Only protection for Minim... | No | Set this to Yes if you wish to have the start of CSE region up to b... | 11 |
| Default Data Partition Enabled | false | Enable CSE Default Data partition | 12 |
| Intel(R) Manifest Extension Utili... | | - | 13 |
| Signing Tool Path | | - | 14 |
| Signing Tool | OpenSSL | - | 15 |

| Parameter | Value | Help Text | # |
|---|---|---|---|
| $WorkingDir | . | Path for environment variable $WorkingDir | |
| $SourceDir | . | Path for environment variable $SourceDir | |
| $DestDir | . | Path for environment variable $DestDir | 16 |
| $UserVar1 | . | Path for environment variable $UserVar1 | |
| $UserVar2 | . | Path for environment variable $UserVar2 | |
| $UserVar3 | . | Path for environment variable $UserVar3 | |

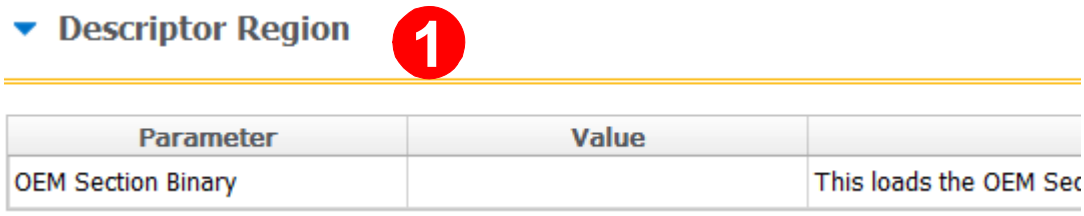
| # | Parameter | CRB | Values |
|---|---|---|---|
| 1 | **Output Path** | | Double click to the right of outimage.bin and click to get browse button to specify path and name of file to create for the build - default is outimage.bin in the same folder as Intel® FIT tool |
| 2 | **FWUpdate Output Path** | | 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 2)

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

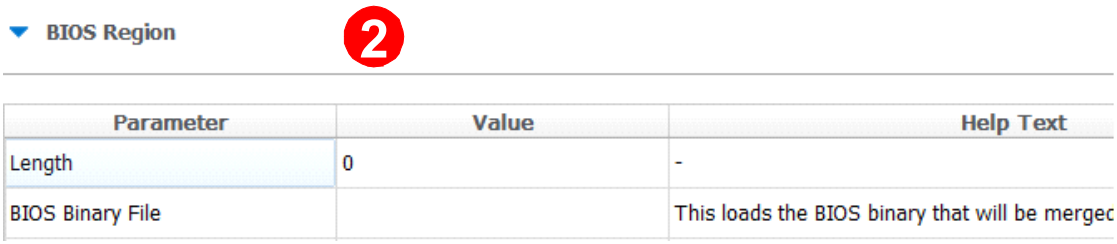
## Table 2-3. - Flash Layout (Sheet 1 of 6)

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




| # | Parameter | Platform | Settings |
|---|---|---|---|
| 1 | **OEM Section Binary**<br>This loads the OEM Section binary that will be merged into the output image generated by the Intel® FIT tool. | UP4<br>UP3 | OEM Binary (optional) |

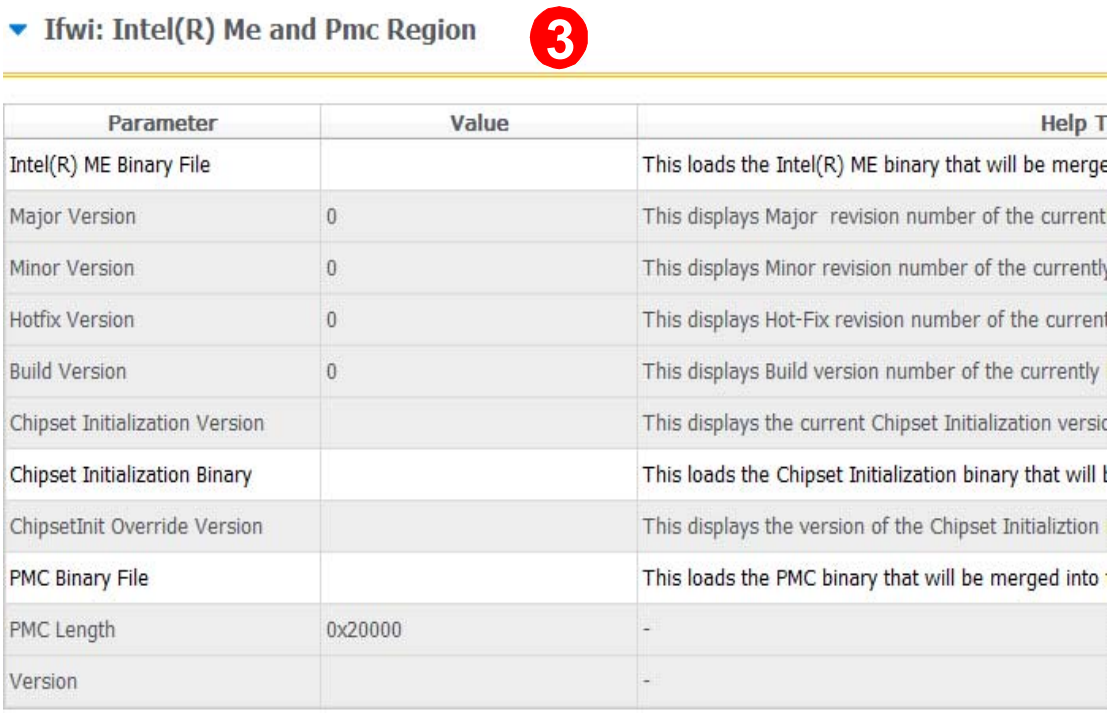
**Click on Flash Layout in the left tabs menu> BIOS Region is expanded by default:**




| # | Parameter | Platform | Settings |
|---|---|---|---|
| 2 | **BIOS Region** | | |
| | **BIOS Region - Length -**This displays the length of the BIOS binary.<br>***Note:*** This value will be automatically populated by Intel® FIT during image build. | | |
| | **BIOS Binary File**<br>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. | UP4<br>UP3 | biosimage.bin<br>biosimage.bin |

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

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



Ifwi: Intel(R) Me and Pmc Region 3

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

| # | Parameter | Platform | Settings |
|---|---|---|---|
| 3 | **Ifwi: Intel® ME and PMC Region** | | |
| | **Intel® CSME Binary File**<br>Navigate to your **Source Directory** (as specified in Table 2-2) and switch to the Intel® CSME subdirectory. Choose the appropriate Intel® CSME Firmware binary image. This loads the Intel® CSME binary that will be merged into the into the output image generated by the Intel® FIT tool.<br>**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.<br>**Note:** If loading meimage.bin file, check that the ME region is enabled in tool before building image. | UP4<br>UP3 | meimage.bin<br>meimage.bin |
| | **Major Version -** This displays Major revision number of the currently loaded Intel® CSME binary. | | |
| | **Minor Version -** This displays Minor revision number of the currently loaded Intel® CSME binary. | | |
| | **Hotfix Version -** This displays Hot-Fix revision number of the currently loaded Intel® CSME binary. | | |
| | **Build Version -** This displays Build version number of the currently loaded Intel® CSME binary. | | |
| | **Chipset Initialization Version -** This displays the current Chipset Initialization version contained in the currently loaded Intel® CSME binary. | | |

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

| | | | |
|---|---|---|---|
| | **Chipset Initialization Binary -** This loads the Chipset Initialization binary that will be merged into the output image generated by the Intel® FIT. If specified, this will override the version contained in the Intel® CSME binary to align with the values programmed by BIOS.<br><br>***Note:*** When BIOS passes new Chipset Initialization settings to ME, a Global Reset is initiated (only required on the first boot, subsequent boots will not incur a global reset). This allows for the new settings to be stored in the ME Region and programmed into the PCH. This global reset can be avoided by loading the proper chipset initialization binary in to the ME Region when building the image that aligns with the values in BIOS. The Chipset Initialization Binary will be included in BIOS RC package. If BIOS contains an older version of Chipset Initialization settings ME will be updated at boot with the older settings regardless of any newer settings being present in firmware. In order to avoid this problem and the additional Global Reset customers should ensure that both BIOS and ME are updated with same Chipset Initialization binary. | UP4<br>UP3 | Chipset.bin (Optional)<br>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. | UP4<br>UP3 | PMC.bin<br>PMC.bin |
| | **PMC Length -** This displays the length of the PMC binary.<br>***Note:*** This value will be automatically populated by Intel® FIT during image build. | | |
| | **Version** - This displays the version of PMC | | |
| **Click on Flash Layout in the left tabs menu> EC Region is expanded by default:** | | | |

EC Region 4

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

| # | Parameter | Platform | Settings |
|---|---|---|---|
| 4 | **EC Region** | UP4<br>UP3 | 0<br>0 |
| | **EC Region - Length**<br>***Note:*** This value will be automatically populated by Intel® FIT during image build. | | |
| | **EC Binary File**<br>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. | UP4<br>UP3 | EC Binary<br>EC Binary |
| | **EC Region Enable**<br>**Values: Enabled / Disabled**<br>This option allows the user to enable or disable the Embedded Controller data region. | UP4<br>UP3 | Enabled<br>Enabled |
| | **EC Region Pointer File**<br>This loads a binary file containing the 16 byte Embedded Controller pointer value at the start of the flash descriptor | UP4<br>UP3 | EC Pointer Binary<br>EC Pointer Binary |
| **Click on Flash Layout in the left tabs menu> GbE Region is expanded by default:** | | | |

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

▼ GbE Region 5

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

| # | Parameter | Platform | Settings |
|---|---|---|---|
| 5 | **GbE Region**<br>This loads the Intel® Integrated LAN binary that will be merged into the output image generated by the Intel® FIT tool. | | |
| | **GbE Region - Length**<br>***Note:*** This value will be automatically populated by Intel® FIT during image build. | | |
| | **GbE Binary File**<br>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.<br>**Note:** If loading gbeimage.bin file, check that the GbE region is enabled in tool before building image. | UP4<br>UP3 | gbeimage.bin<br>gbeimage.bin |
| | **GbE Region Enable**<br>**Values: Enabled / Disabled -** This option allows the user to enable or disable the Gigabit Ethernet Region.<br>**NOTE:** If choosing a configuration that **does not include the GbE LAN the following settings need to be adjusted**: | UP4<br>UP3 | Enabled<br>Enabled |
| | **Image Id -** This displays the Image ID of the currently loaded Intel® Integrated LAN binary. | | |
| | **Major Version -** This displays the Major revision number of the currently loaded Intel® Integrated LAN binary. | | |
| | **Minor Version -** This displays the Minor revision number of the currently loaded Intel® Integrated LAN binary. | | |

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

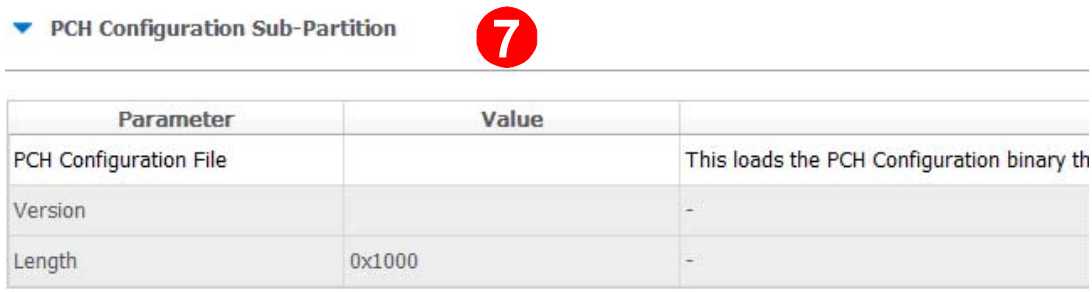
▼ IUnit Sub-Partition 6

| Parameter | Value | |
|---|---|---|
| IUnit Binary File | | This loads the IUnit binary that will be mer |
| Length | 0xA000 | - |
| Version | | - |

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

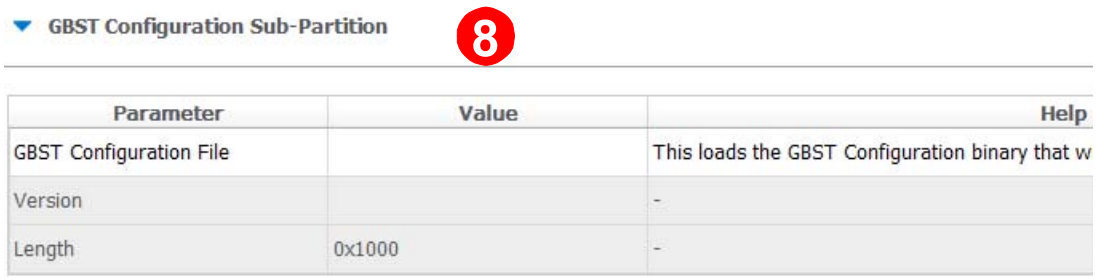
| # | Parameter | Platform | Settings |
|---|---|---|---|
| 6 | **IUNIT Sub-Partition Binary**<br>This loads the IUnit Sub Partition binary that will be merged into the output image generated by the Intel® FIT tool. | UP4<br>UP3 | Iunit.bin (Optional)<br>Iunit.bin (Optional) |
| | **Length -** This displays the length of the IUNIT Sub-Partition.<br>***Note:*** This value will be automatically populated by Intel® FIT during image build. | | |
| | **Version -** This displays the version number of the IUNIT Sub-Partition | | |

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




| # | Parameter | Platform | Settings |
|---|---|---|---|
| 7 | **PCH Configuration Sub-Partition**<br>This loads the PCH Configuration binary that will be merged in the output image generated by the Intel® FIT tool. | | |
| | **PCH Configuration File**<br>Navigate to path to load PCHC.bin file. This loads the PCH Configuration binary. | UP4<br>UP3 | PCHC.bin<br>PCHC.bin |
| | **Version -** This displays the version number of the PCHC Configuration Sub-Partition | | |
| | **Length -** This displays the length of the PCH Configuration Sub-Partition.<br>***Note:*** This value will be automatically populated by Intel® FIT during image build. | | |

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

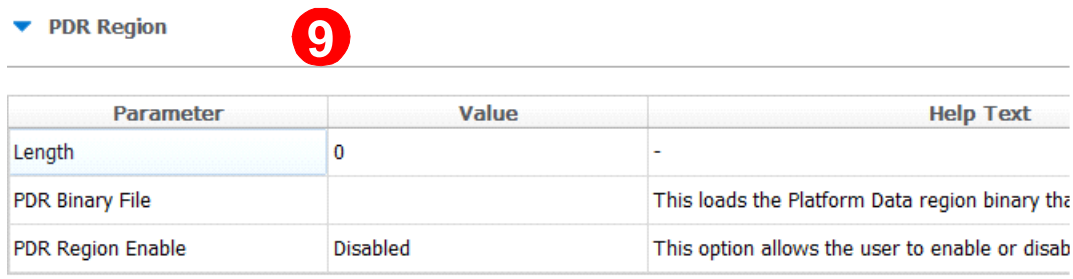



| # | Parameter | Platform | Settings |
|---|---|---|---|
| 8 | **GBST Configuration Sub-Partition**<br>This loads the GBST Configuration binary that will be merged in the output image generated by the Intel® FIT tool.<br><br>***Note:*** The GBST sub-partition is used to enabling FuSa safety standards and is not applicable for client platforms. | | |
| | **GBST Configuration File**<br>Navigate to path to load GBST.bin file. This loads the GBST Configuration binary. | UP4<br>UP3 | GBST.bin (Optional) |

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

| | | | |
|---|---|---|---|
| | **Version -** This displays the version number of the GBST Configuration Sub-Partition | | |
| | **Length -** This displays the length of the GBST Configuration Sub-Partition.<br>***Note:*** This value will be automatically populated by Intel® FIT during image build. | | |

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




| # | Parameter | Platform | Settings |
|---|---|---|---|
| 9 | **PDR Region -** This loads the Platform Data region binary that will be merged into the output image generated by the Intel® FIT tool. | | |
| | **PDR Region - Length**<br>Region is disabled by default. Displays Region size information when **Binary input file** is specified. | | |
| | **PDR Binary File**<br>Navigate to path to load pdrimage.bin file if required and available. | UP4<br>UP3 | PDR.bin (Optional)<br>PDR.bin (Optional) |
| | **PDR Region Enable**<br>**Values: Enabled / Disabled -** This option allows the user to enable or disable the Platform Data Region.<br>**Note:** If loading PDR.bin file, check that the PDR region is enabled in tool before building image. | UP4<br>UP3 | Disabled<br>Disabled |

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

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

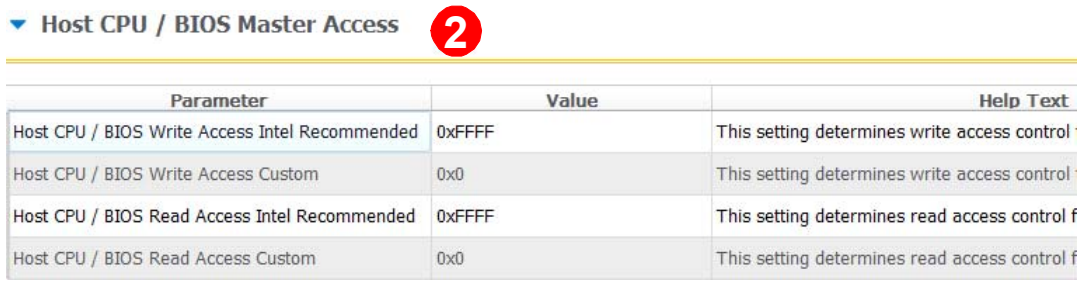
**Flash Components** 1

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

| # | Parameter | Platform | Settings |
|---|---|---|---|
| 1 | **Flash Components** | | |
| | **Number of Components**<br>**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. | UP4<br>UP3 | 1<br>1 |
| | **Flash component 1 Size**<br>**Values: 512KB, 1MB, 2MB, 4MB, 8MB, 16MB, 32MB, 64MB** - This setting determines the size of Flash component 1 for the platform image. | UP4<br>UP3 | 32MB<br>32MB |
| | **Flash component 2 Size**<br>**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'. | UP4<br>UP3 | Greyed Out<br>Greyed Out |
| | **SPI Global Protected Range -** This sets the default value of the Global Protected Range register in the SPI Flash Controller. | UP4<br>UP3 | 0x0<br>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. | UP4<br>UP3 | 0x5<br>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. | UP4<br>UP3 | Yes<br>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. | UP4<br>UP3 | 4us<br>4us |

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

| | | | |
|---|---|---|---|
| | **SPI Max write / erase Resume to Suspend intervals** - This setting specifies the maximum value for the write and erase Resume to Suspend intervals. | UP4<br>UP3 | No Ceiling<br>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. | UP4<br>UP3 | Yes<br>Yes |
| | **Software Re-Binding Enabled**<br>**Values: Yes / No**<br>When enabled this settings will allow for SPI re-binding to a new PCH during manufacturing and re-manufacturing flows prior to platform EOM.<br><br>***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. | UP4<br>UP3 | No<br>No |
| **Click on Flash Layout in the left tabs menu> BIOS Region is expanded by default:** | | | |

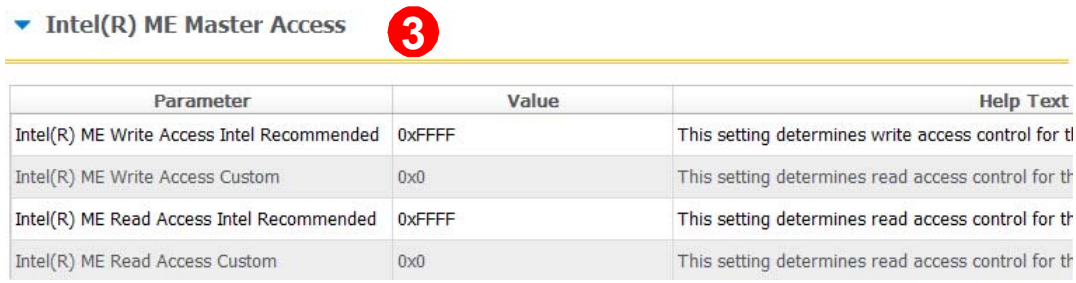



| # | Parameter | Platform | Settings |
|---|---|---|---|
| 2 | **Host CPU / BIOS Master Access** | | |
| | **Host CPU / BIOS Write Access Intel Recommended**<br>**Values: 0xFfFF, 0x000A, 0x001A, 0x010A, 0x011A** - This setting determines write access control for the BIOS region.<br>**0xFfFF** = Debug/Manufacturing<br>**0x000A** = Production<br>**0x001A** = Production with access to PDR (should ONLY be used if PDR region is implemented).<br>**0x010A** = Production with access to EC<br>**0x011A** = Production with access to EC and PDR<br>**Custom** = User custom Host / BIOS Write Access values<br><br>For further details on Region Access Control see Tiger Lake LP SPI Programming guide further details. | UP4<br>UP3 | 0xFFFF<br>0xFFFF |
| | **Host CPU / BIOS Write Access Custom** - This setting allows free form user customized Host CPU / BIOS Write Access regions permissions<br><br>***Note:*** This setting is grayed out unless Custom is selected under the Host CPU / BIOS Write Access Intel Recommended drop down menu.<br><br>***Warning:*** **Setting region access permission values outside of Intel recommendation could result in compromised platform security** | UP4<br>UP3 | Hex Input |

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

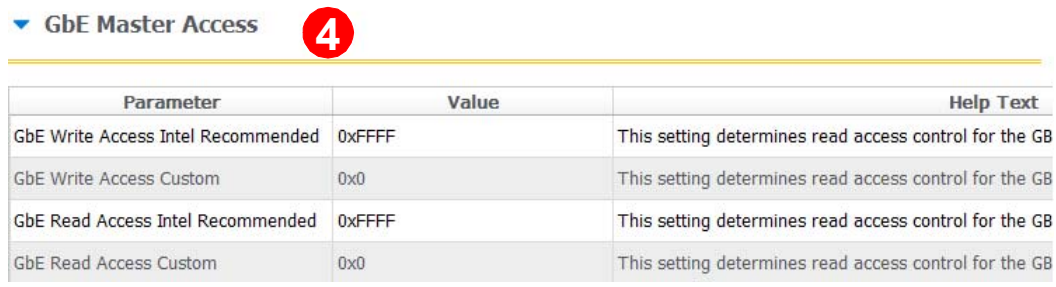
| | | | |
|---|---|---|---|
| | **Host CPU / BIOS Read Access**<br>**Values: 0xFFF, 0x00F, 0x01F, 0x10F, 0x11F** - This setting determines read access control for the BIOS region.<br>**0xFFF** = Debug/Manufacturing<br>**0x00F =** Production<br>**0x01F =** Production with access to PDR (should ONLY be used if PDR region is implemented).<br>**0x10F** = Production with access to EC<br>**0x11F** = Production with access to EC and PDR<br>**Custom** = User custom Host / BIOS Read Access values<br><br>For further details on Region Access Control see Tiger Lake LP SPI Programming guide. | UP4<br>UP3 | 0xFFFF<br>0xFFFF |
| | **Host CPU / BIOS Read Access Custom** - This setting allows free form user customized Host CPU / BIOS Read Access regions permissions<br><br>***Note:*** This setting is grayed out unless Custom is selected under the Host CPU / BIOS Read Access Intel Recommended drop down menu.<br><br>***Warning:*** **Setting region access permission values outside of Intel recommendation could result in compromised platform security** | UP4<br>UP3 | Hex Input |

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




| # | Parameter | Platform | Settings |
|---|---|---|---|
| 3 | **Intel® ME Master Access** | | |
| | **Intel® ME Write Access Intel Recommended**<br>**Values: 0xFFFF, 0x0004**- This setting determines write access control for the ME region.<br>**0xFFFF** = Debug/Manufacturing<br>**0x0004** = Production<br>**Custom** = User custom Intel® ME Write Access values<br><br>For further details on Region Access Control see Tiger Lake LP SPI Programming guide further details. | UP4<br>UP3 | 0xFFFF<br>0xFFFF |
| | **Intel® ME Write Access Custom** - This setting allows free form user customized Intel® ME Write Access regions permissions<br><br>***Note:*** This setting is grayed out unless Custom is selected under the Intel® ME Write Access Intel Recommended drop down menu.<br><br>***Warning:*** **Setting region access permission values outside of Intel recommendation could result in compromised platform security** | UP4<br>UP3 | Hex Input |

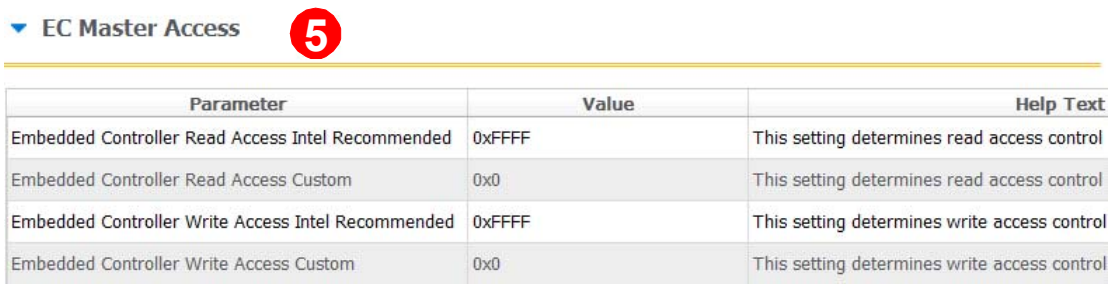
## Table 2-4. - Flash Settings (Sheet 4 of 10)

| | | | |
|---|---|---|---|
| | **Intel® ME Read Access Intel Recommended**<br>**Values: 0xFFFF, 0x000D** - This setting determines read access control for the ME region.<br>**0xFFFF** = Debug/Manufacturing<br>**0x000D** = Production<br>**Custom** = User custom Intel® ME Read Access values<br><br>For further details on Region Access Control see Tiger Lake LP SPI Programming guide further details. | UP4<br>UP3 | 0xFFFF<br>0xFFFF |
| | **Intel® ME Read Access Custom** - This setting allows free form user customized Intel® ME Read Access regions permissions<br><br>***Note:*** This setting is grayed out unless Custom is selected under the Intel® ME Read Access Intel Recommended drop down menu.<br><br>***Warning:*** **Setting region access permission values outside of Intel recommendation could result in compromised platform security** | UP4<br>UP3 | Hex Input |
| **Click on Flash Settings in the left tabs menu> GbE Master Access is expanded by default:** | | | |
|  | | |
| **#** | **Parameter** | **Platform** | **Settings** |
| 4 | **GbE Master Access** | | |
| | **GbE Write Access Intel Recommended**<br>**Values: 0xFFFF, 0x0008** - This setting determines write access control for the Gigabit Ethernet Region.<br>**0xFFFF** = Debug/Manufacturing<br>**0x0008** = Production<br>**Custom** = User custom GbE Write Access values<br><br>For further details on Region Access Control see Tiger Lake LP SPI Programming guide further details. | UP4<br>UP3 | 0xFFFF<br>0xFFFF |
| | **GbE Write Access Custom** - This setting allows free form user customized GbE Write Access regions permissions<br><br>***Note:*** This setting is grayed out unless Custom is selected under the GbE Write Access Intel Recommended drop down menu.<br><br>***Warning:*** **Setting region access permission values outside of Intel recommendation could result in compromised platform security** | UP4<br>UP3 | Hex Input |

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

| | | | |
|---|---|---|---|
| | **GbE Read Access Intel Recommended**<br>**Values: 0xFFFF, 0x0009** - This setting determines read access control for the Gigabit Ethernet Region.<br>**0xFFFF** = Debug/Manufacturing<br>**0x0009** = Production<br>**Custom** = User custom GbE Read Access values<br><br>For further details on Region Access Control see Tiger Lake LP SPI Programming guide further details. | UP4<br>UP3 | 0xFFFF<br>0xFFFF |
| | **GbE Read Access Custom** - This setting allows free form user customized GbE Read Access regions permissions<br><br>***Note:*** This setting is grayed out unless Custom is selected under the GbE Read Access Intel Recommended drop down menu.<br><br>***Warning:*** **Setting region access permission values outside of Intel recommendation could result in compromised platform security** | UP4<br>UP3 | Hex Input |

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




| # | Parameter | Platform | Settings |
|---|---|---|---|
| 5 | **EC Master Access** | | |
| | **EC Write Access Intel Recommended**<br>**Values: 0xFFFF, 0x0100** - This setting determines write access control for the Embedded Controller Region.<br>**0xFFFF** = Debug/Manufacturing<br>**0x0100** = Production<br>**Custom** = User custom EC Write Access values<br><br>For further details on Region Access Control see Tiger Lake LP SPI Programming guide further details. | UP4<br>UP3 | 0xFFFF<br>0xFFFF |
| | **EC Write Access Custom** - This setting allows free form user customized EC Write Access regions permissions<br><br>***Note:*** This setting is grayed out unless Custom is selected under the EC Write Access Intel Recommended drop down menu.<br><br>***Warning:*** **Setting region access permission values outside of Intel recommendation could result in compromised platform security** | UP4<br>UP3 | Hex Input |

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

| | | | |
|---|---|---|---|
| | **EC Read Access Intel Recommended**<br>**Values: 0xFFFF, 0x0101, 0x0103** - This setting determines read access control for the Embedded Controller Region.<br>**0xFFFF** = Debug/Manufacturing<br>**0x0101 =** Production<br>**0x0103** = Production with EC BIOS Read Access<br>**Custom** = User custom EC Read Access values<br><br>For further details on Region Access Control see Tiger Lake LP SPI Programming guide further details. | UP4<br>UP3 | 0xFFFF<br>0xFFFF |
| | **EC Read Access Custom** - This setting allows free form user customized EC Read Access regions permissions<br><br>***Note:*** This setting is grayed out unless Custom is selected under the EC Read Access Intel Recommended drop down menu.<br><br>***Warning:*** **Setting region access permission values outside of Intel recommendation could result in compromised platform security** | UP4<br>UP3 | Hex Input |

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

Flash Configuration 6

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

| # | Parameter | Platform | Settings |
|---|---|---|---|
| 6 | **Flash Configuration** | | |

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

| | | | |
|---|---|---|---|
| | **Dual I/O Read Enabled**<br>**Values: Yes/No** - This setting allows the customer to enable support for Dual I/O Read capabilities for flash components. See Tiger Lake LP SPI Programming guide for further details. | UP4<br>UP3 | Yes<br>Yes |
| | **Dual Output Read Enabled**<br>**Values: Yes/No** - This setting allows the customer to enable support for Dual Output Read capabilities for flash components. See Tiger Lake LP SPI Programming guide for further details. | UP4<br>UP3 | Yes<br>Yes |
| | **Fast Read Clock Frequency**<br>**Values: 14MHz, 25MHz, 33MHz, 50MHz, 100MHz**- This setting allows the customer to configure the flash component clock frequency setting for Fast Read. See Rocket Lake LP SPI Programming guide for further details.<br>***Note:*** The 100MHz frequency setting not valid on client platforms | UP4<br>UP3 | 50MHz<br>50MHz |
| | **Fast Read Supported**<br>**Values: Yes/No** - This setting allows the customer to enable support for Fast Read capabilities for flash components. See Tiger Lake LP SPI Programming guide for further details.<br>**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. | UP4<br>UP3 | Yes<br>Yes |
| | **Invalid Instruction 0** - This setting allows the customer to configure invalid instruction to protect against Chip Erase. See Tiger Lake LP SPI Programming guide for further details. **Note:** This setting should be set to '0' if there are not Invalid instructions. | UP4<br>UP3 | 0x00000021<br>0x00000021 |
| | **Invalid Instruction 1** - This setting allows the customer to configure invalid instruction to protect against Chip Erase. See Tiger Lake LP SPI Programming guide for further details. **Note:** This setting should be set to '0' if there are not Invalid instructions. | UP4<br>UP3 | 0x00000042<br>0x00000042 |
| | **Invalid Instruction 2** - This setting allows the customer to configure invalid instruction to protect against Chip Erase. See Tiger Lake LP SPI Programming guide for further details. **Note:** This setting should be set to '0' if there are not Invalid instructions. | UP4<br>UP3 | 0x00000060<br>0x00000060 |
| | **Invalid Instruction 3** - This setting allows the customer to configure invalid instruction to protect against Chip Erase. See Tiger Lake LP SPI Programming guide for further details. **Note:** This setting should be set to '0' if there are not Invalid instructions. | UP4<br>UP3 | 0x000000AD<br>0x000000AD |
| | **Invalid Instruction 4** - This setting allows the customer to configure invalid instruction to protect against Chip Erase. See Tiger Lake LP SPI Programming guide for further details. **Note:** This setting should be set to '0' if there are not Invalid instructions. | UP4<br>UP3 | 0x000000B7<br>0x000000B7 |
| | **Invalid Instruction 5** - This setting allows the customer to configure invalid instruction to protect against Chip Erase. See Tiger Lake LP SPI Programming guide for further details. **Note:** This setting should be set to '0' if there are not Invalid instructions. | UP4<br>UP3 | 0x000000B9<br>0x000000B9 |
| | **Invalid Instruction 6** - This setting allows the customer to configure invalid instruction to protect against Chip Erase. See Tiger Lake LP SPI Programming guide for further details. **Note:** This setting should be set to '0' if there are not Invalid instructions. | UP4<br>UP3 | 0x000000C4<br>0x000000C4 |
| | **Invalid Instruction 7** - This setting allows the customer to configure invalid instruction to protect against Chip Erase. See Tiger Lake LP SPI Programming guide for further details. **Note:** This setting should be set to '0' if there are not Invalid instructions. | UP4<br>UP3 | 0x000000C7<br>0x000000C7 |
| | **Quad I/O Read Enabled**<br>**Values: Yes/No** - This setting allows the customer to enable support for Quad I/O Read capabilities for flash components. See Tiger Lake LP SPI Programming guide for further details. | UP4<br>UP3 | Yes<br>Yes |
| | **Quad Output Read Enabled**<br>**Values: Yes/No** - This setting allows the customer to enable support for Quad Output Read capabilities for flash components. See Tiger Lake LP SPI Programming guide for further details. | UP4<br>UP3 | Yes<br>Yes |

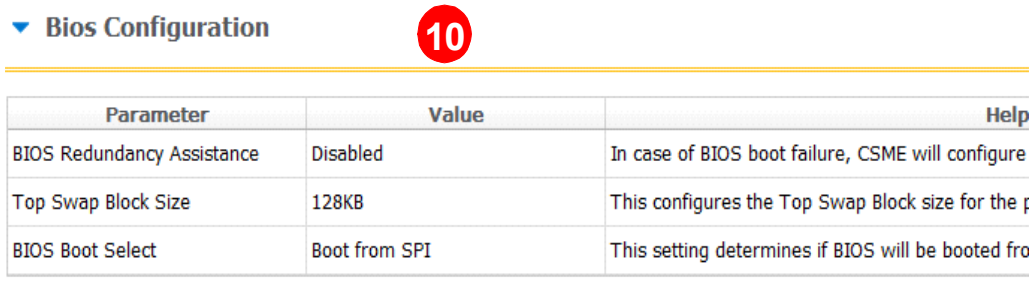
## Table 2-4. - Flash Settings (Sheet 8 of 10)

| | | | |
|---|---|---|---|
| | **Read ID and Read Status clock frequency**<br>**Values: 14MHz, 25MHz, 33MHz, 50MHz, 100MHz**- This setting allows the customer to configure the flash component clock frequency setting for Read ID and Read Status clock. See Rocket Lake LP SPI Programming guide for further details.<br>***Note:*** The 100MHz frequency setting not valid on client platforms | UP4<br>UP3 | 50MHz<br>50MHz |
| | **Write and Erase clock frequency**<br>**Values: 14MHz, 25MHz, 33MHz, 50MHz, 100MHz**- This setting allows the customer to configure the flash component clock frequency setting for Write and Erase. See Rocket Lake LP SPI Programming guide for further details.<br>***Note:*** The 100MHz frequency setting not valid on client platforms | UP4<br>UP3 | 50MHz<br>50MHz |
| **Click on Flash Settings in the left tabs menu> Legacy VSCC Table is expanded by default:** | | | |

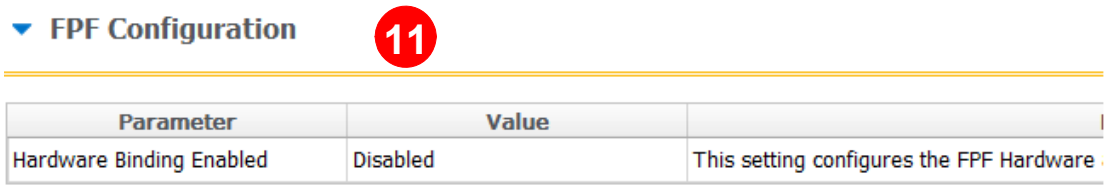
| Parameter | Value | Help Text |
|---|---|---|
| Part Name | W25Q128BV | This setting allow the OEM input a name designation for each flash... |
| Vendor ID | 0xEF | This configures the JEDEC vendor specific byte ID of the SPI flash ... |
| Device ID 0 | 0x40 | This configures the JEDEC device specific byte ID 0 of the SPI flas... |
| Device ID 1 | 0x19 | This configures the JEDEC device specific byte ID 1 of the SPI flas... |

| # | Parameter | Platform | Settings |
|---|---|---|---|
| 7 | **Legacy VSCC Table**<br>**VSCC Entries** | | |
| | **W25Q128BV** | | |
| 8 | **VSCC Entries** | UP4<br>UP3 | |
| | **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. | UP4<br>UP3 | Winbond<br>Winbond |
| | **Vendor ID** - This configures the JEDEC vendor specific byte ID of the SPI flash component. See Tiger Lake LP SPI Programming guide for further details. | UP4<br>UP3 | 0xEF<br>0xEF |
| | **device ID 0** - This configures the JEDEC device specific byte ID 0 of the SPI flash component. See Tiger Lake LP SPI Programming guide for further details. | UP4<br>UP3 | 0x40<br>0x40 |
| | **device ID 1** - This configures the JEDEC device specific byte ID 1 of the SPI flash component. See Tiger Lake LP SPI Programming guide for further details. | UP4<br>UP3 | 0x19<br>0x19 |
| 9 | **+ Add VSCC Entry** | | |
| **Click on Flash Settings in the left tabs menu> BIOS Configuration is expanded by default:** | | | |

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

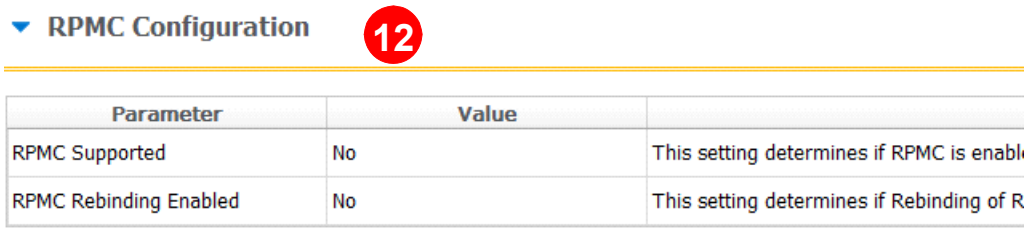



| # | Parameter | Platform | |
|---|---|---|---|
| 10 | **BIOS Configuration** | | |
| | **BIOS Redundancy Assistance**<br>**Values: Enabled, Disabled**<br>In cases of BIOS boot failure, Intel®CSME will configure the platform to boot with backup BIOS using Top Swap when this setting is enabled.<br><br>***Note:*** This option is only applicable when Boot Guard is enabled. | UP4<br>UP3 | Disabled<br>Disabled |
| | **Top Swap Block Size**<br>**Values: 64KB, 128KB, 256KB, 512KB, 1MB** - This configures the Top Swap Block size for the platform. For further details see Tiger Lake LP Platform Controller Hub EDS. | UP4<br>UP3 | 128KB<br>128KB |
| | **BIOS Boot Select**<br>**Values: Boot from SPI / Boot from LPC**<br>This setting determines if BIOS will be booted from LPC or SPI. | UP4<br>UP3 | Boot from SPI<br>Boot from SPI |
| **Click on Flash Settings in the left tabs menu> BIOS Configuration is expanded by default:** | | | |




| | | | |
|---|---|---|---|
| 11 | **FPF Configuration** | | |
| | **Hardware Binding Enabled**<br>**Values: Enabled / Disabled**<br><br>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.<br><br>For Revenue parts this setting will be ignored and FPF Hardware binding will take place when close manufacturing flow is executed. | UP4<br>UP3 | Disabled<br>Disabled |
| **Click on Flash Settings in the left tabs menu> RPMC Configuration is expanded by default:** | | | |

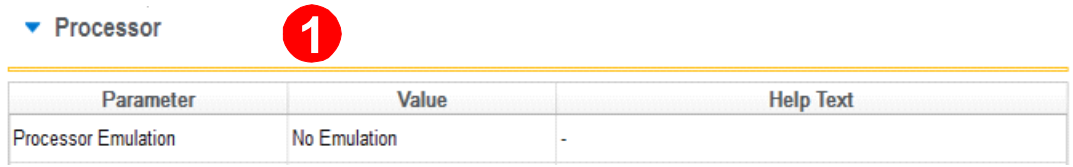
## Table 2-4. - Flash Settings (Sheet 10 of 10)




| | | | |
|---|---|---|---|
| 12 | **RPMC Configuration** | | |
| | **RPMC Supported**<br>**Values: Yes / No**<br><br>This setting determines if RPMC is enabled.<br>***Note:*** The SPI parts being used need to support RPMC In order to use this feature. | UP4<br>UP3 | No<br>No |
| | **RPMC Rebinding Enabled**<br>**Values: Yes / No**<br><br>This setting determines if Rebinding of RPMC enabled SPI parts is enabled. | UP4<br>UP3 | No<br>No |

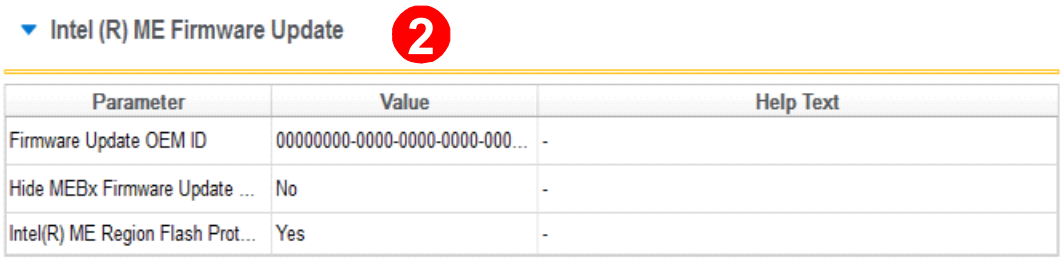
## Table 2-5. - Intel® ME Kernel (Sheet 1 of 4)

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




| # | Parameter | Platform | Settings |
|---|---|---|---|
| 1 | **Processor** | | |
| | **Processor Emulation**<br>**Values: No Emulation**<br>**EMULATE Intel® vPro (TM) capable Processor**<br>**EMULATE Intel® Core (TM) branded Processor**<br>**EMULATE Intel® Celeron (R) branded Processor**<br>**EMULATE Intel® Pentium (R) branded Processor**<br>**EMULATE Intel® Xeon (R) branded Processor**<br>**EMULATE Intel® Xeon (R) Manageability capable Processor**<br>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. | UP4<br>UP3 | EMULATE Intel® Core (TM) branded Processor<br>EMULATE Intel® Core (TM) branded Processor |

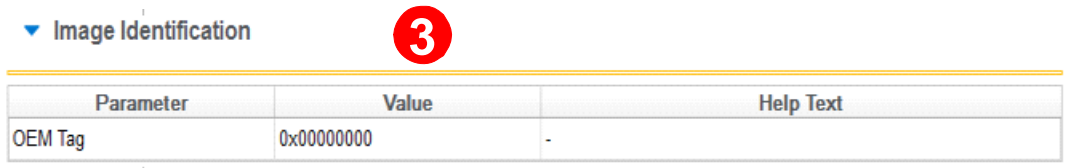
**Click on Intel® ME Kernel in the left tabs menu> Intel® ME Firmware Update is expanded by default:**




| # | Parameter | Platform | Settings |
|---|---|---|---|
| 2 | **Intel® ME Firmware Update** | | |
| | **Firmware Update OEM ID** - This setting allows configuration of an OEM unique ID to ensure that customers can only update their platform with images from the OEM of the platform. | UP4<br>UP3 | 0 string<br>0 string |
| | **Hide Intel® MEBx Firmware Update Control**<br>**Values: Yes/No** - This setting allows the customer to hide the Firmware Update option in the Intel® MEBx interface. | UP4<br>UP3 | No<br>No |
| | **Intel® ME Region Flash Protection Override**<br>**Values: Yes/No** - This setting enables descriptor unlock of the Intel® CSME Region when the HMRFPO message is sent to firmware prior to BIOS End of POST. | UP4<br>UP3 | Yes<br>Yes |

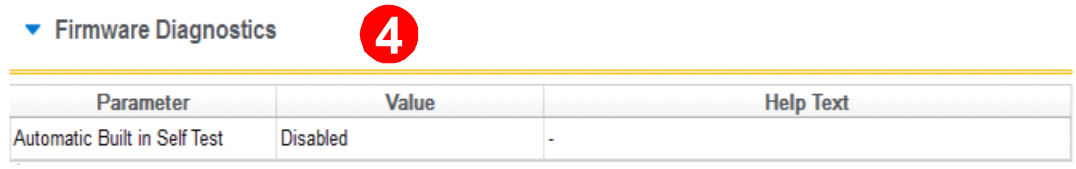
**Click on Intel® ME Kernel in the left tabs menu> Image Identification is expanded by default:**

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



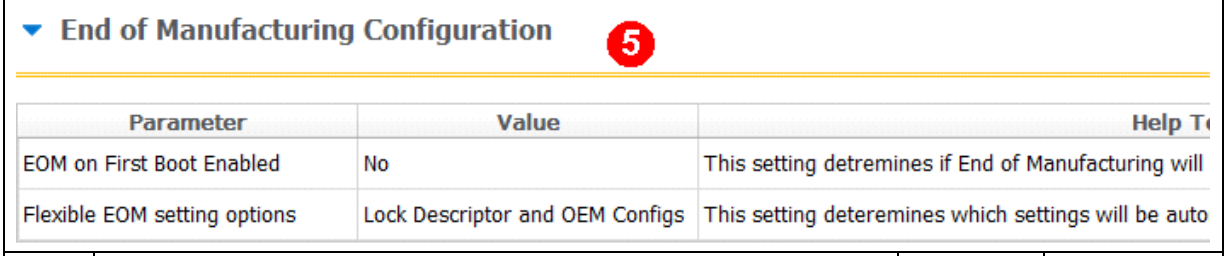

| # | Parameter | Platform | Settings |
|---|---|---|---|
| 3 | **Image Identification** | | |
| | **OEM Tag -** This is a free form 32bit field that allows the OEM to configure their own unique identifier in the firmware image. | UP4<br>UP3 | 0x00000000<br>0x00000000 |

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




| # | Parameter | Platform | Settings |
|---|---|---|---|
| 4 | **Firmware Diagnostics** | | |
| | **Automatic Built in Self Test**<br>**Values: Enabled / Disabled**<br>This setting enables the firmware Automatic Built in Self Test which is executed during first platform boot after initial image flashing. | UP4<br>UP3 | Disabled<br>Disabled |

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

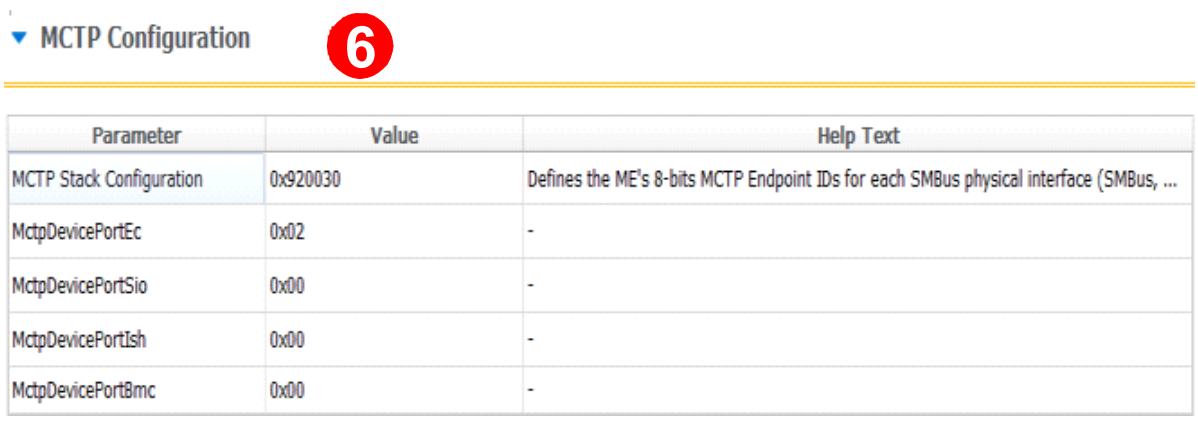



| # | Parameter | Platform | Settings |
|---|---|---|---|
| 5 | **End of Manufacturing Configuration** | | |
| | **EOM of First Boot Enabled**<br>**Value: Yes / No**<br>This setting determines if End of Manufacturing will be triggered on first boot of the platform after flashing. Note: When this setting is enabled Intel® CSME will enter End of Manufacturing regardless of the descriptor settings. | UP4<br>UP3 | No<br>No |

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

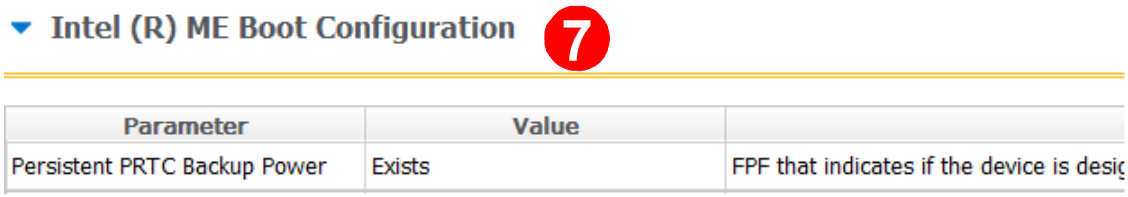
| | | | |
|---|---|---|---|
| | **Flexible EOM setting options**<br>**Value: Lock Descriptor and OEM Configs / Lock OEM Configs Only / Lock Descriptor Only / Do not lock Descriptor and OEM Configs**<br>This setting determines which settings will be automatically committed during End of Manufacturing flows. Note: The FPFs, RPMB / RPMC and set manufacturing mode settings are mandatory and cannot be overridden revenue parts. Simulation can be done on non-revenue part with the Hardware binding set to disabled. | UP4<br>UP3 | Lock Descriptor and OEM Configs |

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



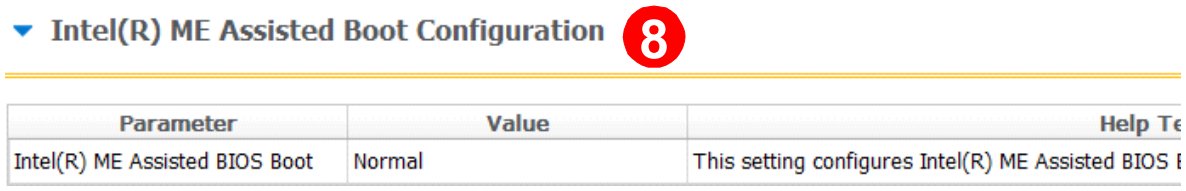
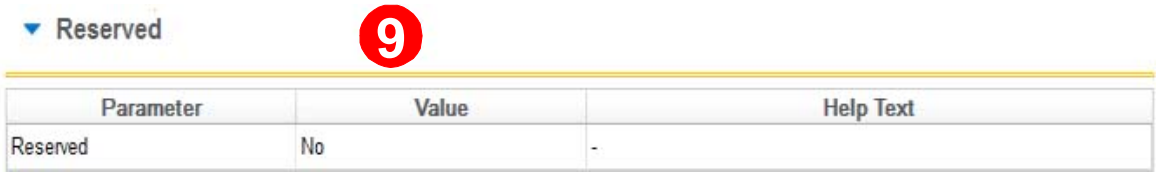

| # | Parameter | Platform | Settings |
|---|---|---|---|
| 6 | **MCTP Configuration** | | |
| | **MCTP Stack Configuration**<br>Defines the Intel® ME's 8-bits MCTP Endpoint ID's for each SMBus physical interface (SMBus, SMLink0, and SMLink1). These values are needed for FW to communicate with MCTP end 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. | UP4<br>UP3 | 0x920030<br>0x920030 |
| | **MctpdevicePortEc** | UP4<br>UP3 | 0x02<br>0x02 |
| | **MctpdevicePortSio** | UP4<br>UP3 | 0x00<br>0x00 |
| | **MctpdevicePortIsh** | UP4<br>UP3 | 0x00<br>0x00 |
| | **MctpdevicePortBmc** | UP4<br>UP3 | 0x00<br>0x00 |

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



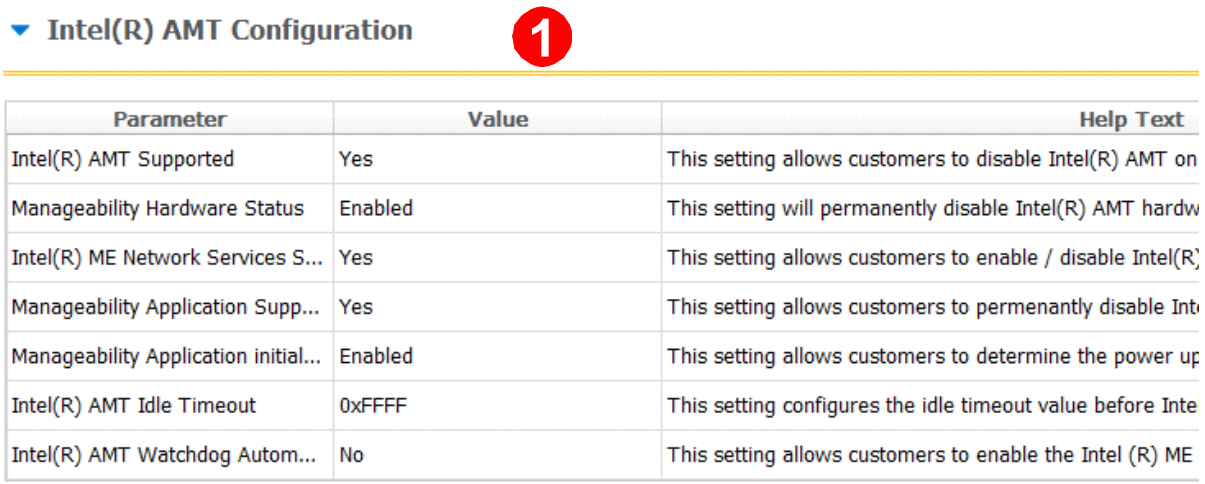

| # | Parameter | Platform | Settings |
|---|---|---|---|

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

| | | | |
|---|---|---|---|
| 7 | **Intel® ME Boot Configuration** | | |
| | **Persistent PRTC Backup Power**<br>**Values: None / Exists**<br>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 | UP4<br>UP3 | Exists<br>Exists |
| **Click on Intel® ME Kernel in the left tabs menu> Intel® ME Assisted Boot Configuration is expanded by default:** | | | |
|  | | | |
| 8 | **Intel® ME Assisted Boot Configuration** | | |
| | **Intel**<br>**Values: Normal / Intel® ME Assisted**<br>This setting configures Intel® ME Assisted BIOS Boot capabilities.<br>***Note:*** Leave this setting configured to "Normal" | UP4<br>UP3 | Normal<br>Normal |
| **Click on Intel® ME Kernel in the left tabs menu> Reserved is expanded by default:** | | | |
|  | | | |
| 9 | **Reserved** | | |
| | **Reserved**<br>**Values: Yes/No** | UP4<br>UP3 | No<br>No |

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

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




| # | Parameter | Platform | Settings |
|---|---|---|---|
| 1 | **Intel® AMT Configuration** | | |
| | **Intel® AMT Supported**<br>**Values: Yes / No** - This setting allows customers to disable Intel® AMT on the platform and force the platform into Standard Manageability mode.<br>***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. | UP4<br>UP3 | No<br>No |
| | **Manageability Hardware Status**<br>**Values: Enabled / Disabled -** This setting will permanently disable Manageability hardware through platform FPFs. At End-of-Manufacturing (EOM), enable/disable policy value is committed to FPF and can never be changed. Permanently disabling Manageability hardware with this setting requires "Manageability Application Supported" and "Disabled" and "Intel® ME Network Services Supported" are set to "No".<br>***Note:*** When "Manageability Application Hardware Status" is Enabled but "Manageability Application Supported" and "Intel® ME Network Services Supported" are set to "No", Manageability Hardware will be disabled by the Intel®CSME through CVAR. | UP4<br>UP3 | Enabled<br>Enabled |
| | **Intel® ME Network Services Supported**<br>**Values: Yes / No -** This setting allows customers to enable / disable Intel® ME Network Services on the platform.<br>***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. | UP4<br>UP3 | No<br>No |
| | **Intel® Manageability Application Supported**<br>**Values: Yes / No -** This setting allows customers to force Intel® AMT enabled platforms to operate in Standard Manageability mode.<br>***Note:*** This setting only applies to Desktop and Workstation platforms. | UP4<br>UP3 | No<br>No |
| | **Manageability Application initial power-up state**<br>**Values: Enabled / Disabled**<br>This setting allows customers to determine the power up state for Intel® AMT or Standard Manageability.<br>***Note:*** If this setting is disabled Intel® AMT or Standard Manageability can still be re-enabled through the Intel® MEBx interface. | UP4<br>UP3 | Disabled<br>Disabled |

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

| # | Parameter | Platform | Settings |
|---|---|---|---|
| | **Intel® AMT Idle Timeout**<br>**Values: 0xFFFF** - This setting configures the idle timeout value before Intel® AMT enters into an off state. | UP4<br>UP3 | 0xFFFF<br>0xFFFF |
| | **Intel® AMT Watchdog Automatic Reset Enabled**<br>**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.<br><br>***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. | UP4<br>UP3 | No<br>No |

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

KVM Configuration 2

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

| # | Parameter | Platform | Settings |
|---|---|---|---|
| 2 | **KVM Configuration** | | |
| | **Firmware KVM Screen Blanking**<br>**Values: Yes / No -** This setting enables KVM Screen blanking capabilities in the firmware image.<br><br>***Note:*** This feature is dependent on processor level support. | UP4<br>UP3 | No<br>No |
| | **KVM Redirection Supported**<br>**Values: Yes / No** - This setting allows OEMs to enable / disable the KVM Redirection capabilities of the firmware.<br><br>***Note:*** If this setting has been set to disabled it cannot be re-enabled once the descriptor has been locked. | UP4<br>UP3 | No<br>No |

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

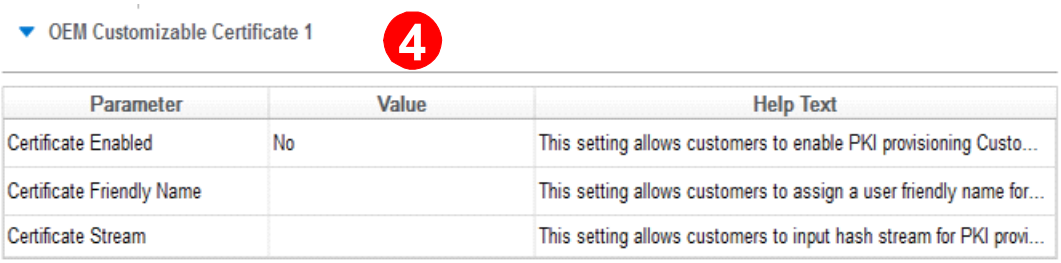
Provisioning Configuration 3

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

| # | Parameter | Platform | |
|---|---|---|---|
| 3 | **Provisioning Configuration** | | |

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

| | | | |
|---|---|---|---|
| | **Embedded Host Based Configuration**<br>**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.<br><br>***Note:*** The Intel® FIT tool will not adjust the Redirection Privacy/Security value based on selection here. Please set security level as needed. | UP4<br>UP3 | No<br>No |
| | **PKI Domain Name Suffix** - This setting allow OEMs to pre-configure the Domain Name Suffix used for PKI provisioning in their firmware image.<br><br>***Note:*** For normal out-of-box provisioning functionality this setting should be left empty. | UP4<br>UP3 | -<br>- |
| **Click on Intel® AMT in the left tabs menu> OEM Customizable Certificate 1 is expanded by default:** | | | |

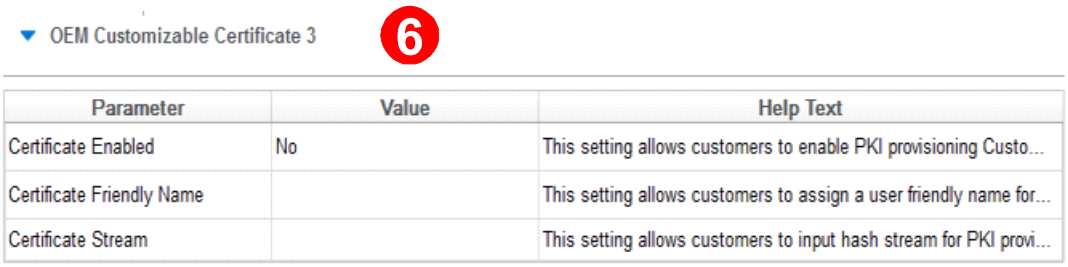



| # | Parameter | Platform | Settings |
|---|---|---|---|
| 4 | **OEM Customizable Certificate 1** | | |
| | **Certificate Enabled**<br>**Values: Yes/No** - This setting allows customers to enable PKI provisioning Custom Certificate 1. | UP4<br>UP3 | No<br>No |
| | **Certificate Friendly Name** - This setting allows customers to assign a user friendly name for PKI provisioning Custom Certificate 1. Maximum of 32 characters. | UP4<br>UP3 | -<br>- |
| | **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.<br><br>***Note:*** If the platform is un-configured the Custom Certificate Hash will be deleted. | UP4<br>UP3 | -<br>- |
| **Click on Intel® AMT in the left tabs menu> OEM Customizable Certificate 2 is expanded by default:** | | | |

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

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

| | | | |
|---|---|---|---|
| | **Certificate Enabled**<br>**Values: Yes/No** - This setting allows customers to enable PKI provisioning Custom Certificate 2. | UP4<br>UP3 | No<br>No |
| | **Certificate Friendly Name** - This setting allows customers to assign a user friendly name for PKI provisioning Custom Certificate 2. Maximum of 32 characters. | UP4<br>UP3 | -<br>- |
| | **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.<br><br>***Note:*** If the platform is un-configured the Custom Certificate Hash will be deleted. | UP4<br>UP3 | -<br>- |
| **Click on Intel® AMT in the left tabs menu> OEM Customizable Certificate 3 is expanded by default:** | | | |

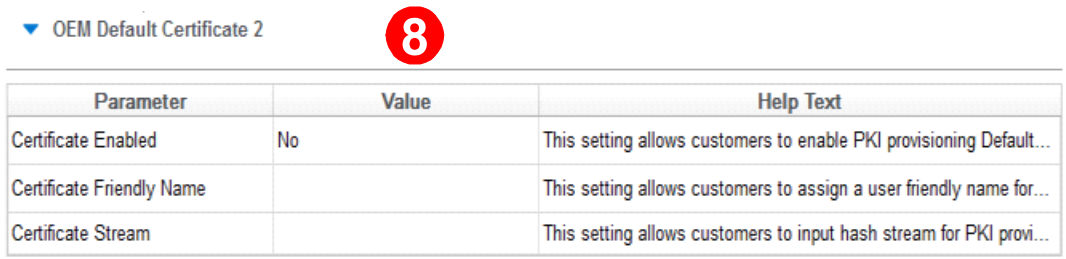



| # | Parameter | Platform | Settings |
|---|---|---|---|
| 6 | **OEM Customizable Certificate 3** | | |
| | **Certificate Enabled**<br>**Values: Yes/No** - This setting allows customers to enable PKI provisioning Custom Certificate 3. | UP4<br>UP3 | No<br>No |
| | **Certificate Friendly Name** - This setting allows customers to assign a user friendly name for PKI provisioning Custom Certificate 3. Maximum 32 characters. | UP4<br>UP3 | -<br>- |
| | **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.<br><br>***Note:*** If the platform is un-configured the Custom Certificate Hash will be deleted. | UP4<br>UP3 | -<br>- |
| **Click on Intel® AMT in the left tabs menu> OEM Default Certificate 1 is expanded by default:** | | | |

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

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

| | | | |
|---|---|---|---|
| | **Certificate Enabled**<br>**Values: Yes/No** - This setting allows customers to enable PKI provisioning Default certificate 1. | UP4<br>UP3 | No<br>No |
| | **Certificate Friendly Name** - This setting allows customers to assign a user friendly name for PKI provisioning Default Certificate 1. Maximum 32 characters. | UP4<br>UP3 | -<br>- |
| | **Certificate Stream** - This setting allows customers to input hash stream for PKI provisioning custom certificate 1.<br><br>***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. | UP4<br>UP3 | -<br>- |
| **Click on Intel® AMT in the left tabs menu> OEM Default Certificate 2 is expanded by default:** | | | |




| # | Parameter | Platform | Settings |
|---|---|---|---|
| 8 | **OEM Default Certificate 2** | | |
| | **Certificate Enabled**<br>**Values: Yes/No** - This setting allows customers to enable PKI provisioning Default certificate 2. | UP4<br>UP3 | No<br>No |
| | **Certificate Friendly Name** - This setting allows customers to assign a user friendly name for PKI provisioning Default Certificate 2. Maximum 32 characters. | UP4<br>UP3 | -<br>- |
| | **Certificate Stream** - This setting allows customers to input hash stream for PKI provisioning custom certificate 2.<br><br>***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. | UP4<br>UP3 | -<br>- |
| **Click on Intel® AMT in the left tabs menu> OEM Default Certificate 3 is expanded by default:** | | | |

| # | Parameter | Platform | Settings |
|---|---|---|---|

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

| | | | |
|---|---|---|---|
| 9 | **OEM Default Certificate 3** | | |
| | **Certificate Enabled**<br>**Values: Yes/No** - This setting allows customers to enable PKI provisioning Default certificate 3. | UP4<br>UP3 | No<br>No |
| | **Certificate Friendly Name** - This setting allows customers to assign a user friendly name for PKI provisioning Default Certificate 3. Maximum 32 characters. | UP4<br>UP3 | -<br>- |
| | **Certificate Stream** - This setting allows customers to input hash stream for PKI provisioning custom certificate 3.<br><br>***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. | UP4<br>UP3 | -<br>- |

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

| # | Parameter | Platform | Settings |
|---|---|---|---|
| 10 | **OEM Default Certificate 4** | | |
| | **Certificate Enabled**<br>**Values: Yes/No** - This setting allows customers to enable PKI provisioning Default certificate 4. | UP4<br>UP3 | No<br>No |
| | **Certificate Friendly Name** - This setting allows customers to assign a user friendly name for PKI provisioning Default Certificate 4. | UP4<br>UP3 | -<br>- |
| | **Certificate Stream** - This setting allows customers to input hash stream for PKI provisioning custom certificate 4.<br><br>***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. | UP4<br>UP3 | -<br>- |

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

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

| # | Parameter | Platform | Settings |
|---|---|---|---|
| 11 | **OEM Default Certificate 5** | | |
| | **Certificate Enabled**<br>**Values: Yes/No** - This setting allows customers to enable PKI provisioning Default certificate 5. | UP4<br>UP3 | No<br>No |
| | **Certificate Friendly Name** - This setting allows customers to assign a user friendly name for PKI provisioning Default Certificate 5. | UP4<br>UP3 | -<br>- |
| | **Certificate Stream** - This setting allows customers to input hash stream for PKI provisioning custom certificate 5.<br><br>***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. | UP4<br>UP3 | -<br>- |

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

Redirection Configuration 12

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

| # | Parameter | Platform | Settings |
|---|---|---|---|
| 12 | **Redirection Configuration** | | |
| | **Redirection Localized Language -** This setting allows customers to configure which localized language will be used initially by firmware for user consent output information (Examples: May be displayed before SOL / KVM session starts). | UP4<br>UP3 | English<br>English |
| | **Redirection Privacy / Security Level** - This setting allows customers to configure the Privacy and Security level for redirection operations.<br>**Default** enables all redirection ports (User consent is configurable).<br>**Enhanced** - Enables all redirection ports. (User consent is required and cannot be disabled).<br>**Extreme -** Disables Redirection and Remote Configuration / Client Control Mode.<br><br>***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. | UP4<br>UP3 | Default<br>Default |

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

TLS Configuration 13

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

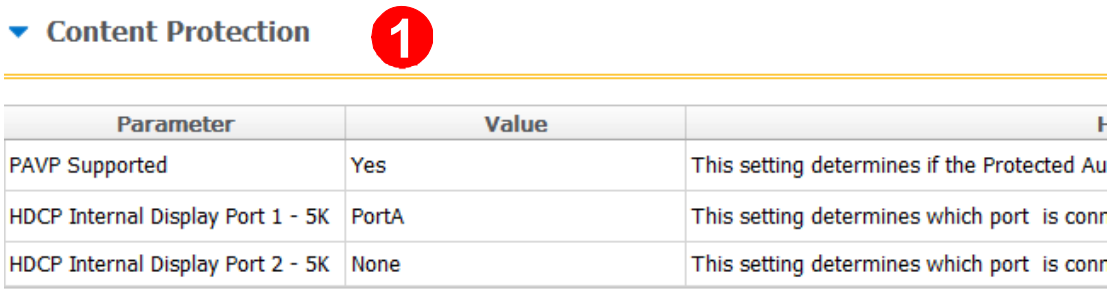
| # | Parameter | Platform | Settings |
|---|---|---|---|
| 13 | **TLS Configuration** | | |

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

| | | | |
|---|---|---|---|
| | **Transport Layer Security Supported**<br>**Values: Yes / No** - This setting allows customers to enable / disable firmware Transport Layer Security support.<br><br>***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. | UP4<br>UP3 | No<br>No |

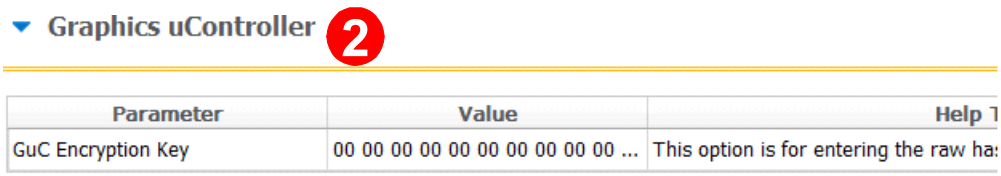
## Table 2-7. - Platform Protection (Sheet 1 of 6)

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




| # | Parameter | Platform | Settings |
|---|---|---|---|
| 1 | **Content Protection** | | |
| | **PAVP Supported**<br>**Values: Yes / No**<br>This setting determines if the Protected Audio Video Path (PAVP) feature will be permanently disabled in the FW image. | UP4<br>UP3 | Yes<br>Yes |
| | **HDCP Internal Display Port 1 - 5K**<br>**Values: None, Port A, Port B, Port C, Port D**<br>This setting determines which port is connected for 5K output on the Internal Display 1.<br><br>***Note:*** Both Display Port 1 & 2 need to be configured for proper operation. | UP4<br>UP3 | PortA<br>PortA |
| | **HDCP Internal Display Port 2 - 5K**<br>**Values: None, Port A, Port B, Port C, Port D**<br>This setting determines which port is connected for 5K output on the Internal Display 2.<br><br>***Note:*** Both Display Port 1 & 2 need to be configured for proper operation. | UP4<br>UP3 | None<br>None |

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




| # | Parameter | Platform | Settings |
|---|---|---|---|
| 2 | **Graphics UController** | | |
| | **GuC Encryption Key**<br>**Values:** This option is for entering the raw hash 256 bit string or certificate file for the Graphics uController. | UP4<br>UP3 | 0x00000000<br>0x00000000 |

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

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

### Hash Key Configuration for Bootguard / ISH 3

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

| # | Parameter | Platform | |
|---|---|---|---|
| 3 | **Hash Key Configuration for Bootguard / ISH** | | |
| | **OEM Public Key Hash**<br>**Values:** This option is for entering the raw hash string or certificate file for Boot Guard and ISH. This 384-bit field represents the SHA-384 hash of the OEM public key corresponding to the private key used to sign the BIOS-SM or ISH image. Please see Appendix F for further details. | UP4<br>UP3 | 0x00000000<br>0x00000000 |
| | **OEM Key Manifest Binary**<br>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). | UP4<br>UP3 | |
| | **Second OEM Key hash**<br>**Values:** This option is for entering a secondary raw hash string or certificate file for Boot Guard and ISH used in instances of OEM Key Revocation. This 384-bit field represents the SHA-384 hash of the OEM public key corresponding to the private key used to sign the BIOS-SM or ISH image. Please see Appendix F for further details.<br>***Note:*** This setting is greyed out and not configurable until the Second OEM Key Revocation Enable is set to Yes. | UP4<br>UP3 | 0x00000000<br>0x00000000 |
| | **OEM Key Revocation Enabled**<br>**Values: Yes/No**<br>This setting enables firmware OEM Key Revocation capabilities.<br>***Note:*** This setting requires that both OEM Public Key Hash and Second OEM Key Hash are configured. | UP4<br>UP3 | No<br>No |

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

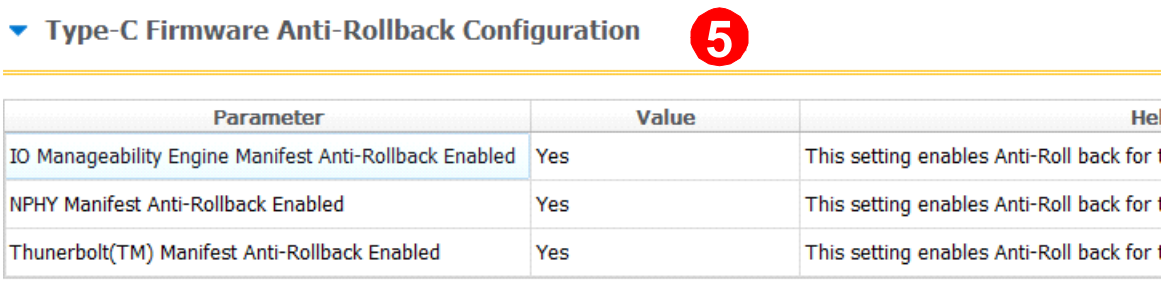
### Boot Guard Configuration 4

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

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

| # | Parameter | Platform | Settings |
|---|---|---|---|
| 4 | **Boot Guard Configuration** | | |
| | **Key Manifest ID**<br>**Values:** This option is for entering the hash of another public key, used by the ACM to verify the Boot Policy Manifest. | UP4<br>UP3 | 0x0<br>0x0 |
| | **Boot Guard Profile Configuration**<br>**Values: Boot Guard Profile 0 - No_FVME**<br>**Boot Guard Profile 3 - VM**<br>**Boot Guard Profile 4 - FVE**<br>**Boot Guard Profile 5 - FVME**<br>This option configures which Boot Guard Policy Profile will be used. | UP4<br>UP3 | Boot Guard Profile 0 - No_FVME<br>Boot Guard Profile 0 - No_FVME |
| | **CPU Debugging**<br>**Values: Enabled / Disabled**<br>This setting determines if CPU debug modes will be displayed. When set to 'Enabled' CPU debugging is enabled. | UP4<br>UP3 | Enabled<br>Enabled |
| | **BSP Initialization**<br>**Values: Enabled / Disabled**<br>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). | UP4<br>UP3 | Enabled<br>Enabled |
| | **S3 Optimization**<br>**Values: Enabled / Disabled**<br>This setting overrides Boot Guard S3 optimization.<br><br>***Note:*** This setting is for testing purposes only. | UP4<br>UP3 | Enabled<br>Enabled |

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




| # | Parameter | Platform | Settings |
|---|---|---|---|
| 5 | **Type-C Firmware Anti-Rollback Configuration** | | |
| | **IO Manageability Engine Manifest Anti-Rollback Enabled**<br>**Values: Yes / No**<br>This setting enables Anti-Rollback for the Type-C Subsystem I/O Manageability Engine binary. | UP4<br>UP3 | Yes<br>Yes |
| | **NPHY Manifest Anti-Rollback Enabled**<br>**Values: Yes / No**<br>This setting enabled Anti-Rollback for the Type-C Subsystem NPHY binary. | UP4<br>UP3 | Yes<br>Yes |

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

| | | | |
|---|---|---|---|
| | **Thunerbolt(TM) Manifest Anti-Rollback Enabled**<br>**Values: Yes/No**<br>This | UP4<br>UP3 | Yes<br>Yes |
| **Click on Platform Protection in the left tabs menu> Intel® PTT Configuration is expanded by default:** | | | |

Intel(R) PTT Configuration 6

| Parameter | Value | |
|---|---|---|
| Intel(R) PTT Supported | Yes | This setting permanently disables |
| Intel(R) PTT initial power-up state | Enabled | - |
| Intel(R) PTT Supported [FPF] | Yes | This setting will permanently disa |

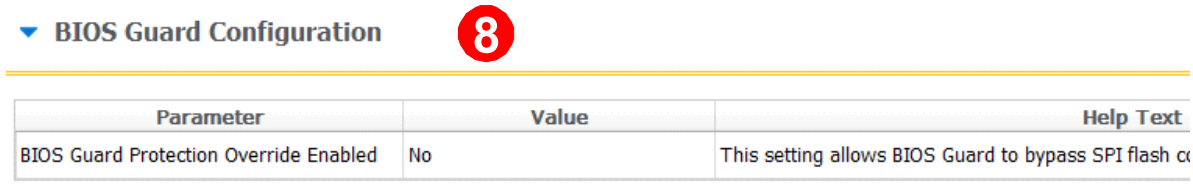
| # | Parameter | Platform | Settings |
|---|---|---|---|
| 6 | **Intel® PTT Configuration** | | |
| | **Intel® PTT Supported**<br>**Values: Yes/No** - This setting permanently disables Intel® PTT in the firmware image. | UP4<br>UP3 | Yes<br>Yes |
| | **Intel® PTT initial power-up state**<br>**Values: Enabled/Disabled** - This setting determines if Intel® PTT is enabled on platform power-up. | UP4<br>UP3 | Enabled<br>Enabled |
| | **Intel® PTT Supported [FPF]**<br>**Values: Yes/No** - This setting will permanently disable Intel® PTT through platform FPFs.<br>***Caution:*** Setting this option to Yes will permanently disable Intel® PTT on the platform hardware. | UP4<br>UP3 | Yes<br>Yes |
| **Click on Platform Protection in the left tabs menu> TPM Over SPI Bus Configuration is expanded by default:** | | | |

TPM Over SPI Bus Configuration 7

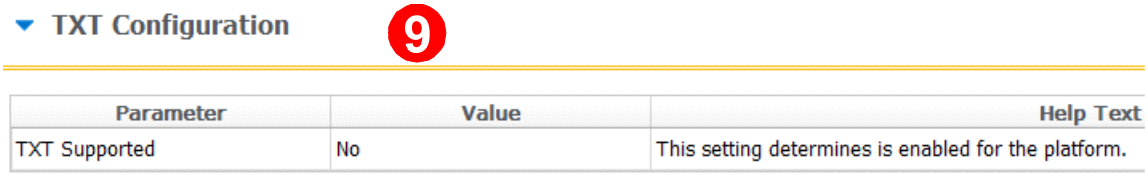
| Parameter | Value | Help Text |
|---|---|---|
| TPM Clock Frequency | 14MHz | This setting determines the clock frequency setting to be used fo |
| TPM Over SPI Bus Enabled | Yes | This setting determines the clock frequency setting to be used fo |

| # | Parameter | Platform | Settings |
|---|---|---|---|
| 7 | **TPM Over SPI Bus Configuration** | | |
| | **TPM Clock Frequency**<br>**Values: 14MHz, 25MHz, 48MHz** - This setting determines the clock frequency setting to be used for the TPM over SPI bus. | UP4<br>UP3 | 14MHz<br>14MHz |
| | **TPM Over SPI Bus Enabled**<br>**Values: Yes/No** - This setting determines if TPM over SPI bus is enabled on the platform. | UP4<br>UP3 | No<br>No |
| **Click on Platform Protection in the left tabs menu> BIOS Guard Configuration is expanded by default:** | | | |

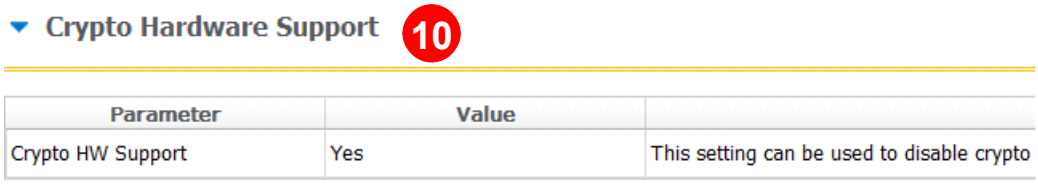
## Table 2-7. - Platform Protection (Sheet 5 of 6)




| # | Parameter | Platform | Settings |
|---|---|---|---|
| 8 | **BIOS Guard Configuration** | | |
| | **BIOS Guard Protection Override Enabled**<br>This setting allows BIOS Guard to bypass SPI flash controller protections (i.e. Protected Range Registers and Top Swap). | UP4<br>UP3 | No<br>No |
| **Click on Platform Protection in the left tabs menu> TXT Configuration is expanded by default:** | | | |

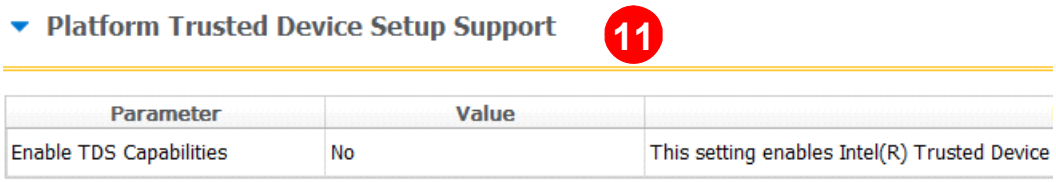



| # | Parameter | Platform | Settings |
|---|---|---|---|
| 9 | **TXT Configuration** | | |
| | **TXT Supported**<br>This setting determines if enabled for the platform. | UP4<br>UP3 | No<br>No |
| **Click on Platform Protection in the left tabs menu> Crypto Hardware Support is expanded by default:** | | | |



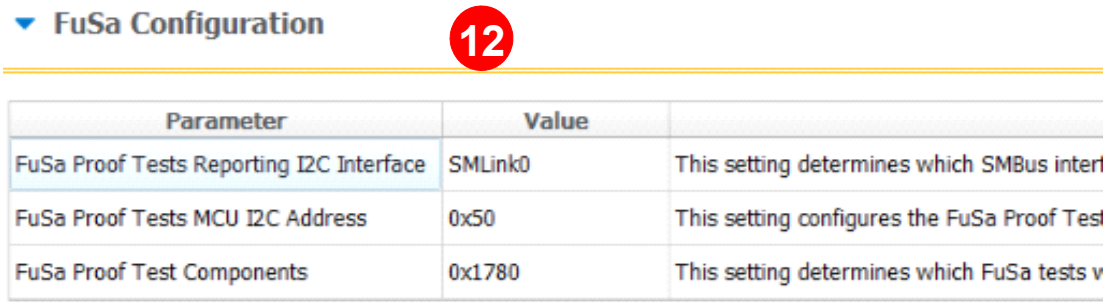

| # | Parameter | Platform | Settings |
|---|---|---|---|
| 10 | **Crypto HW Support** | | |
| | **Crypto HW Support**<br>**Values: Yes / No** - This setting can be used to disable Intel® CSME cryptographic functionality.<br>***Caution:*** Configuring this setting to "No" will disables all Intel® CSME cryptographic related features. | UP4<br>UP3 | Yes<br>Yes |
| **Click on Platform Protection in the left tabs menu> Platform Trusted Device Setup Support is expanded by default:** | | | |

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




| # | Parameter | Platform | Settings |
|---|---|---|---|
| 11 | **Platform Trusted Device Setup Support** | | |
| | **Enable TDS Capabilities**<br>**Values: Yes / No** - This setting enables Intel® Trusted Device Setup on the platform. | UP4<br>UP3 | No<br>No |

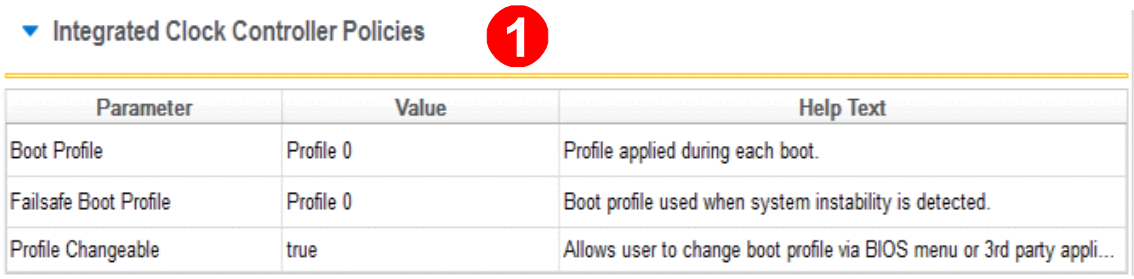
**Click on Platform Protection in the left tabs menu> FuSa Configuration is expanded by default:**




| # | Parameter | Platform | Settings |
|---|---|---|---|
| 12 | **FuSa Configuration**<br>***Note:*** The GBST sub-partition is used to enabling FuSa safety standards and is not applicable for client platforms. | | |
| | **FuSa Proof Tests Reporting I2C Interface**<br>**Values:** | UP4<br>UP3 | SMLink0<br>SMLink0 |
| | **FuSa Proof Tests MCU I2C Address**<br>**Values:** | UP4<br>UP3 | 0x50<br>0x50 |
| | **FuSa Proof Tests Components**<br>**Values:** | UP4<br>UP3 | 0x1780<br>0x1780 |

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

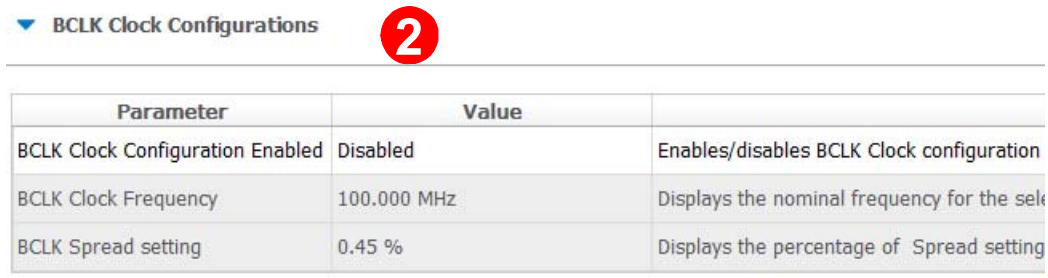
**Click on Integrated Clock Controller in the left tabs menu> Integrated Clock Controller Policies are expanded by default:**




| # | Parameter | Platform | Settings |
|---|---|---|---|
| 1 | **Integrated Clock Controller Policies** | | |
| | **Boot Profile**<br><br>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.<br><br>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".<br><br>The 'Record #' refers to profile created under the "Integrated Clock Controller \| Profiles".<br>Default boot profile for system is Profile 0.<br><br>Double click on value column of this parameter to choose from available options. | UP4<br>UP3 | Profile 0<br>Profile 0 |
| | **Failsafe Profile**<br><br>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.<br><br>The 'Record #' refers to profile created under the "Integrated Clock Controller \| Profiles".<br>Default Failsafe boot profile for system is Profile 0.<br><br>Double click on value column of this parameter to choose from available options. | UP4<br>UP3 | Profile 0<br>Profile 0 |
| | **Profile Changeable**<br><br>Possible configuration: True/False.<br><br>This parameter controls if BIOS or 3rd party application can select boot profile or not. When set to true, it allows user to change boot profile via BIOS or 3rd party application. When set to false, Runtime change to boot profile is not allowed and boot profile selected by **"Integrated Clock Controller \|Integrated Clock Controller Policies - Boot Profile "** parameter will be used to boot platform.<br><br>Double click on value column of this parameter to choose from available options. | UP4<br>UP3 | True<br>True |

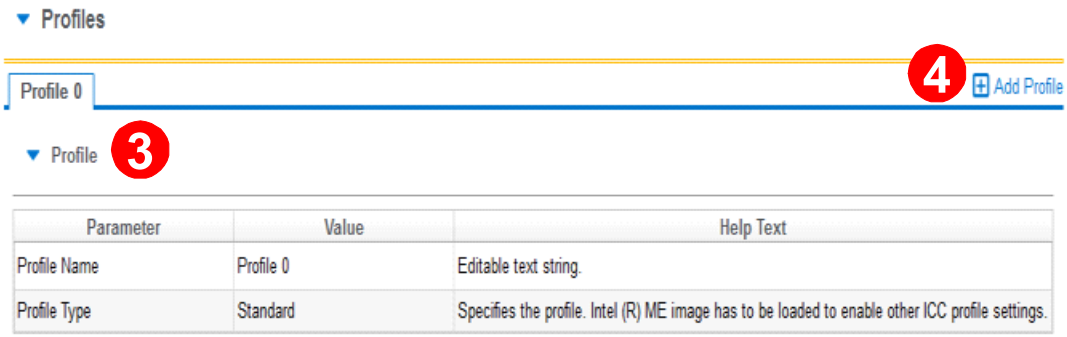
**Click on Integrated Clock Controller in the left tabs menu> Profiles >Profile> Bclk Clock Configuration is expanded by default:**

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




| # | Parameter | Platform | Settings |
|---|---|---|---|
| 2 | **BCLK Clock Configuration** | | |
| | **BCLK Clock Configuration Enabled**<br>**Values: Enabled / Disabled**<br><br>This setting enables / disables BCLK Clock configuration values for Adaptive / Overclocking profiles | UP4<br>UP3 | Disabled<br>Disabled |
| | **BCLK Clock Frequency**<br><br>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.<br><br>**Standard Setting Profile Type -** Option is grayed out.<br>**Adaptive Setting Profile Type -** Option is able to be edited. | UP4<br>UP3 | N/A<br>N/A |
| | **BCLK Spread Setting**<br><br>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.<br><br>**BCLK Clock Frequency**<br>**Standard Setting Profile Type -** Option is grayed out.<br>**Adaptive Setting Profile Type -** Option is able to be edited. | UP4<br>UP3 | N/A<br>N/A |

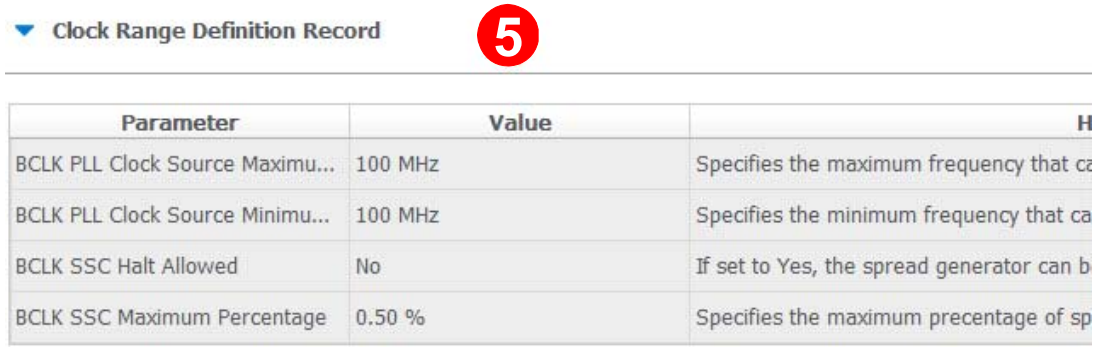
**Click on Integrated Clock Controller in the left tabs menu> Profiles are expanded by default:**



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

| # | Parameter | Platform | Settings |
|---|---|---|---|
| 3 | **Profiles - Profile 0**<br><br>**Note:** Intel® ME image has to be loaded to enable other ICC profile settings.<br><br>**For UP4/U,** Intel® FIT provides 2 pre-defined ICC profiles to choose from.<br>•**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.<br>•**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.<br><br>**For** TGL UP3/UP4**,** Intel® FIT provides 5 pre-defined ICC profiles to choose from.<br><br>•**Standard**<br>•**Adaptive**<br><br>**Note**: User can select pre-defined profiles via **"Integrated Clock Controller \| Profiles - Profile Type "** parameter<br><br>User can add up to maximum 16 profiles.To add new profile, please use **"Integrated Clock Controller \| Profiles - + Add Profile Button"** | UP4<br>UP3 | Standard<br>Standard |
| | **Profile Name**<br><br>This parameter allows user to customize profile name for easy identification. By default it uses pre-defined profile name like Profile 0. | UP4<br>UP3 | Profile 0<br>Profile 0 |
| | **Profile Type**<br><br>Available ICC profiles for TGL UP3/UP4 are Standard, Adaptive.<br><br>This parameter indicates which pre- defined profile selected for each profile#.<br><br>Double click on value column of this parameter to choose from available options. | UP4<br>UP3 | Standard<br>Standard |
| 4 | **+ Add Profile Button**<br><br>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**.** | UP4<br>UP3 | |
| **Click on Integrated Clock Controller in the left tabs menu> Profiles >Profile> Clock Range Definition Record is expanded by default:** | | | |

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




| # | Parameter | Platform | Settings |
|---|---|---|---|
| 5 | **Clock Range Definition Record** | | |
| | **BCLK PLL Clock Source Maximum Frequency -** This parameter allows user to specify the maximum frequency that can be applied to BCLK clock source when overclocking the platform. Value is limited by divider/frequency limits determined by HW SKU, and cannot be less than 100 MHz.<br><br>**Standard Setting Profile Type -** Option is grayed out.<br>**Adaptive Setting Profile Type -** Option is able to be edited. | UP4<br>UP3 | |
| | **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.<br><br>**Standard Setting Profile Type -** Option is grayed out.<br>**Adaptive Setting Profile Type -** Option is able to be edited. | UP4<br>UP3 | |
| | **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.<br><br>**Standard Setting Profile Type -** Option is grayed out.<br>**Adaptive Setting Profile Type -** Option is able to be edited. | UP4<br>UP3 | |
| | **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%)<br><br>**Standard Setting Profile Type -** Option is grayed out.<br>**Adaptive Setting Profile Type -** Option is able to be edited. | UP4<br>UP3 | |

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

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

Clock Output Configuration 6

| Parameter | Value | |
|---|---|---|
| SRC0 | Enabled | Enable/Disable the CLKOUT_SRC0 |
| SRC1 | Enabled | Enable/Disable the CLKOUT_SRC1 |
| SRC2 | Enabled | Enable/Disable the CLKOUT_SRC2 |
| SRC3 | Enabled | Enable/Disable the CLKOUT_SRC3 |
| SRC4 | Enabled | Enable/Disable the CLKOUT_SRC4 |
| SRC5 | Enabled | Enable/Disable the CLKOUT_SRC5 |
| SRC6 | Enabled | Enable/Disable the CLKOUT_SRC6 |

| # | Parameter | Platform | Settings |
|---|---|---|---|
| 6 | **Clock Output Configuration** | | |
| | **SRC0[6:15]**<br>**Values: Enabled / Disabled**<br>These parameters come under the Power Management section and they control Enabling /Disabling of specific Output Clocks at boot time.<br>These settings should match with platform hardware design.<br><br>For CRB, recommend keeping defaults for bring up with Intel® CSME FW.<br><br>These parameters are specifically used to Enable/Disable the respective CLKOUT_XXX differential output buffers | UP4<br>UP3 | Enabled<br>Enabled |
| | **SRC1**<br>**Values: Enabled / Disabled**<br>Enables or Disables the CLKOUT_SRC1 differential output buffer. | UP4<br>UP3 | Enabled<br>Enabled |
| | **SRC2**<br>**Values: Enabled / Disabled**<br>Enables or Disables the CLKOUT_SRC2 differential output buffer. | UP4<br>UP3 | Enabled<br>Enabled |
| | **SRC3**<br>**Values: Enabled / Disabled**<br>Enables or Disables the CLKOUT_SRC3 differential output buffer. | UP4<br>UP3 | Enabled<br>Enabled |
| | **SRC4**<br>**Values: Enabled / Disabled**<br>Enables or Disables the CLKOUT_SRC4 differential output buffer. | UP4<br>UP3 | Enabled<br>Enabled |
| | **SRC5**<br>**Values: Enabled / Disabled**<br>Enables or Disables the CLKOUT_SRC5 differential output buffer. | UP4<br>UP3 | Disabled<br>Disabled |
| | **SRC6**<br>**Values: Enabled / Disabled**<br>Enables or Disables the CLKOUT_SRC6 differential output buffer. | UP4<br>UP3 | Disabled<br>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:**

Power Management Configuration 7

| Parameter | Value | |
|---|---|---|
| SRC0 CLKREQ# Mapping | GPP_D5 | Assign the CLKREQ# signal associat |
| SRC1 CLKREQ# Mapping | GPP_D6 | Assign the CLKREQ# signal associat |
| SRC2 CLKREQ# Mapping | GPP_D7 | Assign the CLKREQ# signal associat |
| SRC3 CLKREQ# Mapping | GPP_D8 | Assign the CLKREQ# signal associat |
| SRC4 CLKREQ# Mapping | GPP_H10 | Assign the CLKREQ# signal associat |
| SRC5 CLKREQ# Mapping | GPP_H11 | Assign the CLKREQ# signal associat |
| SRC6 CLKREQ# Mapping | GPPC_F19 | Assign the CLKREQ# signal associat |

| # | Parameter | Platform | Settings |
|---|---|---|---|
| 7 | **Profile Power Management Configuration**<br><br>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.<br><br>**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**<br>Possible configuration: Select one of the GPIOs from the list to map it as a CLKREQ# for specific SRC# Output clock.<br>This parameter controls association of dynamic CLKREQ control with SRC (PCIe) clocks.<br><br>**SRC[15:6] CLKREQ# Mapping - TGL/CFL H/S Only**<br>Possible configuration: Select one of the GPIOs from the list to map it as a CLKREQ# for specific SRC# Output put clock.<br>This parameter controls association of dynamic CLKREQ control with SRC (PCIe) clocks. | UP4<br>UP3 | GPP_D5<br>GPP_D5 |
| | **SRC1 CLKREQ# Mapping**<br>Assign the CLKREQ# signal associated with CLKOUT_SRC1. | UP4<br>UP3 | GPP_D6<br>GPP_D6 |
| | **SRC2 CLKREQ# Mapping**<br>Assign the CLKREQ# signal associated with CLKOUT_SRC2. | UP4<br>UP3 | GPP_D7<br>GPP_D7 |
| | **SRC3 CLKREQ# Mapping**<br>Assign the CLKREQ# signal associated with CLKOUT_SRC3. | UP4<br>UP3 | GPP_D8<br>GPP_D8 |
| | **SRC4 CLKREQ# Mapping**<br>Assign the CLKREQ# signal associated with CLKOUT_SRC4. | UP4<br>UP3 | GPP_H10<br>GPP_H10 |
| | **SRC5 CLKREQ# Mapping**<br>Assign the CLKREQ# signal associated with CLKOUT_SRC5. | UP4<br>UP3 | GPP_H11<br>GPP_H11 |

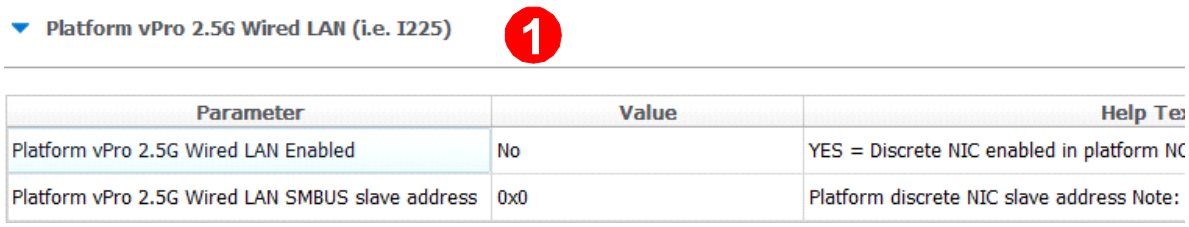
## Table 2-8. - Integrated Clock Controller (Sheet 7 of 7)

| | | | |
|---|---|---|---|
| | **SRC6 CLKREQ# Mapping**<br>Assign the CLKREQ# signal associated with CLKOUT_SRC6. | UP4<br>UP3 | GPP_F19<br>GPP_F19 |
| **Click on Integrated Clock Controller in the left tabs menu> Profiles >Profile> PCIe RefClock Configuration is expanded by default:** | | | |

| # | Parameter | Platform | Settings |
|---|---|---|---|
| 8 | **PCIe RefClock Configuration** | | |
| | **SSCEN**<br>**Values: Enabled / Disabled** | UP4<br>UP3 | Enabled<br>Enabled |

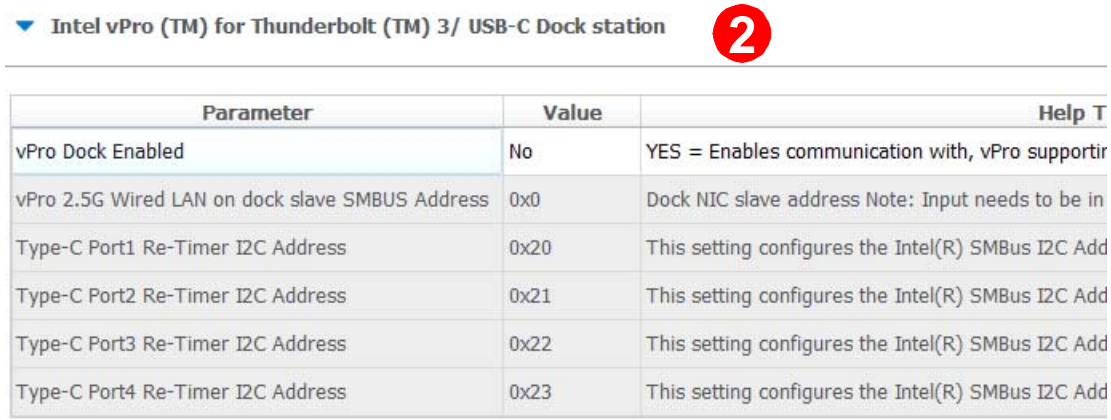
## Table 2-9. - Networking & Connectivity (Sheet 1 of 5)

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




| # | Parameter | Platform | Settings |
|---|---|---|---|
| 1 | **Platform vPro 2.5G Wired LAN** | | |
| | **Platform vPro 2.5G Wired LAN Enabled**<br>**Values: Yes / No**<br>This setting enables / disables Discrete Intel® vPro Network adapter support on the platform. | UP4<br>UP3 | No<br>No |
| | **Platform vPro 2.5G Wired LAN slave SMBus Address**<br>**Values: Hex**<br>This setting configures the SMBus address for the Discrete Intel® vPro Network adapter. | UP4<br>UP3 | 0x49<br>0x49 |
| **Click on Networking & Connectivity in the left tabs menu> Docking Station is expanded by default:** | | | |

## Table 2-9. - Networking & Connectivity (Sheet 2 of 5)

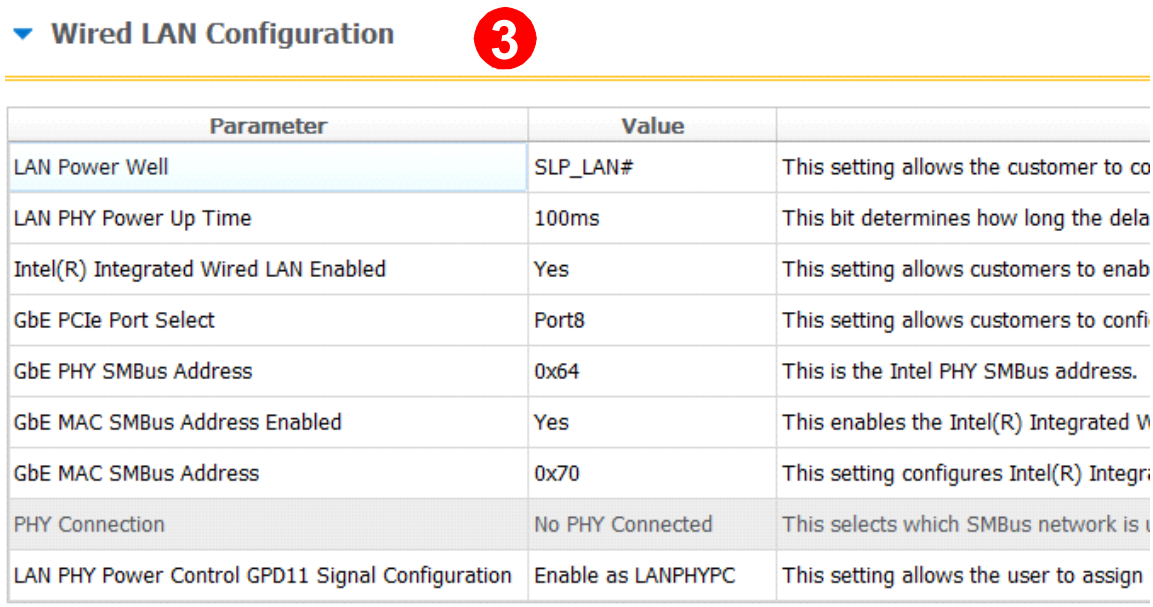


Intel vPro (TM) for Thunderbolt (TM) 3/ USB-C Dock station

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

| # | Parameter | Platform | Settings |
|---|---|---|---|
| 2 | **Intel vPro(TM) for Thinderbolt 3(TM) / USB-C Dock Station** | | |
| | **vPro Dock Enabled**<br>This setting enables Intel® vPro communication over supported NIC in a Thunderbolt™ Dock. | UP4<br>UP3 | No<br>No |
| | **vPro 2.5G Wired LAN on dock slave SMBus Address**<br>This setting configures the NIC SMBus slave address. | UP4<br>UP3 | 0x0<br>0x0 |
| | **Type-C Port1 Re-Timer I2C Address**<br>This setting configures Intel® SMBus I2C Address. | UP4<br>UP3 | 0x20<br>0x20 |
| | **Type-C Port2 Re-Timer I2C Address**<br>This setting configures Intel® SMBus I2C Address. | UP4<br>UP3 | 0x21<br>0x21 |
| | **Type-C Port3 Re-Timer I2C Address**<br>This setting configures Intel® SMBus I2C Address. | UP4<br>UP3 | 0x22<br>0x22 |
| | **Type-C Port4 Re-Timer I2C Address**<br>This setting configures Intel® SMBus I2C Address. | UP4<br>UP3 | 0x23<br>0x23 |
| **Click on Networking & Connectivity in the left tabs menu> Wired LAN Configuration is expanded by default:** | | | |

## Table 2-9. - Networking & Connectivity (Sheet 3 of 5)



Wired LAN Configuration 3

| Parameter | Value | |
|---|---|---|
| LAN Power Well | SLP_LAN# | This setting allows the customer to co |
| LAN PHY Power Up Time | 100ms | This bit determines how long the dela |
| Intel(R) Integrated Wired LAN Enabled | Yes | This setting allows customers to enab |
| GbE PCIe Port Select | Port8 | This setting allows customers to confi |
| GbE PHY SMBus Address | 0x64 | This is the Intel PHY SMBus address. |
| GbE MAC SMBus Address Enabled | Yes | This enables the Intel(R) Integrated W |
| GbE MAC SMBus Address | 0x70 | This setting configures Intel(R) Integr |
| PHY Connection | No PHY Connected | This selects which SMBus network is u |
| LAN PHY Power Control GPD11 Signal Configuration | Enable as LANPHYPC | This setting allows the user to assign |

| # | Parameter | Platform | Settings |
|---|---|---|---|
| 3 | **Wired LAN Configuration** | | |
| | **LAN Power Well**<br>**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.<br>**Note:** Recommended setting is SLP_LAN#. | UP4<br>UP3 | SLP_LAN#<br>SLP_LAN# |
| | **LAN PHY Power Up Time**<br>**Values: 50ms, 100ms** | UP4<br>UP3 | 100ms<br>100ms |
| | **Intel® Integrated Wired LAN Enable**<br>**Values: Enabled/Disabled -** This setting enables or disables the Intel® Integrated LAN. | UP4<br>UP3 | Enabled<br>Enabled |
| | **GbE PCIe Port Select**<br>**Values: None, PORT7, PORT8, PORT9** - This setting allows customers to configure the PCIe Port that will Intel® Integrated LAN will operate on. | UP4<br>UP3 | Port 7<br>Port 7 |
| | **GbE PHY SMBus Address**<br>This setting configures Intel® Integrated Wired LAN SMBus address to accept SMBus cycles from the MAC. **Note:** Recommended setting is 64h. | UP4<br>UP3 | 0x64<br>0x64 |
| | **GbE SMBus Address Enabled**<br>**Values: Yes/No** - This enables the Intel® Integrated Wired LAN MAC SMBus address. **Note:** This setting must be enabled if using Intel® Integrated LAN. | UP4<br>UP3 | Yes<br>Yes |
| | **GbE MAC SMBus Address** | UP4<br>UP3 | 0x70<br>0x70 |
| | **PHY Connection**<br>**Values: No PHY connected, PHY on SMLink0** | UP4<br>UP3 | PHY on SMLink0<br>PHY on SMLink0 |
| | **LAN PHY Power Control GPD11 Signal Configuration**<br>**Values: GPD11, LANPHYPC -** This setting allows the customer to assign the LAN PHY Power Control signal to GbE or as GDP11.<br>**Note:** If using Intel® Integrated LAN this setting should be set to "Enable as LANPHYPC". | UP4<br>UP3 | LANPHYPC<br>LANPHYPC |
| **Click on Networking & Connectivity in the left tabs menu> Wireless LAN Configuration is expanded by default:** | | | |

## Table 2-9. - Networking & Connectivity (Sheet 4 of 5)

### Wireless LAN Configuration 4

| Parameter | Value | |
|---|---|---|
| Intel(R) ME CLINK Signal Enabled | Yes | This setting allows customers to enable / dis |
| WLAN Microcode | 0x9DF0 PULSAR | This setting allows OEMs to configure which |
| WLAN Power Well | SLP_WLAN# | - |
| On Die CLINK Enabled | Enabled | This setting determines whether the interna |
| SLP_WLAN# / GDP9 Signal Con... | Enable as SLP_WLAN# | This setting allows user the to assign the WI |

| # | Parameter | Platform | Settings |
|---|---|---|---|
| 4 | **Wireless LAN Configuration** | | |
| | **CLINK Enabled**<br>**Values: Yes/No**<br>This setting allows customers to enable / disable the Wireless LAN CLINK signal through Intel® CSME firmware.<br>***Note:*** For using Intel® vPro Wireless solutions this should be set to "Yes". | UP4<br>UP3 | No<br>No |
| | **WLAN Microcode**<br>This setting allow OEMs to configure which Intel® Wireless LAN card microcode to load into the firmware image. | UP4<br>UP3 | 0xA0F0<br>0xA0F0 |
| | **WLAN Power Well**<br>**Values: Disabled, Sus Well, ME Well, SLP_M#\|\|SPDA, SLP_WLAN#**<br>This setting allows OEMs to configure the power well that will be used by Intel® Wireless LAN.<br>WLAN Sleep via SLP_WLAN# (default)<br>***Note:*** Recommended setting is SLP_WLAN#. | UP4<br>UP3 | SLP_WLAN#<br>SLP_WLAN# |
| | **On Die CLINK Enabled**<br>**Values: Enabled/Disabled**<br>This setting determines if the internal CNVi / On-die CLINK port is enabled. | UP4<br>UP3 | Enabled<br>Enabled |
| | **SLP_WLAN# / GPD9 Signal Configuration**<br>**Values: SLP_WLAN#, GPD9**<br>This setting allows the customer to assign the WLAN Power Control signal to WLAN or as GDP9.<br>***Note:*** If using Intel® Wireless LAN this setting should be set to "Enable as SLP_WLAN#". | UP4<br>UP3 | Enable as SLP_WLAN#<br>Enabled as SLP_WLAN # |

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

### Time Sensitive Networking Configuration 5

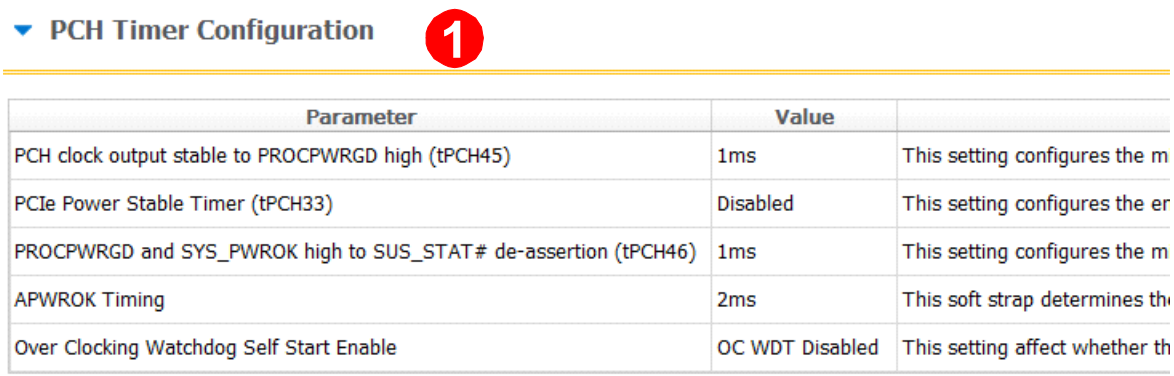
| Parameter | Value | |
|---|---|---|
| Time Sensitive Networking | TSN Disabled | This setting allows customers to enable / di |
| TSN GbE Port Select | None | This setting allows customers to configure t |

## Table 2-9. - Networking & Connectivity (Sheet 5 of 5)

| # | Parameter | Platform | Settings |
|---|---|---|---|
| 5 | **Time Sensitive Networking Configuration** | | |
| | **Time Sensitive Networking**<br>**Values: TSN Enable / TSN Disabled**<br><br>***Note:*** Time Sensitive Networking and Wired LAN are mutually exclusive only one of these features can enabled on the platform. | UP4<br>UP3 | Disabled<br>Disabled |
| | **TSN GbE PCIe Port Select**<br>**Values: None, TSN PORT6, TSN PORT 7** - This setting allows customers to configure the PCIe port that TSN will operate on.<br><br>***Note:*** The Intel® Integrated LAN and TSN GbE are mutually exclusive. | UP4<br>UP3 | None<br>None |

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

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




| # | Parameter | Platform | Settings |
|---|---|---|---|
| 1 | **PCH Timer Configuration** | | |
| | **PCH clock output stable to PROCPWRGD high (tPCH45)**<br>**Values: 100ms, 50ms, 5ms, 1ms** - This setting configures the minimum timing from XCK_PLL locked to CPUPWRGD high. For further details see Tiger Lake LP Platform Controller Hub EDS. | UP4<br>UP3 | 1ms<br>1ms |
| | **PCIe Power Stable Timer (tPCH33)**<br>**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.<br>***Note:*** The recommended setting is "Disabled". | UP4<br>UP3 | Disabled<br>Disabled |
| | **PROCPWRGD and SYS_PWROK high to SUS_STAT# de-assertion (tPCH46)**<br>**Values: 1ms, 2ms, 5ms** - This setting configures the minimum timing from CPUPWRGD assertion to SUS_STAT#. For further details see Tiger Lake LP Platform Controller Hub EDS. | UP4<br>UP3 | 1ms<br>1ms |
| | **APWROK Timing**<br>**Values: 2ms, 4ms, 8ms, 15ms** - This soft strap determines the time between the SLP_A# pin de-asserting and the APWROK timer expiration. For further details see Tiger Lake LP Platform Controller Hub EDS. | UP4<br>UP3 | 2ms<br>2ms |
| | **Over Clocking Watchdog Self Start Enable**<br>**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 | UP4<br>UP3 | OC WDT Disabled<br>OC WDT Disabled |

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

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

### SMBus / SMLink Configuration 2

| Parameter | Value | |
|---|---|---|
| Intel(R) SMLink0 MCTP Address Enabled | No | This setting enables / disables the Intel(R) SMLink0 MCT |
| Intel(R) SMLink0 MCTP Address | 0x0 | This setting configures the Intel(R) SMLink0 MCTP Addre |
| Intel(R) SMBus ASD Address | 0x0 | This setting configures the Intel(R) SMBus Alert Sending |
| Intel(R) SMBus ASD Address Enabled | No | This setting enables / disables the Intel(R) SMBus Alert S |
| Intel(R) SMBus Subsystem Vendor and Device ID for ASF | 0x0 | This setting configures the Intel(R) SMBus Subsystem Ve |
| Intel(R) SMBus I2C Address | 0x0 | This setting configures the Intel(R) SMBus I2C Address. I |
| Intel(R) SMBus I2C Address Enabled | No | This setting enables / disables the Intel(R) SMBus I2C Ac |
| Intel(R) SMBus MCTP Address | 0x0 | This setting configures the Intel(R) SMBus MCTP Address |
| Intel(R) SMBus MCTP Address Enabled | No | This setting enables / disables the Intel(R) SMBus MCTP |
| SMBus / SMLink TCO Slave Connection | Intel(R) SMBus | This setting configures the TCO Slave connection to ethe |
| SMLink0 Enabled | Yes | This setting enables / disables SMLink0 interface. For fur |
| SMLink0 Frequency | 1 MHz | This setting determines the frequency at which the SMLi |
| SMLink1 I2C Target Address | 0x0 | This setting configures SMLink1 I2C Target Address. For |
| SMLink1 I2C Target Address Enabled | No | This setting configures SMLink1 I2C Target Address. For |
| SMLink1 GP Target Address | 0x0 | This setting configures SMLink1 GP Target Address. For |
| SMLink1 GP Target Address Enabled | No | This setting enables / disables SMLink1 GP Target Addre |
| SMLink1 Enabled | No | This setting enables / disables SMLink1 interface. For fur |
| SMLink1 MCTP Address | 0x0 | This setting configures the Intel(R) SMBus MCTP Address |
| SMLink1 MCTP Address Enabled | No | This setting enables / disables the Intel(R) SMBus MCTP |
| SMLink1 Frequency | 100 KHz | This setting determines the frequency at which the SMLi |
| Intel(R) SMBus ASD Mode Configuration | Enable as GPP_C2 | This setting determines the native mode of operation for |
| SMLink0 I2C Address | 0x0 | This setting configures the SMLink0 I2C Address. Note: |
| SMLink0 I2C Address Enabled | No | This setting enables / disables the SMLink0 I2C Address. |

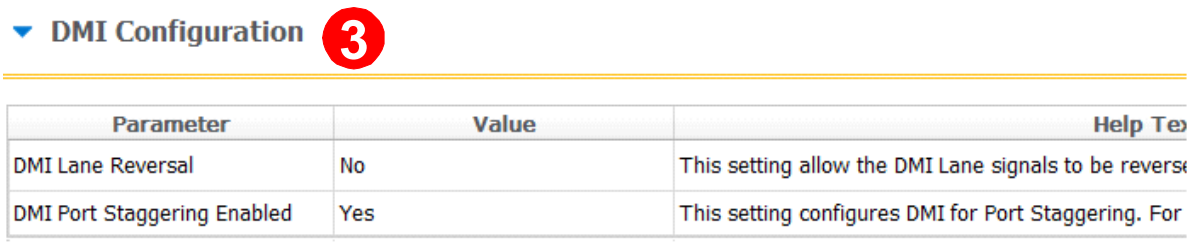
| # | Parameter | Platform | Settings |
|---|---|---|---|
| 2 | **SMBus / SMLink Configuration** | | |
| | **Intel® SMLink0 MCTP Address**<br>This setting configures the Intel® SMLink0 MCTP Address.<br>***Note:*** This setting is only used for testing. | UP4<br>UP3 | 0x0<br>0x0 |
| | **Intel® SMLink0 MCTP Address Enabled**<br>**Value: Yes/No**<br>This setting configures the Intel® SMLink0b MCTP Address.<br>***Note:*** This setting is only used for testing. | UP4<br>UP3 | No<br>No |
| | **Intel® SMBus ASD Address** - This setting configures the Intel® SMBus Alert Sending device Address. For details see Tiger Lake LP SPI Programming guide for further details. | UP4<br>UP3 | 0x0<br>0x0 |

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

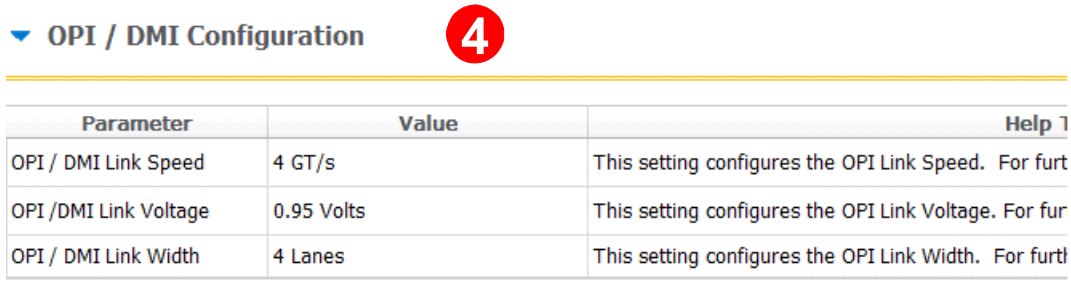
| # | Parameter | Platform | Settings |
|---|---|---|---|
| | **Intel® SMBus ASD Address Enabled**<br>**Values: Yes/No** - This setting enables / disables the Intel® SMBus Alert Sending device. For details see Tiger Lake LP SPI Programming guide for further details. | UP4<br>UP3 | No<br>No |
| | **Intel® SMBus Subsystem Vendor & device ID for ASF** - This setting configures the Intel® SMBus Subsystem Vendor & device ID for ASF. For details see Tiger Lake LP SPI Programming guide further details. | UP4<br>UP3 | 0x0<br>0x0 |
| | **Intel® SMBus I2C Address** - This setting configures the Intel® SMBus I2C Address. **Note:** This setting is only used for testing purposes. The recommended setting is "0000000". | UP4<br>UP3 | 0x0<br>0x0 |
| | **Intel® SMBus I2C Address Enabled**<br>**Values: Yes/No** - This setting enables / disables the Intel® SMBus I2C Address. Note: This setting is only used for testing purposes. The recommended setting is "No". | UP4<br>UP3 | No<br>No |
| | **Intel® SMBus MTCP Address** - This setting configures the Intel® SMBus MCTP Address. **Note:** This setting is only used for testing purposes. The default setting is "0000000". | UP4<br>UP3 | 0x0<br>0x0 |
| | **Intel® SMBus MCTP Address Enabled**<br>**Values: Yes/No** - This setting enables / disables the Intel® SMBus MCTP Address. **Note:** This setting is only used for testing purposes. The recommended setting is "No". | UP4<br>UP3 | No<br>No |
| | **SMBus / SMLink TCO Slave Connection**<br>**Values: Intel® SMBus, SMLink0** - This setting configures the TCO Slave connection to ether the Intel® SMBus or SMLink0. For further details see Tiger Lake LP Platform Controller Hub EDS. | UP4<br>UP3 | Intel® SMBus<br>Intel® SMBus |
| | **SMLink0 Enabled**<br>**Values: Yes/No** - This setting enables / disables SMLink0 interface. For further details see Tiger Lake LP Platform Controller Hub EDS. | UP4<br>UP3 | Yes<br>Yes |
| | **SMLink0 Frequency**<br>**Values: 100KHz, 400KHz, 1 MHz** - This setting determines the frequency at which the SMLink0 will operate. **Note:** The recommended setting is "1MHz". | UP4<br>UP3 | 1 MHz<br>1 MHz |
| | **SMLink1 I2C Target Address** - This setting configures SMLink1 I2C Target Address. For further details see Tiger Lake LP Platform Controller Hub EDS. | UP4<br>UP3 | 0x0<br>0x0 |
| | **SMLink1 I2C Target Address Enabled**<br>**Values: Yes/No** - This setting configures SMLink1 I2C Target Address. For further details see Tiger Lake LP Platform Controller Hub EDS. | UP4<br>UP3 | No<br>No |
| | **SMLink1 GP Target Address** - This setting configures SMLink1 GP Target Address. For further details see Tiger Lake LP Platform Controller Hub EDS. | UP4<br>UP3 | 0x0<br>0x0 |
| | **SMLink1 GP Target Address Enabled**<br>**Values: Yes/No** - This setting enables / disables SMLink1 GP Target Address interface. For further details see Tiger Lake LP Platform Controller Hub EDS. **Note:** This setting must be set to "Yes" if using PCH / MCP Thermal reporting. | UP4<br>UP3 | Yes<br>Yes |
| | **SMLink1 Enabled**<br>**Values: Yes/No** - This setting enables / disables SMLink1 interface. For further details see Tiger Lake LP Platform Controller Hub EDS. **Note:** This setting must be set to "Yes" if using PCH / MCP Thermal reporting. | UP4<br>UP3 | Yes<br>Yes |
| | **SMLine1 MTCP Address** - This setting configures the SMLink1 MCTP Address. **Note:** This setting is only used for testing purposes. The default setting is "0000000". | UP4<br>UP3 | 0x0<br>0x0 |
| | **SMLink1 MCTP Address Enabled**<br>**Values: Yes/No** - This setting enables / disables the SMLink1 MCTP Address. **Note:** This setting is only used for testing purposes. The recommended setting is "No". | UP4<br>UP3 | No<br>No |
| | **SMLink1 Frequency**<br>**Values: 100KHz, 400KHz, 1 MHz** - This setting determines the frequency at which the SMLink1 will operate. **Note:** The recommended setting is "100KHz". | UP4<br>UP3 | 100 KHz<br>100 KHz |
| | **Intel® SMBus ASD Mode Configuration**<br>This setting determines the native mode of operation for the Intel® SMBus ASD signal. | UP4<br>UP3 | Enable as GPP_C2<br>Enable as GPP_C2 |

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

| # | Parameter | Platform | Settings |
|---|---|---|---|
| | **SMLink0 I2C Target Address** - This setting configures SMLink0 I2C Target Address. For further details see Rocket Lake LP Platform Controller Hub EDS. | UP4<br>UP3 | 0x0<br>0x0 |
| | **SMLink0 I2C Target Address Enabled**<br>**Values: Yes/No** - This setting configures SMLink0 I2C Target Address. For further details see Rocket Lake LP Platform Controller Hub EDS. | UP4<br>UP3 | No<br>No |
| **Click on Internal PCH Buses in the left tabs menu> DMI Configuration is expanded by default:** | | | |

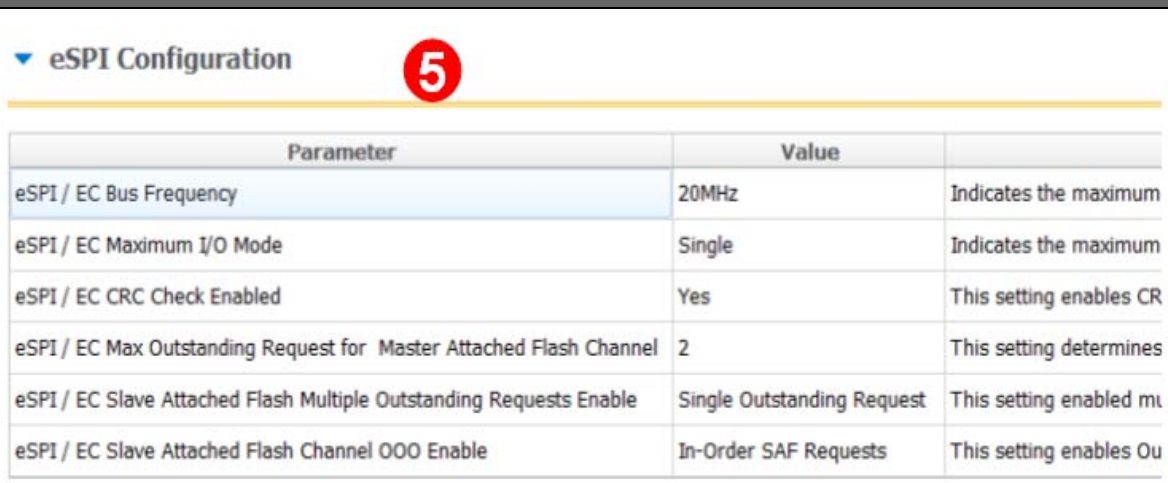



| # | Parameter | Platform | Settings |
|---|---|---|---|
| 3 | **DMI Configuration** | | |
| | **DMI Lane Reversal**<br>**Values: Yes/No** - This setting allows the DMI Lane signals to be reversed. For further details see Tiger Lake LP Platform Controller Hub EDS. | UP4<br>UP3 | No<br>No |
| | **DMI Port Staggering**<br>**Values: Yes/No** - This setting configures DMI for Port Staggering. For further details see Tiger Lake LP Platform Controller Hub EDS. | UP4<br>UP3 | Yes<br>Yes |
| **Click on Internal PCH Buses in the left tabs menu> OPI Configuration is expanded by default:** | | | |




| # | Parameter | Platform | Settings |
|---|---|---|---|
| 4 | **OPI / DMI Configuration** | | |
| | **OPI Link Speed**<br>**Values: GT2/GT4 -** This setting configures the OPI / DMI Link Speed. For further details see Tiger Lake PCH EDS. | UP4<br>UP3 | 2 GT/s<br>4 GT/s |
| | **OPI Link Voltage**<br>**Values: 0.85 Volts, 0.95 Volts, 1.05 Volts -** This setting configures the OPI / DMI Link Voltage. For further details see Tiger Lake PCH EDS. | UP4<br>UP3 | 0.95 Volts<br>0.95 Volts |
| | **OPI Link Width**<br>**Values: 1 Lanes, 2 Lanes, 4 Lanes, 8 Lanes -** This setting configures the OPI / DMI Link Width. For further details see Tiger Lake PCH EDS. | UP4<br>UP3 | 8 Lanes<br>8 Lanes |
| **Click on Internal PCH Buses in the left tabs menu> eSPI Configuration is expanded by default:** | | | |

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



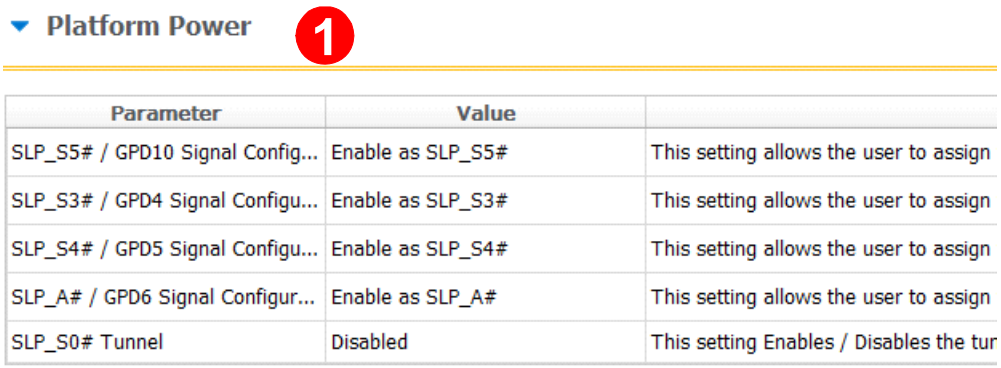
eSPI Configuration 5

| Parameter | Value | |
|---|---|---|
| eSPI / EC Bus Frequency | 20MHz | Indicates the maximum |
| eSPI / EC Maximum I/O Mode | Single | Indicates the maximum |
| eSPI / EC CRC Check Enabled | Yes | This setting enables CR |
| eSPI / EC Max Outstanding Request for Master Attached Flash Channel | 2 | This setting determines |
| eSPI / EC Slave Attached Flash Multiple Outstanding Requests Enable | Single Outstanding Request | This setting enabled mu |
| eSPI / EC Slave Attached Flash Channel OOO Enable | In-Order SAF Requests | This setting enables Ou |

| # | Parameter | Platform | Settings |
|---|---|---|---|
| 5 | **eSPI Configuration** | | |
| | **eSPI / EC Bus Frequency**<br>**Value: 20MHz, 25MHz, 33MHz, 50MHz**<br>Indicates the maximum frequency of the eSPI bus that is supported by the eSPI Master and platform configuration (trace length, number of Slaves, etc.). The actual frequency of the eSPI bus will be the minimum of this field and the Slave's maximum frequency advertised in its General Capabilities register. | UP4<br>UP3 | 20MHz<br>20MHz |
| | **eSPI / EC Maximum I/O Mode**<br>**Values: Single, Single and Dual, Single and Quad, Single Dual and Quad**<br>Indicates the maximum IO Mode (Single/Dual/Quad) of the eSPI bus that is supported by the eSPI Master and specific platform configuration. The actual IO Mode of the eSPI bus will be the minimum of this field and the Slave's maximum IO Mode advertised in its General Capabilities register. | UP4<br>UP3 | Single<br>Single |
| | **eSPI / EC CRC Check Enabled**<br>**Values: Yes/No**<br>This setting enables CRC checking on eSPI Slave 0 channel. | UP4<br>UP3 | No<br>No |
| | **eSPI / EC Max Outstanding Request for Master Attached Flash Channel**<br>**Values: 1/2**<br>This setting determines the Maximum outstanding requests on the eSPI / EC Master Attached Flash Channel. | UP4<br>UP3 | 2<br>2 |
| | **eSPI / EC Slave Attached Flash Multiple Outstanding Requests Enable**<br>**Values: Single Outstanding Request/Multiple Outstanding Requests**<br>This setting enabled multiple outstanding requests for the eSPI / EC Slave Attached Flash device. | UP4<br>UP3 | Single Outstanding Request<br>Single Outstanding Request |
| | **eSPI / EC Slave Attached Flash Channel OOO Enable**<br>**Values: In-Order SAF Requests/Out-of-Order SAF Requests**<br>This setting enables Out or Order requests on the eSPI / EC Slave Attached Flash device. | UP4<br>UP3 | In-Order SAF Requests<br>In-Order SAF Requests |

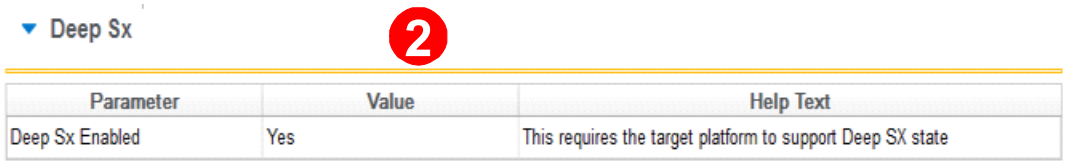
## Table 2-11. - Power (Sheet 1 of 2)

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




| # | Parameter | Platform | Settings |
|---|---|---|---|
| 1 | **Platform Power** | | |
| | **SLP_S3# / GPD4 Signal Configuration**<br>**Values: SLP_S3#, GPD4** - This setting allows the customer to assign the SLP_S3# Power Control signal as SLP_S3# or as GDP4. For further details see Tiger Lake LP Platform Controller Hub EDS. | UP4<br>UP3 | SLP_S3#<br>SLP_S3# |
| | **SLP_S4# / GPD5 Signal Configuration**<br>**Values: SLP_S4#, GPD5** - This setting allows the customer to assign the SLP_S4# Power Control signal as SLP_S4# or as GDP5. For further details see Tiger Lake LP Platform Controller Hub EDS. | UP4<br>UP3 | SLP_S4#<br>SLP_S4# |
| | **SLP_S5# / GPD10 Signal Configuration**<br>**Values: SLP_S5#, GPD10** - This setting allows the customer to assign the SLP_S5# Power Control signal as SLP_S5# or as GDP10. For further details see Tiger Lake LP Platform Controller Hub EDS. | UP4<br>UP3 | SLP_S5#<br>SLP_S5# |
| | **SLP_A# / GPD6 Signal Configuration**<br>**Values: SLP_A#, GPD6** - This setting allows the customer to assign the SLP_A# Power Control signal as SLP_A# or as GDP6. For further details see Tiger Lake LP Platform Controller Hub EDS. | UP4<br>UP3 | SLP_A#<br>SLP_A# |
| | **SLP_S0# Tunnel**<br>This setting Enables / Disables the tunneling of the SLP_S0# pin over ESPI to the EC when in ESPI mode. | UP4<br>UP3 | Disabled<br>Disabled |

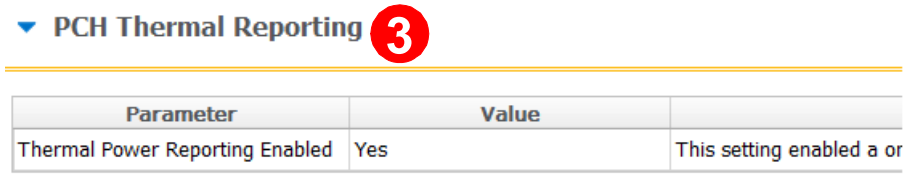
**Click on Power in the left tabs menu> Deep Sx is expanded by default:**




| # | Parameter | Platform | Settings |
|---|---|---|---|
| 2 | **Deep Sx** | | |
| | **Deep Sx Enabled**<br>**Values: Yes/ No -** This setting enables / disables support for Deep Sx operation. For further details see Tiger Lake LP Platform Controller Hub EDS. **Note:** Support for Deep Sx is board design dependent. | UP4<br>UP3 | Yes<br>Yes |

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

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



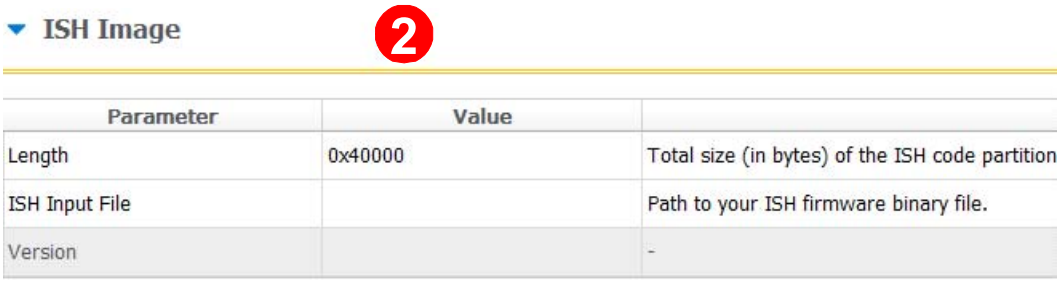

| # | Parameter | Platform | Settings |
|---|---|---|---|
| 3 | **PCH Thermal Reporting** | | |
| | **Thermal Power Reporting Enabled**<br>This setting enabled a once-per-second timer interrupt is enabled which triggers firmware to report power and temperature information as enabled by configuration registers. Note: When this setting is disabled ensure that the once-per-second timer interrupt associated with this feature is also disabled. | UP4<br>UP3 | Yes<br>Yes |

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

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

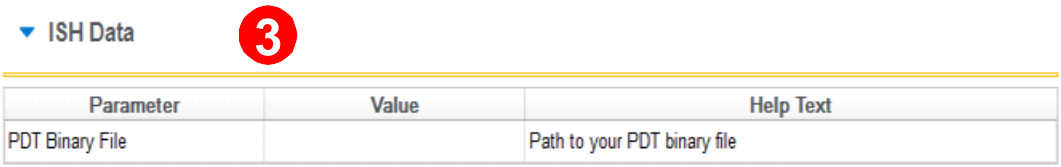
| # | Parameter | Platform | Settings |
|---|---|---|---|
| 1 | **Integrated Sensor Hub** | | |
| | **Integrated Sensor Hub Supported**<br>**Values: Yes / No**<br>This setting allows customers to disable ISH on the platform. | UP4<br>UP3 | No<br>No |
| | **Integrated Sensor Hub Power Up State**<br>**Values: Enabled / Disabled**<br>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. | UP4<br>UP3 | Disabled<br>Disabled |

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




| # | Parameter | Platform | Settings |
|---|---|---|---|
| 2 | **ISH Image** | | |
| | **Length** - Total size (in bytes) of the ISH code partition including reserved space. It is recommended to be at least 256kb. | | |
| | **Input File** | UP4<br>UP3 | ISH Binary (Optional) |
| | **Version** - This displays the version of ISH | | |

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



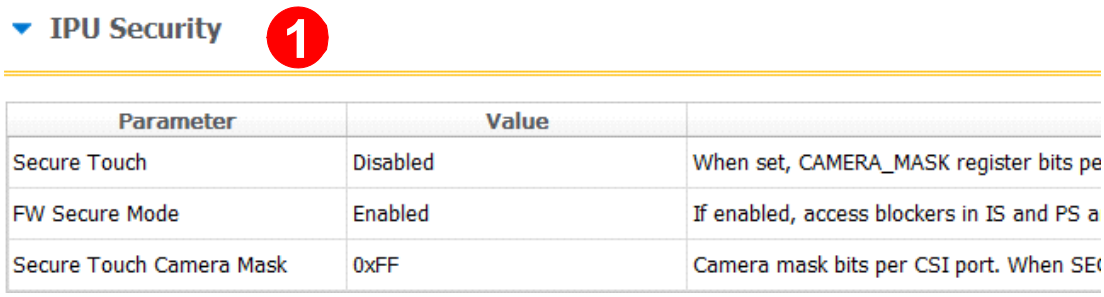

| # | Parameter | Platform | Settings |
|---|---|---|---|

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

| | | | |
|---|---|---|---|
| 3 | **Integrated Sensor Hub - ISH Data** | | |
| | **PDT Binary File** | UP4<br>UP3 | Path for PDT Binary file<br>Path for PDT Binary file |

## Table 2-13. - Camera

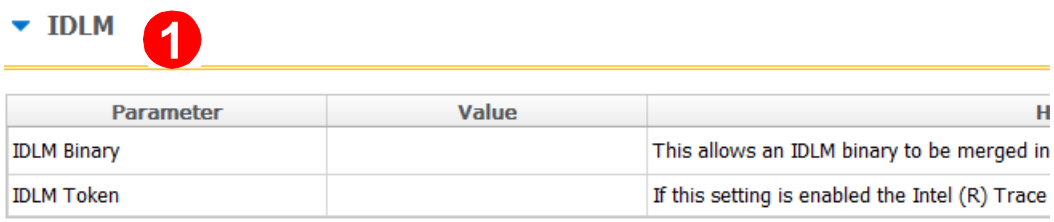
**Click on Camera in the left tabs menu> IPU Security is expanded by default:**




| # | Parameter | Platform | Settings |
|---|---|---|---|
| 1 | **IPU Security** | | |
| | **Secure Touch**<br>**Values: Enabled / Disabled**<br>When set, CAMERA_MASK register bits per CSI port are used to mask the data of cameras. When cleared, camera data is not masked. | UP4<br>UP3 | Disabled<br>Disabled |
| | **FW Secure Mode**<br>**Values: Enabled / Disabled**<br>If enabled, access blockers in IS and PS are enabled, and FW is read from IMR. Must be enabled for FW authentication flow and execution of authenticated FW. | UP4<br>UP3 | Enabled<br>Enabled |
| | **Secure Touch Camera Mask**<br>**Values: Hex Input**<br>Camera mask bits per CSI port. When SECURE_TOUCH is set each set bit masks a CSI port for secure touch. When SECURE_TOUCH is cleared this register has no impact on the CSI ports. | UP4<br>UP3 | 0xFF<br>0xFF |

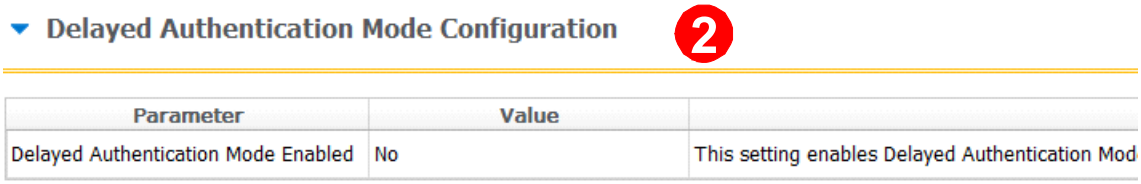
## Table 2-14. - Debug (Sheet 1 of 5)

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



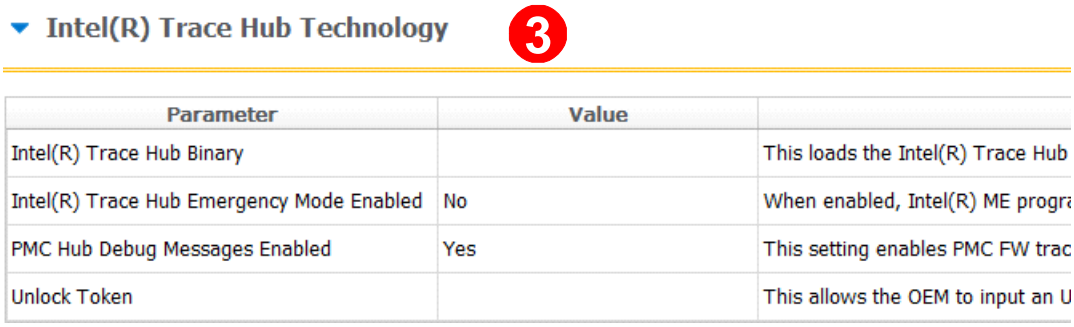

| # | Parameter | Platform | Settings |
|---|---|---|---|
| 1 | **IDLM** | | |
| | **IDLM Binary**<br>This allows an IDLM binary to be merged into output image built by Intel® FIT. | UP4<br>UP3 | IDLM Binary (Optional) |

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




| # | Parameter | Platform | Settings |
|---|---|---|---|
| 2 | **Delayed Authentication Mode Configuration** | | |
| | **Delayed Authentication Mode Enabled**<br>**Values: Yes / No** - This setting enable / disables Delayed Authentication Mode on the platform. | UP4<br>UP3 | No<br>No |

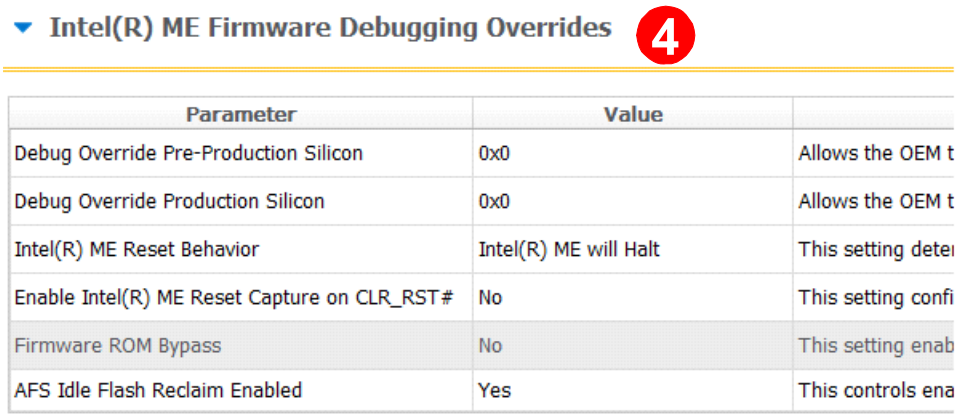
**Click on Debug in the left tabs menu> Intel® Trace Hub Technology is expanded by default:**




| # | Parameter | Platform | Settings |
|---|---|---|---|
| 3 | **Intel® Trace Hub Technology** | | |

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

| | | | |
|---|---|---|---|
| | **Intel® Trace Hub Binary -** This loads the Intel® Trace Hub binary that will be merged into the output image generated by the Intel® FIT tool. | UP4<br>UP3 | Trace Hub Binary<br>Trace Hub Binary |
| | **Intel® Trace Hub Emergency Mode Enabled**<br>**Values: Yes / No** - This setting enable / disables Intel® Trace Hub in the firmware base image. | UP4<br>UP3 | No<br>No |
| | **PMC Debug Messages Enabled**<br>**Values: Yes / No** - This setting enables/disables the PMC debug messages. | UP4<br>UP3 | Yes<br>Yes |
| | **Unlock Token**<br>This allows the OEM to input an Unlock Token binary file for closed chassis debug. | UP4<br>UP3 | Unlock Token Binary (Optional) |
| **Click on Debug in the left tabs menu> Intel® ME Debugging Overrides is expanded by default:** | | | |

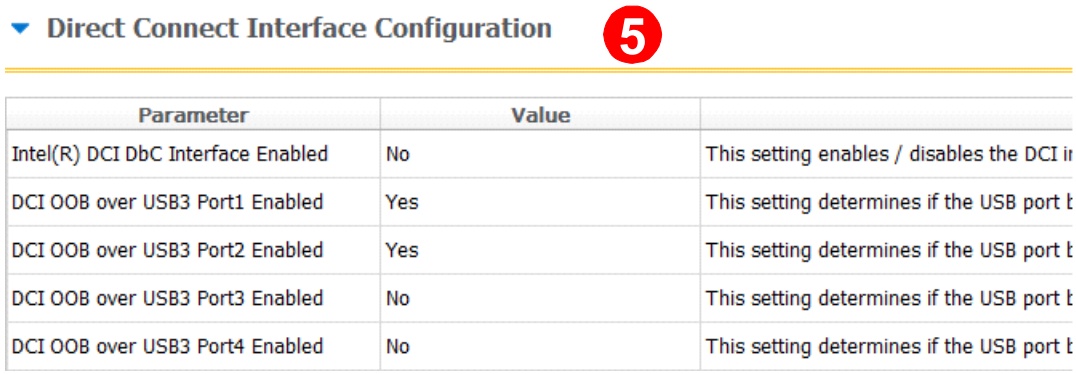



| # | Parameter | Platform | Settings |
|---|---|---|---|
| 4 | **Intel® ME Firmware Debugging Overrides** | | |
| | **Debug Override Pre-Production Silicon -** Allows the OEM to control FW features to assist with pre-production platform debugging. This control has no effect if used on production silicon.<br>**Bit 0:** Disable DRAM_INIT_DONE (default timeout 60 seconds)<br>**Bit 1:** Disable Host Reset Timer<br>**Bit 2:** Disable CPU_RESET_DONE timeout<br>**Bit 3:** Reserved<br>**Bit 4:** Disable Intel® ME Power Gating<br>**Bit 5:** Reserved<br>**Bit 6:** Secure Boot debug hook. Used to shorten wait time before ENF shutdown.<br>**Bit 7:** Force real FPFs on preproduction (default is to use flash)<br>**Bit 8:** Secure Boot debug hook. Used to reduce S3 or FFS optimization tries.<br>**Bit 9:** Reserved<br>**Bit 10:** Override power package to always enter M3.<br>**Note:** Certain options do not work when the descriptor is locked. | UP4<br>UP3 | 0x00000007<br>0x00000007 |
| | **Debug Override Production Silicon** - Allows the OEM to control FW features to assist with production platform debugging.<br>**Bit 0:** Extend DRAM_INIT_DONE timeout to 30 minutes (default timeout 15 seconds)<br>**Bit 1:** Disable Host Reset Timer<br>**Bit 2:** Disable CPU_RESET_DONE timeout<br>**Note:** Certain options do not work when the descriptor is locked. | UP4<br>UP3 | 0x00000000<br>0x00000000 |

## Table 2-14. - Debug (Sheet 3 of 5)

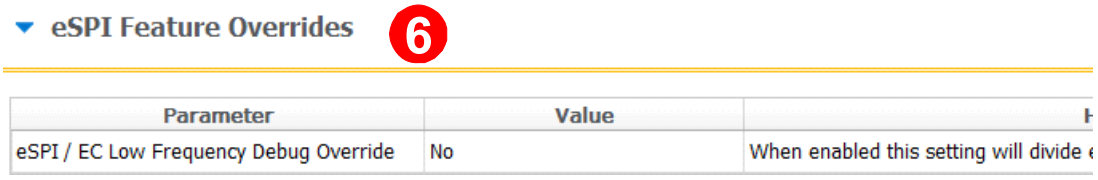
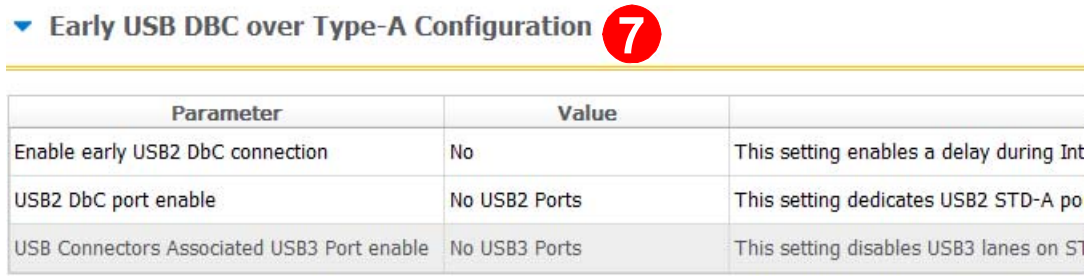
| | | | |
|---|---|---|---|
| | **Intel® ME Reset Behavior**<br>**Values: Intel® ME will Halt / Intel® Alternate image boot**<br>This setting determines Intel® ME behavior when boot image errors are encountered. Warning: This setting should be used for debug purposes only. Note: This may block normal Firmware functional flows. | UP4<br>UP3 | Intel® ME will Halt<br>Intel® ME will Halt |
| | **Enable Intel® ME Reset Capture on CLR_RST#** | UP4<br>UP3 | No<br>No |
| | **Firmware ROM Bypass**<br>**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. | UP4<br>UP3 | No<br>No |
| | **ASF Idle Flash Reclaim Enabled**<br>**Values: Yes / No**<br>This controls enabling / disable the Intel® AFS Idle flash reclaim capabilities.<br><br>***Note:*** This setting should be used for debug purposes only. | UP4<br>UP3 | Yes<br>Yes |

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

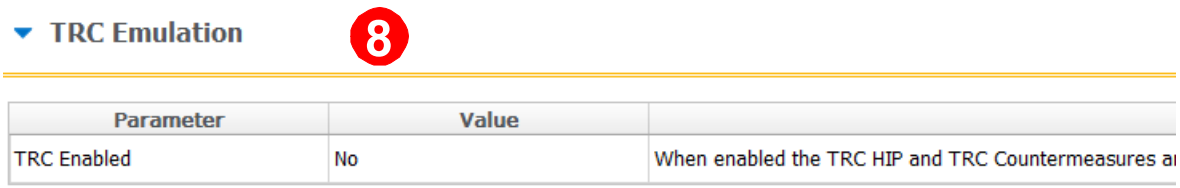



| # | Parameter | Platform | Settings |
|---|---|---|---|
| 5 | **Direct Connection Interface Configuration**<br><br>***Note:*** When any of the DCI BSSB USB3 Port interfaces are enabled the associated USB3 port selection control will be greyed out under the USB3 Port Configuration settings section under the Flex I/O tab | | |
| | **Intel® DCI DbC Interface Enabled**<br>**Values: Yes/No** - This setting enables / disables the Intel® DCI DbC interface. | UP4<br>UP3 | Yes<br>Yes |
| | **DCI OOB over USB3 Port1 Enabled**<br>**Values: Yes / No**<br>This setting determines if the USB port being enabled for DCI OOB. If disabled it will block DCI OOB connection.<br><br>***Note:*** When this setting is enabled the corresponding USB3 Combo Port in the Flex I/O Tab will be Grayed out. | UP4<br>UP3 | Yes<br>Yes |
| | **DCI OOB over USB3 Port 2 Enabled**<br>**Values: Yes / No**<br>This setting determines if the USB port being enabled for DCI OOB. If disabled it will block DCI OOB connection.<br><br>***Note:*** When this setting is enabled the corresponding USB3 Combo Port in the Flex I/O Tab will be Grayed out. | UP4<br>UP3 | Yes<br>Yes |

## Table 2-14. - Debug (Sheet 4 of 5)

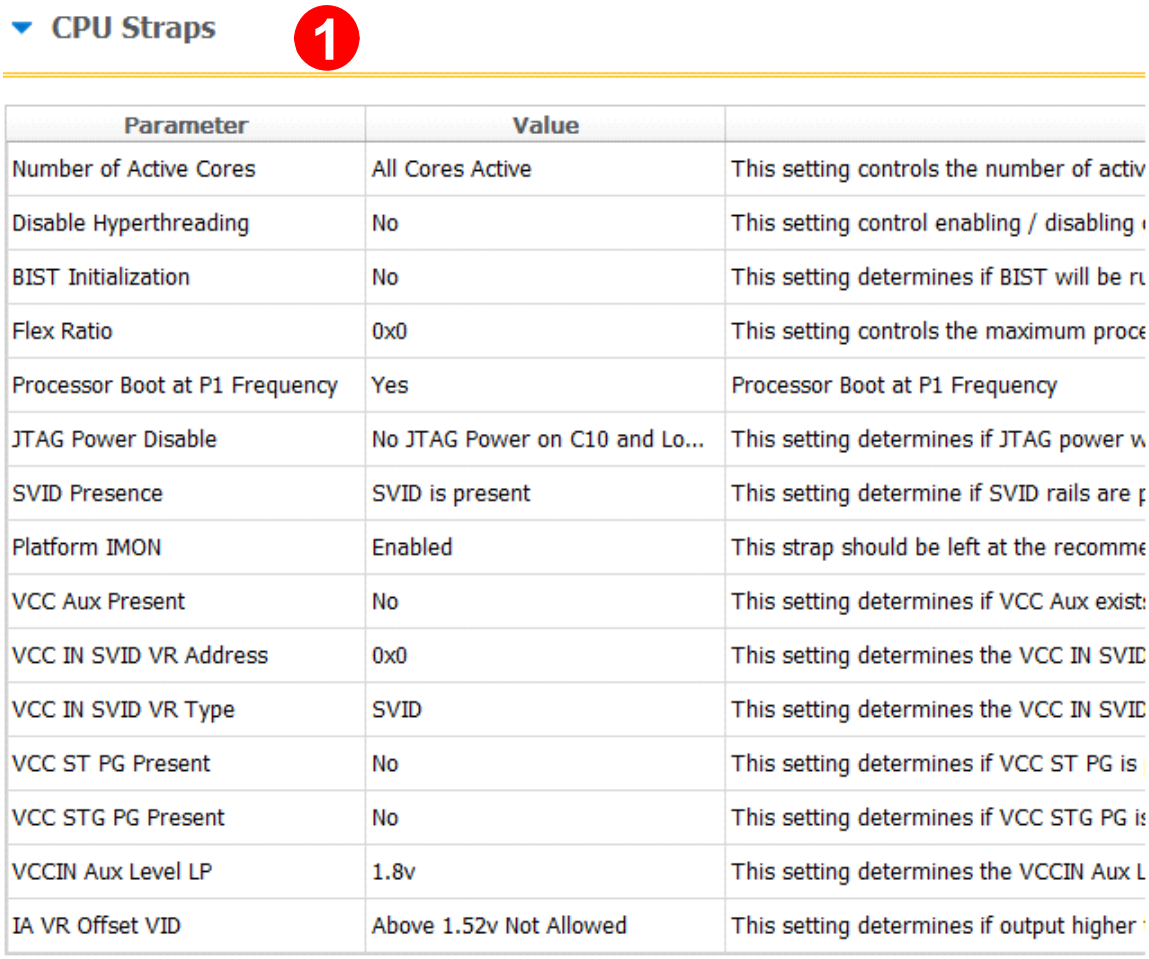
| | | | |
|---|---|---|---|
| | **DCI OOB over USB3 Port 3 Enabled**<br>**Values: Yes / No**<br>This setting determines if the USB port being enabled for DCI OOB. If disabled it will block DCI OOB connection.<br><br>***Note:*** When this setting is enabled the corresponding USB3 Combo Port in the Flex I/O Tab will be Grayed out. | UP4<br>UP3 | No<br>No |
| | **DCI OOB over USB3 Port 4 Enabled**<br>**Values: Yes / No**<br>This setting determines if the USB port being enabled for DCI OOB. If disabled it will block DCI OOB connection.<br><br>***Note:*** When this setting is enabled the corresponding USB3 Combo Port in the Flex I/O Tab will be Grayed out. | UP4<br>UP3 | No<br>No |
| **Click on Debug in the left tabs menu> eSPI Feature Overrides is expanded by default:** | | | |
|  | | | |
| **#** | **Parameter** | **Platform** | **Settings** |
| 6 | **eSPI Feature Overrides** | | |
| | **eSPI / EC Low Frequency Debug Override**<br>When enabled this setting will divide eSPI clock frequency by 8.<br><br>***Note:*** This setting should only be used for debugging purposes. Leaving this set to "Yes" will impact eSPI performance on the platform. | UP4<br>UP3 | No<br>No |
| **Click on Debug in the left tabs menu> Early USB DBC Type-A Configuration is expanded by default:** | | | |
|  | | | |
| **#** | **Parameter** | **Platform** | **Settings** |
| 7 | **Early USB DBC Type-A Configuration** | | |
| | **Enabled early USB2 DbC connection**<br>**Values: Yes / No**<br>This setting enabled a delay during Intel® ME firmware bring-up to allow USB2 DbC connection to be established | UP4<br>UP3 | No<br>No |
| | **USB2 DbC port enable**<br>This setting determines which USB2 ports are enabled for Early DbC debugging. | UP4<br>UP3 | No USB2 Ports<br>No USB2 Ports |

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

| | | | |
|---|---|---|---|
| | **USB Connectors associated USB3 Port enable**<br>This setting determines which USB3 ports goes to the target USB2 ports connector for Early DbC debugging. | UP4<br>UP3 | No USB3 Ports<br>No USB3 Ports |
| **Click on Debug in the left tabs menu> Early TRC Emulation is expanded by default:** | | | |
|  | | | |
| **#** | **Parameter** | **Platform** | **Settings** |
| 8 | **TRC Emulation** | | |
| | **TRC Enabled**<br>**Values: Yes / No**<br>This setting enables TRC HIP and TRC Countermeasures used by Intel® CSME for the detection of hardware glitches as a part of security hardening. The purpose of this setting is to allow OEMs to enable TRC for testing prior to close of manufacturing and FPF commit. | UP4<br>UP3 | No<br>No |
| | **TRC Enabled (FPF)**<br>**Values: Yes / No**<br>When enabled the TRC HIP and TRC Countermeasures are enabled. When manufacture is completed, this value is burned into an FPF.<br><br>***Note:*** This setting should be set to "Yes" for production platforms. | UP4<br>UP3 | No<br>No |

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

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



CPU Straps 1

| Parameter | Value | |
|---|---|---|
| Number of Active Cores | All Cores Active | This setting controls the number of activ |
| Disable Hyperthreading | No | This setting control enabling / disabling |
| BIST Initialization | No | This setting determines if BIST will be ru |
| Flex Ratio | 0x0 | This setting controls the maximum proce |
| Processor Boot at P1 Frequency | Yes | Processor Boot at P1 Frequency |
| JTAG Power Disable | No JTAG Power on C10 and Lo... | This setting determines if JTAG power w |
| SVID Presence | SVID is present | This setting determine if SVID rails are p |
| Platform IMON | Enabled | This strap should be left at the recomme |
| VCC Aux Present | No | This setting determines if VCC Aux exist: |
| VCC IN SVID VR Address | 0x0 | This setting determines the VCC IN SVID |
| VCC IN SVID VR Type | SVID | This setting determines the VCC IN SVID |
| VCC ST PG Present | No | This setting determines if VCC ST PG is |
| VCC STG PG Present | No | This setting determines if VCC STG PG is |
| VCCIN Aux Level LP | 1.8v | This setting determines the VCCIN Aux L |
| IA VR Offset VID | Above 1.52v Not Allowed | This setting determines if output higher |

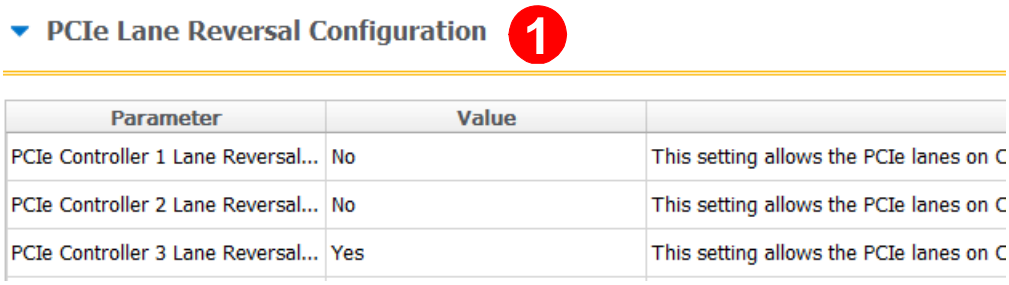
| # | Parameter | Platform | Settings |
|---|---|---|---|
| 1 | **CPU Straps - CPU Straps** | | |
| | **Number of Active Cores**<br>**Values: All, 1, 2, 3, 4, 5, 6, 7, 8**<br>This setting controls the number of active processor cores.<br>***Note:*** This strap is intended for debugging purposes only. See BIOS Spec for more details on enabling or disabling processor cores. | UP4<br>UP3 | All Cores Active<br>All Cores Active |
| | **Disable Hyperthreading**<br>**Values: Yes / No**<br>This setting controls enabling or disabling of Hyper threading.<br>***Note:*** This strap is intended for debugging purposes only. See BIOS Spec for more details on enabling / disabling Hyperthreading. | UP4<br>UP3 | No<br>No |

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

| | | | |
|---|---|---|---|
| | **BIST Initialization**<br>**Values: Yes/No**<br>This setting determines if BIST will be run at platform reset after BIOS requested actions.<br>***Note:*** This strap is intended for debugging purposes only. | UP4<br>UP3 | No<br>No |
| | **Flex Ratio**<br>This setting controls the maximum processor non-turbo ratio.<br>***Note:*** This strap is intended for debugging purposes only. See BIOS Spec for more details on maximum processor non-turbo ratio configuration. | UP4<br>UP3 | 0x0<br>0x0 |
| | **Processor Boot at P1 Frequency**<br>**Values: Yes/No**<br>This setting determines if the processor will operate at maximum frequency at power-on and boot.<br>***Note:*** This strap is intended for debugging purposes only. | UP4<br>UP3 | Yes<br>Yes |
| | **JTAG Power Disable**<br>**Values: Yes - JTAG Power on C10 and Lower/No - No Power on C10 and Lower**<br>This setting determines if JTAG power will be maintained on C10 or lower power states.<br>***Note:*** This strap is intended for debugging purposes only. | UP4<br>UP3 | No JTAG Power on C10 and Lower<br>No JTAG Power on C10 and Lower |
| | **SVID Presence**<br>**Value: SVID Present/SVID Not Present**<br>This setting determines if SVID rails are present on the platform. See Processor EDS for details. | UP4<br>UP3 | SVID Present<br>SVID Present |
| | **Platform IMON**<br>**Value: Enabled/Disabled**<br>***Note:*** This strap should be left at the recommended default setting. | UP4<br>UP3 | Enabled<br>Enabled |
| | **VCC Aux Present**<br>**Value: Yes/No**<br>This setting determines if VCC Aux exists as a separate VR. | UP4<br>UP3 | Yes<br>Yes |
| | **VCCIN SVID Address**<br>This setting determines the VCCIN SVID Address. See Processor EDS for details.<br>**Note:** This strap should be left at the recommended default setting. | UP4<br>UP3 | 0x0<br>0x0 |
| | **VCC SVID VR Type**<br>**Values: SVID/Fixed VR**<br>This setting determines the VCC IN SVID VR Type. See Processor EDS for details. | UP4<br>UP3 | SVID<br>SVID |
| | **VCC ST PG Present**<br>**Values: Yes/No**<br>This setting determines if VCC ST PG is present on the platform. | UP4<br>UP3 | No<br>No |
| | **VCC STG PG Present**<br>**Values: Yes/No**<br>This setting determines if VCC STG PG is present on the platform. | UP4<br>UP3 | No<br>No |
| | **VCCIN Aux Level LP**<br>**Values: 1.8v/1.65v**<br>This setting determines the VCCIN Aux Level LP Voltage.<br>***Note:*** On UP4 based MCP this setting can be configured to 1.65v. On the UP3 MCP types set to 1.8v | UP4<br>UP3 | 1.65v or 1.8v<br>1.8v |
| | **IA VR Offset VID**<br>**Values: Above 1.52v Not Allowed/Above 1.52v Allowed**<br>This setting determines if output higher than 1.52v is allowed for 8 or higher core count processors. | UP4<br>UP3 | Above 1.52v Not Allowed<br>Above 1.52v Not Allowed |

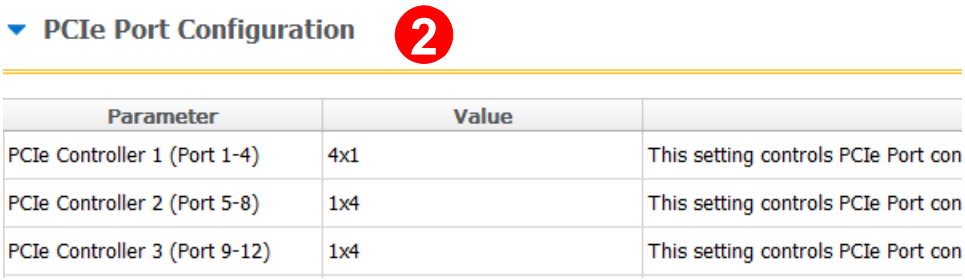
## Table 2-16. - Flex I/O Straps (Sheet 1 of 15)

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




| # | Parameter | Platform | Settings |
|---|---|---|---|
| 1 | **PCIe Lane Reversal Configuration** | | |
| | **PCIe Controller 1 Lane Reversal Enabled**<br>**Values: Yes/ No** - This setting allows the PCIe lanes on Controller 1 to be reversed. **Note:** Refer to EDS for PCIe supported port configurations. | UP4<br>UP3 | No<br>No |
| | **PCIe Controller 2 Lane Reversal Enabled**<br>**Values: Yes/ No** - This setting allows the PCIe lanes on Controller 2 to be reversed. **Note:** Refer to EDS for PCIe supported port configurations. | UP4<br>UP3 | No<br>No |
| | **PCIe Controller 3 Lane Reversal Enabled**<br>**Values: Yes/ No** - This setting allows the PCIe lanes on Controller 3 to be reversed. **Note:** Refer to EDS for PCIe supported port configurations. | UP4<br>UP3 | Yes<br>Yes |

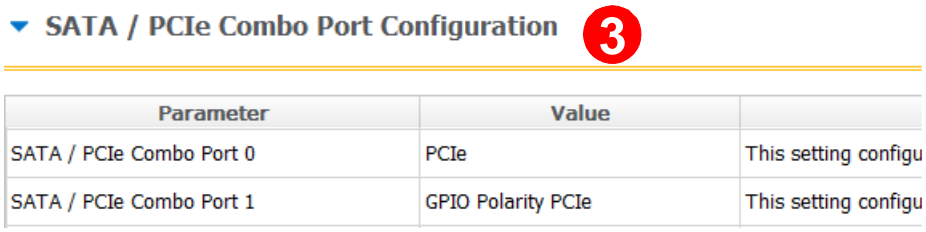
**Click on Flex I/O in the left tabs menu> PCIe Port Configuration is expanded by default:**




| # | Parameter | Platform | Settings |
|---|---|---|---|
| 2 | **PCIe Port Configuration** | | |
| | **PCIe Controller 1 (Port 1-4)**<br>**Values: 4x1, (1x2, 2x1), 2x2, 1x4** - This setting controls PCIe Port configurations for PCIe Controller 1. For further details see Tiger Lake LP Platform Controller Hub EDS. | UP4<br>UP3 | 4x1<br>4x1 |
| | **PCIe Controller 2 (Port 5-8)**<br>**Values: 4x1, (1x2, 2x1), 2x2, 1x4** - This setting controls PCIe Port configurations for PCIe Controller 2. For further details see Tiger Lake LP Platform Controller Hub EDS.<br><br>***Note:*** On UP4 only lanes 7 and 8 are available for use. | UP4<br>UP3 | 4x1<br>1x2, 2x1 |

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

| | | | |
|---|---|---|---|
| | **PCIe Controller 3 (Port 9-12)**<br>**Values: 4x1, (1x2, 2x1), 2x2, 1x4** - This setting controls PCIe Port configurations for PCIe Controller 3. For further details see Tiger Lake LP Platform Controller Hub EDS. | UP4<br>UP3 | 1x4<br>1x4 |
| **Click on Flex I/O in the left tabs menu> SATA / PCIe Combo Port Configuration is expanded by default:** | | | |




| # | Parameter | Platform | Settings |
|---|---|---|---|
| 3 | **SATA / PCIe Combo Port Configuration** | | |
| | **SATA / PCIe Combo Port 0**<br>**Values: SATA, PCIe, GPIO Polarity PCIe, GPIO Polarity SATA** - This setting configures the PCIe port to operate as either:<br>PCIe Port 11 or SATA Port 0<br>For further details on Flex I/O see Tiger Lake LP Platform Controller Hub EDS. | UP4<br>UP3 | PCIe<br>PCIe |
| | **SATA / PCIe Combo Port 1**<br>**Values: SATA, PCIe, GPIO Polarity PCIe, GPIO Polarity SATA** - This setting configures the PCIe port to operate as either:<br>PCIe Port 12 or SATA Port 1<br>For further details on Flex I/O see Tiger Lake LP Platform Controller Hub EDS. | UP4<br>UP3 | GPIO Polarity PCIe<br>GPIO Polarity PCIe |
| **Click on Flex I/O in the left tabs menu> USB3 Port Configuration is expanded by default:** | | | |

## Table 2-16. - Flex I/O Straps (Sheet 3 of 15)

### USB3 Port Configuration 4

| Parameter | Value | H |
|---|---|---|
| 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 / PCIe Combo Port 3 | USB3 | This setting configures the PCIe port to opera |
| USB3 Port 1 Connector Type Se... | Type A | This setting configures the physical connecto |
| USB3 Port 2 Connector Type Se... | Type A | This setting configures the physical connecto |
| USB3 Port 3 Connector Type Se... | Type C | This setting configures the physical connecto |
| USB3 Port 4 Connector Type Se... | Type C | This setting configures the physical connecto |
| USB3 Port 1 Initialization Speed... | USB3.1 Gen1 LBPM | This setting determines USB3 Port 1 speed d |
| USB3 Port 2 Initialization Speed... | USB3.1 Gen1 LBPM | This setting determines USB3 Port 2 speed d |
| USB3 Port 3 Initialization Speed... | USB3.1 Gen1 LBPM | This setting determines USB3 Port 3 speed d |
| USB3 Port 4 Initialization Speed... | USB3.1 Gen1 LBPM | This setting determines USB3 Port 4 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 Gen2 | 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 |
| USB Type AB Mode Select | USB Type AB HW Select | This setting determines how the USB Type A |

| # | Parameter | Platform | Settings |
|---|---|---|---|
| 4 | **USB3 Port Configuration** | | |
| | **USB3 / PCIe Combo Port 0**<br>**Values: PCIe (or GbE), USB3 -** This setting configures the PCIe port to operate as either:<br>PCIe Port 1 or USB3 Port 1<br>For further details on Flex I/O see Tiger Lake LP Platform Controller Hub EDS.<br><br>***Note:*** If DCI BSSB for this USB3 Combo port it will be Grayed out. | UP4<br>UP3 | USB3<br>USB3 |

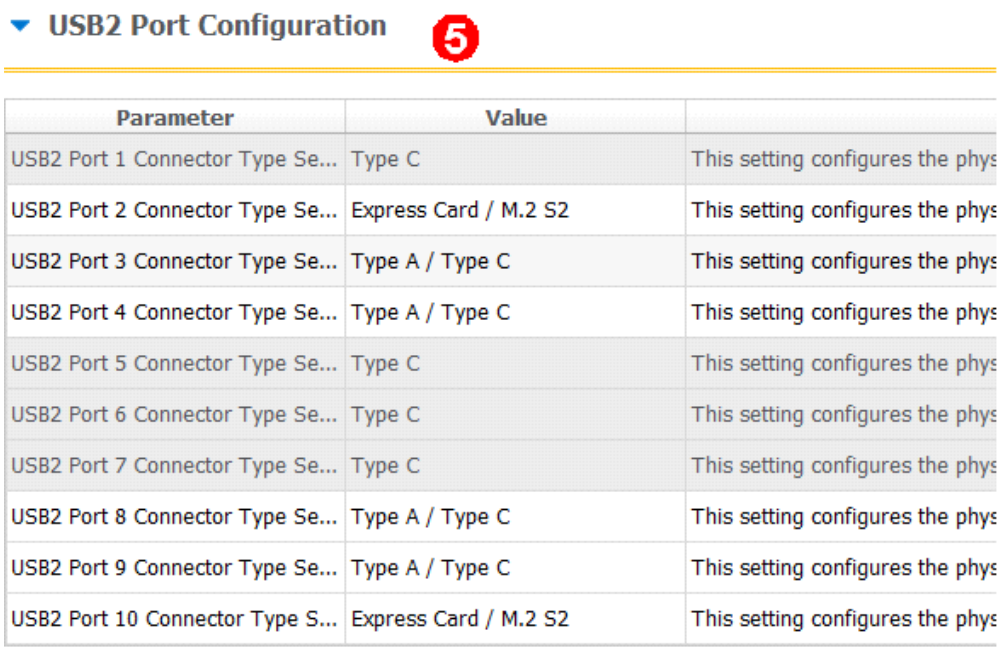
## Table 2-16. - Flex I/O Straps (Sheet 4 of 15)

| | | | |
|---|---|---|---|
| | **USB3 / PCIe Combo Port 1**<br>**Values: PCIe (or GbE), USB3 -** This setting configures the PCIe port to operate as either:<br>PCIe Port 2 or USB3 Port 2<br>For further details on Flex I/O see Tiger Lake LP Platform Controller Hub EDS.<br><br>***Note:*** If DCI BSSB for this USB3 Combo port it will be Grayed out. | UP4<br>UP3 | USB3<br>USB3 |
| | **USB3 / PCIe Combo Port 2**<br>**Values: PCIe (or GbE), USB3** - This setting configures the PCIe port to operate as either:<br>PCIe Port 3 or USB3 Port 3<br>For further details on Flex I/O see Tiger Lake LP Platform Controller Hub EDS.<br><br>***Note:*** If DCI BSSB for this USB3 Combo port it will be Grayed out. | UP4<br>UP3 | PCIe<br>PCIe |
| | **USB3 / PCIe Combo Port 3**<br>**Values: PCIe (or GbE), USB3** - This setting configures the PCIe port to operate as either:<br>PCIe 4 or USB3 Port 4<br>For further details on Flex I/O see Tiger Lake LP Platform Controller Hub EDS.<br><br>***Note:*** If DCI BSSB for this USB3 Combo port it will be Grayed out. | UP4<br>UP3 | PCIe<br>PCIe |
| | **USB3 Port 1 Connector Type Select**<br>This setting configures the physical connector type to be used for USB 3.0 / 3.1 Port 1. | UP4<br>UP3 | Type-A<br>Type-A |
| | **USB3 Port 2 Connector Type Select**<br>This setting configures the physical connector type to be used for USB 3.0 / 3.1 Port 2. | UP4<br>UP3 | Type-A<br>Type-A |
| | **USB3 Port 3 Connector Type Select**<br>This setting configures the physical connector type to be used for USB 3.0 / 3.1 Port 3. | UP4<br>UP3 | Type-C<br>Type-C |
| | **USB3 Port 4 Connector Type Select**<br>This setting configures the physical connector type to be used for USB 3.0 / 3.1 Port 4. | UP4<br>UP3 | Type-C<br>Type-C |
| | **USB3 Port 1 Initialization Speed Select**<br>This setting determines USB3 Port 1 speed during platform power-up. | UP4<br>UP3 | USB3.1 Gen1 LBPM<br>USB3.1 Gen1 LBPM |
| | **USB3 Port 2 Initialization Speed Select**<br>This setting determines USB3 Port 2 speed during platform power-up. | UP4<br>UP3 | USB3.1 Gen1 LBPM<br>USB3.1 Gen1 LBPM |
| | **USB3 Port 3 Initialization Speed Select**<br>This setting determines USB3 Port 3 speed during platform power-up. | UP4<br>UP3 | USB3.1 Gen1 LBPM<br>USB3.1 Gen1 LBPM |
| | **USB3 Port 4 Initialization Speed Select**<br>This setting determines USB3 Port 4 speed during platform power-up. | UP4<br>UP3 | USB3.1 Gen1 LBPM<br>USB3.1 Gen1 LBPM |
| | **USB3 Port 1 Speed Capability**<br>This setting determines the USB3 Port 1 speed capabilities.<br><br>***Note:*** When a USB 3.2 Gen 2x1 (10 Gb/s) capable port is configured to USB 3.2 Gen 1x1 (5 Gb/s) speed using the soft strap, the port may still send 10 Gb/s compliance patterns if the USB compliance test (TD1.4, and TD1.7) is run on the port. | UP4<br>UP3 | USB 3.1 Gen2<br>USB 3.1 Gen2 |
| | **USB3 Port 2 Speed Capability**<br>This setting determines the USB3 Port 2 speed capabilities.<br><br>***Note:*** When a USB 3.2 Gen 2x1 (10 Gb/s) capable port is configured to USB 3.2 Gen 1x1 (5 Gb/s) speed using the soft strap, the port may still send 10 Gb/s compliance patterns if the USB compliance test (TD1.4, and TD1.7) is run on the port. | UP4<br>UP3 | USB 3.1 Gen2<br>USB 3.1 Gen2 |

## Table 2-16. - Flex I/O Straps (Sheet 5 of 15)

| | | | |
|---|---|---|---|
| | **USB3 Port 3 Speed Capability**<br>This setting determines the USB3 Port 3 speed capabilities.<br><br>***Note:*** When a USB 3.2 Gen 2x1 (10 Gb/s) capable port is configured to USB 3.2 Gen 1x1 (5 Gb/s) speed using the soft strap, the port may still send 10 Gb/s compliance patterns if the USB compliance test (TD1.4, and TD1.7) is run on the port. | UP4<br>UP3 | USB 3.1 Gen2<br>USB 3.1 Gen2 |
| | **USB3 Port 4 Speed Capability**<br>This setting determines the USB3 Port 4 speed capabilities.<br><br>***Note:*** When a USB 3.2 Gen 2x1 (10 Gb/s) capable port is configured to USB 3.2 Gen 1x1 (5 Gb/s) speed using the soft strap, the port may still send 10 Gb/s compliance patterns if the USB compliance test (TD1.4, and TD1.7) is run on the port. | UP4<br>UP3 | USB 3.1 Gen2<br>USB 3.1 Gen2 |
| | **USB Type AB Mode Select**<br>This setting determines how the USB Type AB connector switching is handled. | UP4<br>UP3 | USB Type AB SW Select<br>USB Type AB SW Select |

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




| # | Parameter | Platform | Settings |
|---|---|---|---|
| 5 | **Flex I/O - USB2 Port Configuration** | | |
| | **USB2 Port 1 Connector Type Select**<br>This setting configures the physical connector type to be used for USB2 Port 1. | UP4<br>UP3 | Type-C<br>Type-C |
| | **USB2 Port 2 Connector Type Select**<br>This setting configures the physical connector type to be used for USB2 Port 2. | UP4<br>UP3 | Type A / Type C<br>Express Card / M.2 S2 |
| | **USB2 Port 3 Connector Type Select**<br>This setting configures the physical connector type to be used for USB2 Port 3. | UP4<br>UP3 | Type A / Type C<br>Type A / Type C |
| | **USB2 Port 4 Connector Type Select**<br>This setting configures the physical connector type to be used for USB2 Port 4. | UP4<br>UP3 | Type A / Type C<br>Type A / Type C |

## Table 2-16. - Flex I/O Straps (Sheet 6 of 15)

| | | | |
|---|---|---|---|
| | **USB2 Port 5 Connector Type Select**<br>This setting configures the physical connector type to be used for USB2 Port 5. | UP4<br>UP3 | Type-C<br>Type-C |
| | **USB2 Port 6 Connector Type Select**<br>This setting configures the physical connector type to be used for USB2 Port 6. | UP4<br>UP3 | Type-C<br>Type-C |
| | **USB2 Port 7 Connector Type Select**<br>This setting configures the physical connector type to be used for USB2 Port 7. | UP4<br>UP3 | Type A / Type C<br>Type-C |
| | **USB2 Port 8 Connector Type Select**<br>This setting configures the physical connector type to be used for USB2 Port 8. | UP4<br>UP3 | Type A / Type C<br>Type A / Type C |
| | **USB2 Port 9 Connector Type Select**<br>This setting configures the physical connector type to be used for USB2 Port 9. | UP4<br>UP3 | Type A / Type C<br>Type A / Type C |
| | **USB2 Port 10 Connector Type Select**<br>This setting configures the physical connector type to be used for USB2 Port 10. | UP4<br>UP3 | Express Card / M.2 S2<br>Express Card / M.2 S2 |
| **Click on Flex I/O in the left tabs menu> Type-C Subsystem Configuration is expanded by default:** | | | |

## Table 2-16. - Flex I/O Straps (Sheet 7 of 15)

### Type-C Subsystem Configuration 6

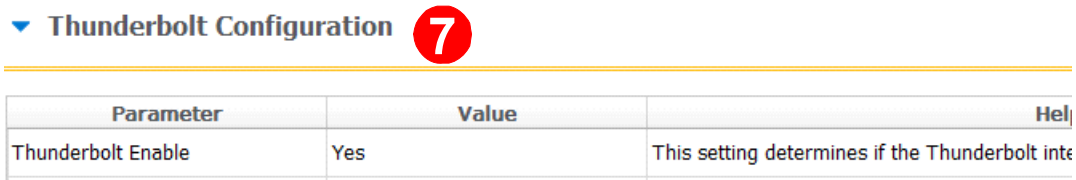
| Parameter | Value | |
|---|---|---|
| IO Manageability Engine Binary File | | This loads the Type-C Subsystem IO Manageability Engine |
| IO Manageability Engine Enabled | Yes | This setting enables\ disables the Type-C Subsystem IO M |
| IO Manageability Engine Length | 0x12000 | Set the length of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

## Table 2-16. - Flex I/O Straps (Sheet 8 of 15)

| # | Parameter | Platform | Settings |
|---|---|---|---|
| 6 | **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. | UP4<br>UP3 | IOM Binary<br>IOM Binary |
| | **IO Manageability Engine Enabled**<br>**Values: Yes/No**<br>This setting enables / disables the Type-C Subsystem IO Manageability Engine on the platform. | UP4<br>UP3 | Yes<br>Yes |
| | **IO Manageability Engine Length -** This displays the length of the IO Manageability binary.<br>***Note:*** This value will be automatically populated by Intel® FIT during image build. | | |
| | **IO Manageability Engine Version** - This displays the version of IO Manageability binary. | | |
| | **PHY Binary File -** This loads the MG PHY binary that will be merged into the output image generated by the Intel® FIT. | UP4<br>UP3 | PHY Binary<br>PHY Binary |
| | **PHY Manifest Enabled**<br>**Values: Yes/No**<br>This setting enables / disables the NPHY on the platform. | UP4<br>UP3 | Yes<br>Yes |
| | **PHY Length -** This displays the length of the PHY binary.<br>***Note:*** This value will be automatically populated by Intel® FIT during image build. | | |
| | **PHY Version** - This displays the version of PHY binary. | | |
| | **Thunderbolt(TM)/USB4(TM) Binary File**<br>**Values: Yes/No**<br>This setting enables Anti-Roll back for the Type-C Subsystem Thunderbolt(TM)/USB4(TM) binary. | UP4<br>UP3 | TBT Binary<br>TBT Binary |
| | **Thunderbolt(TM)/USB4(TM) Length -** This displays the length of the Thunderbolt(TM)/USB4(TM) binary.<br>***Note:*** This value will be automatically populated by Intel® FIT during image build. | | |
| | **Thunderbolt(TM)/USB4(TM) Version** - This displays the version of Thunderbolt(TM)/USB4(TM) binary. | | |
| | **Tcss - Partial Update Enabled**<br>**Values: Enabled/Disabled**<br>This setting enabled partial firmware update of the TCSS partitions. | UP4<br>UP3 | Disabled<br>Disabled |
| | **Type-C Subsystem Port Enable Mask**<br>This setting determines the Type-C Subsystem Port Enable Mask | UP4<br>UP3 | 0xF<br>0xF |
| | **Type-C Subsystem Authentication Enabled**<br>**Values: Yes/No**<br>This setting enables / disables firmware authentication for the Type-C Subsystem on power-up. | UP4<br>UP3 | Yes<br>Yes |
| | **Type-C Port 1 Configuration**<br>**Value: No Restrictions/DP Fixed Connection/No Thunderbolt**<br>This setting determines the configuration for Type-C Port 1 | UP4<br>UP3 | No Restrictions<br>No Restrictions |
| | **Type-C Port 2 Configuration**<br>**Value: No Restrictions/DP Fixed Connection/No Thunderbolt**<br>This setting determines the configuration for Type-C Port 2 | UP4<br>UP3 | No Restrictions<br>No Restrictions |
| | **Type-C Port 3 Configuration**<br>**Value: No Restrictions/DP Fixed Connection/No Thunderbolt**<br>This setting determines the configuration for Type-C Port 3 | UP4<br>UP3 | No Restrictions<br>No Restrictions |
| | **Type-C Port 4 Configuration**<br>**Value: No Restrictions/DP Fixed Connection/No Thunderbolt**<br>This setting determines the configuration for Type-C Port 4 | UP4<br>UP3 | No Restrictions<br>No Restrictions |

## Table 2-16. - Flex I/O Straps (Sheet 9 of 15)

| | | | |
|---|---|---|---|
| | **Type-C Port 1 Speed Capability**<br>**Values: USB 3.1 Gen2/USB 3.1 Gen1**<br>This setting determines the Type-C Port 1 speed capability | UP4<br>UP3 | USB 3.1 Gen2<br>USB 3.1 Gen2 |
| | **Type-C Port 2 Speed Capability**<br>**Values: USB 3.1 Gen2/USB 3.1 Gen1**<br>This setting determines the Type-C Port 2 speed capability | UP4<br>UP3 | USB 3.1 Gen2<br>USB 3.1 Gen2 |
| | **Type-C Port 3 Speed Capability**<br>**Values: USB 3.1 Gen2/USB 3.1 Gen1**<br>This setting determines the Type-C Port 3 speed capability | UP4<br>UP3 | USB 3.1 Gen2<br>USB 3.1 Gen2 |
| | **Type-C Port 4 Speed Capability**<br>**Values: USB 3.1 Gen2/USB 3.1 Gen1**<br>This setting determines the Type-C Port 4 speed capability | UP4<br>UP3 | USB 3.1 Gen2<br>USB 3.1 Gen2 |
| | **Type-C Port 1 Initialization Speed Select**<br>**Values: USB3.1 Gen1 LBPM/USB3.1 Gen2 skip LBPM**<br>This setting determines Type-C Port 1 speed during platform power-up. | UP4<br>UP3 | USB3.1 Gen1 LBPM<br>USB3.1 Gen1 LBPM |
| | **Type-C Port 2 Initialization Speed Select**<br>**Values: USB3.1 Gen1 LBPM/USB3.1 Gen2 skip LBPM**<br>This setting determines Type-C Port 2 speed during platform power-up. | UP4<br>UP3 | USB3.1 Gen1 LBPM<br>USB3.1 Gen1 LBPM |
| | **Type-C Port 3 Initialization Speed Select**<br>**Values: USB3.1 Gen1 LBPM/USB3.1 Gen2 skip LBPM**<br>This setting determines Type-C Port 3 speed during platform power-up. | UP4<br>UP3 | USB3.1 Gen1 LBPM<br>USB3.1 Gen1 LBPM |
| | **Type-C Port 4 Initialization Speed Select**<br>**Values: USB3.1 Gen1 LBPM/USB3.1 Gen2 skip LBPM**<br>This setting determines Type-C Port 4 speed during platform power-up. | UP4<br>UP3 | USB3.1 Gen1 LBPM<br>USB3.1 Gen1 LBPM |
| | **Type-C Port 1 Connector Type Select**<br>This setting configures the physical connector type to be used for Type-C Port 1. | UP4<br>UP3 | Type-C<br>Type-C |
| | **Type-C Port 2 Connector Type Select**<br>This setting configures the physical connector type to be used for Type-C Port 2. | UP4<br>UP3 | Type-C<br>Type-C |
| | **Type-C Port 3 Connector Type Select**<br>This setting configures the physical connector type to be used for Type-C Port 3. | UP4<br>UP3 | Type-C<br>Type-C |
| | **Type-C Port 4 Connector Type Select**<br>This setting configures the physical connector type to be used for Type-C Port 4. | UP4<br>UP3 | Type-C<br>Type-C |
| | **xDCI Split Die Configuration**<br>**Values: xDCI Split Die Enabled, xDCI Split Die Disabled** | UP4<br>UP3 | xDCI Split Die Enabled<br>xDCI Split Die Enabled |
| **Click on Flex I/O in the left tabs menu> Thunderbolt Configuration is expanded by default:** | | | |




| # | Parameter | Platform | Settings |
|---|---|---|---|
| 7 | **Thunderbolt Configuration** | | |
| | **Thunderbolt Enable**<br>**Values: Yes/No**<br>This setting determines if the Thunderbolt(tm) interface is enabled on the platform. | UP4<br>UP3 | Yes<br>Yes |
| **Click on Flex I/O in the left tabs menu> Power Delivery PD Controller Configuration is expanded by default:** | | | |

## Table 2-16. - Flex I/O Straps (Sheet 10 of 15)

### Power Delivery PD Controller Configuration 8

| Parameter | Value | |
|---|---|---|
| PMC-PD controller USB-C Mode Enabled | PMC / SMBus | This bit defines how the PMC interfaces with the type C components on the board |
| Re-timer Power Gating Enabled | No | Indicates whether platform Re-timer power gating is enabled. |
| Type-C port 1 Enabled | Yes | Indicates whether the associated Type-C port is enabled. |
| USB2 Port Number associated for Type-C Port 1 | USB2 Port 1 | USB2 port number for the associated Type-C port |
| USB3 Port Number associated for Type-C Port 1 | Type-C Port 1 | USB3 port number for the associated Type-C port |
| Type-C Port 1 Re-Timer Present | Yes | Indicates whether a re-timer is present for the associated Type-C port. |
| Type-C Port 1 Re-timer Configuration Enabled | No | Indicates whether the associated re-timer requires configuration. Enabled = configu |
| 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 enabled |
| USB2 Port Number associated for Type-C Port 2 | USB2 Port 5 | USB2 port number for the associated Type-C port |
| USB3 Port Number associated for Type-C Port 2 | Type-C Port 2 | USB3 port number for the associated Type-C port |
| Type-C Port 2 Re-Timer Present | Yes | Indicates whether a re-timer is present for the associated Type-C port. |
| Type-C Port 2 Re-timer Configuration Enabled | No | Indicates whether the associated re-timer requires configuration. Enabled = configu |
| 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 enabled |
| USB2 Port Number associated for Type-C Port 3 | USB2 Port 6 | USB2 port number for the associated Type-C port |
| USB3 Port Number associated for Type-C Port 3 | Type-C Port 3 | USB3 port number for the associated Type-C port |
| Type-C Port 3 Re-Timer Present | Yes | Indicates whether a re-timer is present for the associated Type-C port. |
| Type-C Port 3 Re-timer Configuration Enabled | No | Indicates whether the associated re-timer requires configuration. Enabled = configu |
| 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 enabled |
| USB2 Port Number associated for Type-C Port 4 | USB2 Port 7 | USB2 port number for the associated Type-C port |
| USB3 Port Number associated for Type-C Port 4 | Type-C Port 4 | USB3 port number for the associated Type-C port |
| Type-C Port 4 Re-Timer Present | Yes | Indicates whether a re-timer is present for the associated Type-C port. |
| Type-C Port 4 Re-timer Configuration Enabled | No | Indicates whether the associated re-timer requires configuration. Enabled = configu |
| Type-C Port 4 Re-timer SMBus Address | 0x43 | SMBus address for the associated re-timer |
| Type-C Port 4 SMBus Address | 0x53 | SMBus address for the associated Type-C port |
| Type-C Port 1 Re-Timer Configuration Type | 1 Re-Timer | This setting determines the number of Re-Timers being use for Type-C Port 1. |
| Type-C Port 2 Re-Timer Configuration Type | 1 Re-Timer | This setting determines the number of Re-Timers being use for Type-C Port 2. |
| Type-C Port 3 Re-Timer Configuration Type | 1 Re-Timer | This setting determines the number of Re-Timers being use for Type-C Port 3. |
| Type-C Port 4 Re-Timer Configuration Type | 1 Re-Timer | This setting determines the number of Re-Timers being use for Type-C Port 4. |

| | | | |
|---|---|---|---|
| 8 | **Power Delivery PD Controller Configuration** | | |

## Table 2-16. - Flex I/O Straps (Sheet 11 of 15)

| | | | |
|---|---|---|---|
| | **PMC-PD controller USB-C Mode Enabled**<br>**Values:**<br>**0: PMC interfaces with an eSPI connected agent via eSPI OOB**<br>**1: PMC interfaces with PD chips/Re-timer via ALERT# pin which triggers SMBus transactions.**<br><br>This bit defines how the PMC interfaces with the Type-C components on the board.<br><br>***Notes:***<br>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.<br>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. | UP4<br>UP3 | PMC / SMBus<br>PMC / SMBus |
| | **Re-timer Power Gating Enabled**<br>**Values: Yes / No**<br>This setting indicates whether platform Re-timer power gating is enabled. | UP4<br>UP3 | No<br>No |
| | **Type-C port 1 Enabled**<br>**Values: Yes / No**<br>This setting indicates whether the associated Type-C port1 is enabled.<br><br>***Note:*** This setting is only available for configuration when PMC-PD controller USB-C Mode Enabled parameter is set to 1. | UP4<br>UP3 | Yes<br>Yes |
| | **USB2 Port Number associated for Type-C Port 1**<br>**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**<br>This indicates the USB2 port number for the associated Type-C port1.<br><br>***Notes:***<br>1. This parameter is applicable only when Type-C port 1 Enabled is set to yes.<br>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”.<br>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) | UP4<br>UP3 | USB2 Port 1<br>USB2 Port 1 |
| | **USB3 Port number associated for Type-C Port 1**<br>**Values: USB3 Port 1,USB3 Port 2,USB3 Port 3,USB3 Port 4**<br>This indicates the USB3 port number for the associated Type-C port1.<br><br>***Notes:***<br>1. This parameter is applicable only when Type-C port 1 Enabled is set to yes.<br>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”.<br>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) | UP4<br>UP3 | USB3 Port 1<br>USB3 Port 1 |
| | **Type-C Port 1 Re-timer Present**<br>**Values: Yes / No**<br>This indicates whether a re-timer is present for the associated Type-C port. | UP4<br>UP3 | Yes<br>Yes |

## Table 2-16. - Flex I/O Straps (Sheet 12 of 15)

| | | | |
|---|---|---|---|
| | **Type-C Port 1 Re-timer Configuration Enabled**<br>**Values: Yes / No**<br>Indicates whether the associated re-timer requires configuration. Yes = configuration done via PMC; No = configuration done via PD Controller. | UP4<br>UP3 | No<br>No |
| | **Type-C Port 1 Re-timer SMBus Address**<br>**Value: Hex**<br>This indicates the SMBus address for the associated re-timer. | UP4<br>UP3 | 0x40<br>0x40 |
| | **Type-C Port 1 SMBus Address**<br>**Value: Hex**<br>This indicates the SMBus address for the associated Type-C port.<br><br>***Note:*** OEMs are recommended to set unique SMBus address allocation for Type-C port and Re-timer associated. | UP4<br>UP3 | 0x20<br>0x50 |
| | **Type-C port 2 Enabled**<br>**Values: Yes / No**<br>This setting indicates whether the associated Type-C port is enabled.<br><br>***Note:*** This setting is only available for configuration when PMC-PD controller USB-C Mode Enabled parameter is set to 1. | UP4<br>UP3 | Yes<br>Yes |
| | **USB2 Port Number associated for Type-C Port 2**<br>**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**<br>This indicates the USB2 port number for the associated Type-C port.<br><br>***Notes:***<br>1. This parameter is applicable only when Type-C port 2 Enabled is set to yes.<br>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”.<br>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) | UP4<br>UP3 | USB2 Port 5<br>USB2 Port 5 |
| | **USB3 Port number associated for Type-C Port 2**<br>**Values: USB3 Port 1,USB3 Port 2,USB3 Port 3,USB3 Port 4**<br>This indicates the USB3 port number for the associated Type-C port.<br><br>***Notes:***<br>1. This parameter is applicable only when Type-C port 2Enabled is set to yes.<br>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”.<br>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) | UP4<br>UP3 | USB3 Port 2<br>USB3 Port 2 |
| | **Type-C Port 2 Re-timer Present**<br>**Values: Yes / No**<br>This indicates whether a re-timer is present for the associated Type-C port. | UP4<br>UP3 | Yes<br>Yes |
| | **Type-C Port 2 Re-timer Configuration Enabled**<br>**Values: Yes / No**<br>Indicates whether the associated re-timer requires configuration. Yes = configuration done via PMC; No = configuration done via PD Controller. | UP4<br>UP3 | No<br>No |

## Table 2-16. - Flex I/O Straps (Sheet 13 of 15)

| | | | |
|---|---|---|---|
| | **Type-C Port 2 Re-timer SMBus Address**<br>**Value: Hex**<br>This indicates the SMBus address for the associated re-timer. | UP4<br>UP3 | 0x41<br>0x41 |
| | **Type-C Port 2 SMBus Address**<br>**Value: Hex**<br>This indicates the SMBus address for the associated Type-C port.<br><br>***Note:*** OEMs are recommended to set unique SMBus address allocation for Type-C port and Re-timer associated. | UP4<br>UP3 | 0x24<br>0x51 |
| | **Type-C port 3 Enabled**<br>**Values: Yes / No**<br>This setting indicates whether the associated Type-C port is enabled.<br><br>***Note:*** This setting is only available for configuration when PMC-PD controller USB-C Mode Enabled parameter is set to 1. | UP4<br>UP3 | Yes<br>Yes |
| | **USB2 Port Number associated for Type-C Port 3**<br>**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**<br>This indicates the USB2 port number for the associated Type-C port.<br><br>***Notes:***<br>1. This parameter is applicable only when Type-C port 3 Enabled is set to yes.<br>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”.<br>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) | UP4<br>UP3 | USB2 Port 6<br>USB2 Port 6 |
| | **USB3 Port number associated for Type-C Port 3**<br>**Values: USB3 Port 1,USB3 Port 2,USB3 Port 3,USB3 Port 4**<br>This indicates the USB3 port number for the associated Type-C port.<br><br>***Notes:***<br>1. This parameter is applicable only when Type-C port 3 Enabled is set to yes.<br>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”.<br>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) | UP4<br>UP3 | USB3 Port 3<br>USB3 Port 3 |
| | **Type-C Port 3 Re-timer Present**<br>**Values: Yes / No**<br>This indicates whether a re-timer is present for the associated Type-C port. | UP4<br>UP3 | Yes<br>Yes |
| | **Type-C Port 3 Re-timer Configuration Enabled**<br>**Values: Yes / No**<br>Indicates whether the associated re-timer requires configuration. Yes = configuration done via PMC; No = configuration done via PD Controller. | UP4<br>UP3 | No<br>No |
| | **Type-C Port 3 Re-timer SMBus Address**<br>**Value: Hex**<br>This indicates the SMBus address for the associated re-timer. | UP4<br>UP3 | 0x42<br>0x42 |

## Table 2-16. - Flex I/O Straps (Sheet 14 of 15)

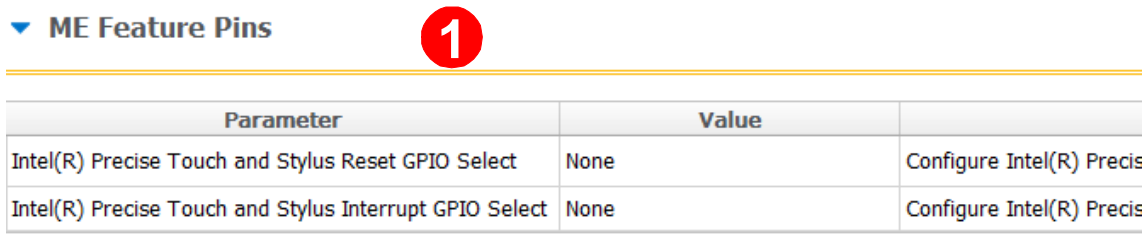
| | | | |
|---|---|---|---|
| | **Type-C Port 3 SMBus Address**<br>**Value: Hex**<br>This indicates the SMBus address for the associated Type-C port.<br><br>***Note:*** OEMs are recommended to set unique SMBus address allocation for Type-C port and Re-timer associated. | UP4<br>UP3 | 0x23<br>0x52 |
| | **Type-C port 4 Enabled**<br>**Values: Yes / No**<br>This setting indicates whether the associated Type-C port is enabled.<br><br>***Note:*** This setting is only available for configuration when PMC-PD controller USB-C Mode Enabled parameter is set to 1. | UP4<br>UP3 | No<br>Yes |
| | **USB2 Port Number associated for Type-C Port 4**<br>**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**<br>This indicates the USB2 port number for the associated Type-C port.<br><br>***Notes:***<br>1. This parameter is applicable only when Type-C port 4 Enabled is set to yes.<br>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”.<br>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) | UP4<br>UP3 | USB2 Port 7<br>USB2 Port 7 |
| | **USB3 Port number associated for Type-C Port 4**<br>**Values: USB3 Port 1,USB3 Port 2,USB3 Port 3,USB3 Port 4**<br>This indicates the USB3 port number for the associated Type-C port.<br><br>***Notes:***<br>1. This parameter is applicable only when Type-C port 4 Enabled is set to yes.<br>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”.<br>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) | UP4<br>UP3 | USB3 Port 4<br>USB3 Port 4 |
| | **Type-C Port 4 Re-timer Present**<br>**Values: Yes / No**<br>This indicates whether a re-timer is present for the associated Type-C port. | UP4<br>UP3 | No<br>Yes |
| | **Type-C Port 4 Re-timer Configuration Enabled**<br>**Values: Yes / No**<br>Indicates whether the associated re-timer requires configuration. Yes = configuration done via PMC; No = configuration done via PD Controller. | UP4<br>UP3 | No<br>No |
| | **Type-C Port 4 Re-timer SMBus Address**<br>**Value: Hex**<br>This indicates the SMBus address for the associated re-timer. | UP4<br>UP3 | 0x0<br>0x43 |
| | **Type-C Port 4 SMBus Address**<br>**Value: Hex**<br>This indicates the SMBus address for the associated Type-C port.<br><br>***Note:*** OEMs are recommended to set unique SMBus address allocation for Type-C port and Re-timer associated. | UP4<br>UP3 | 0x0<br>0x53 |

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

| | | | |
|---|---|---|---|
| | **Type-C Port 1 Connector Type Select**<br>**Values: 1 Re-Timer, 2 Re-Timers**<br>This setting determines the number of Re-Timers being used for TYpe-C Port 1 | UP4<br>UP3 | 1 Re-Timer<br>1 Re-Timer |
| | **Type-C Port 2 Connector Type Select**<br>**Values: 1 Re-Timer, 2 Re-Timers**<br>This setting determines the number of Re-Timers being used for TYpe-C Port 2 | UP4<br>UP3 | 1 Re-Timer<br>1 Re-Timer |
| | **Type-C Port 3 Connector Type Select**<br>**Values: 1 Re-Timer, 2 Re-Timers**<br>This setting determines the number of Re-Timers being used for TYpe-C Port 3 | UP4<br>UP3 | 1 Re-Timer<br>1 Re-Timer |
| | **Type-C Port 4 Connector Type Select**<br>**Values: 1 Re-Timer, 2 Re-Timers**<br>This setting determines the number of Re-Timers being used for TYpe-C Port 4 | UP4<br>UP3 | 1 Re-Timer<br>1 Re-Timer |

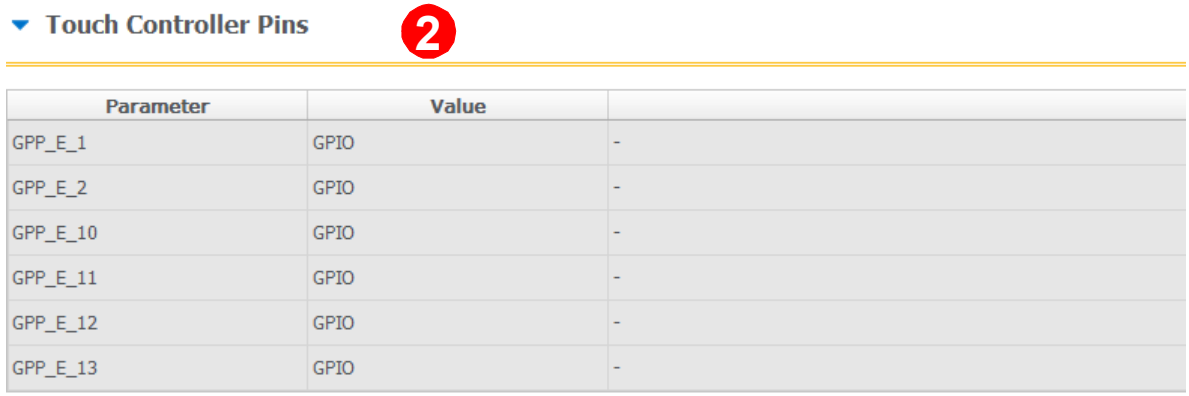
## Table 2-17. - GPIO (Sheet 1 of 20)

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




| # | Parameter | Platform | Settings |
|---|---|---|---|
| 1 | **ME Feature Pins** | | |
| | **Intel® Precise Touch and Stylus Reset GPIO Select**<br>Configure Intel® Precise Touch and Stylus Reset GPIO. | UP4<br>UP3 | None<br>None |
| | **Intel® Precise Touch and Stylus Interrupt GPIO Select**<br>Configure Intel® Precise Touch and Stylus Interrupt GPIO. | UP4<br>UP3 | None<br>None |

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




| # | Parameter | Platform | Settings |
|---|---|---|---|
| 2 | **Touch Controller Pins** | | |
| | **GPP_E_1** | UP4<br>UP3 | GPIO<br>GPIO |
| | **GPP_E_2** | UP4<br>UP3 | GPIO<br>GPIO |
| | **GPP_E_10** | UP4<br>UP3 | GPIO<br>GPIO |
| | **GPP_E_11** | UP4<br>UP3 | GPIO<br>GPIO |
| | **GPP_E_12** | UP4<br>UP3 | GPIO<br>GPIO |
| | **GPP_E_13** | UP4<br>UP3 | GPIO<br>GPIO |

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

## Table 2-17. - GPIO (Sheet 2 of 20)

### GPIO VCCIO Voltage Control

3

| Parameter | Value | |
|---|---|---|
| GPP_A0 Individual Voltage Select | 1.8Volts | This setting controls the VCCIO voltage for the GPP_ |
| GPP_A1 Individual Voltage Select | 1.8Volts | This setting controls the VCCIO voltage for the GPP_ |
| GPP_A2 Individual Voltage Select | 1.8Volts | This setting controls the VCCIO voltage for the GPP_ |
| GPP_A3 Individual Voltage Select | 1.8Volts | This setting controls the VCCIO voltage for the GPP_ |
| GPP_A4 Individual Voltage Select | 1.8Volts | This setting controls the VCCIO voltage for the GPP_ |
| GPP_A5 Individual Voltage Select | 1.8Volts | This setting controls the VCCIO voltage for the GPP_ |
| GPP_A6 Individual Voltage Select | 1.8Volts | This setting controls the VCCIO voltage for the GPP_ |
| GPP_A7 Individual Voltage Select | 1.8Volts | This setting controls the VCCIO voltage for the GPP_ |
| GPP_A8 Individual Voltage Select | 1.8Volts | This setting controls the VCCIO voltage for the GPP_ |
| GPP_A9 Individual Voltage Select | 1.8Volts | This setting controls the VCCIO voltage for the GPP_ |
| GPP_A10 Individual Voltage Sel... | 1.8Volts | This setting controls the VCCIO voltage for the GPP_ |
| GPP_A11 Individual Voltage Sel... | 3.3Volts | This setting controls the VCCIO voltage for the GPP_ |
| GPP_A12 Individual Voltage Sel... | 3.3Volts | This setting controls the VCCIO voltage for the GPP_ |
| GPP_A13 Individual Voltage Sel... | 3.3Volts | This setting controls the VCCIO voltage for the GPP_ |
| GPP_A14 Individual Voltage Sel... | 3.3Volts | This setting controls the VCCIO voltage for the GPP_ |
| GPP_A15 Individual Voltage Sel... | 3.3Volts | This setting controls the VCCIO voltage for the GPP_ |
| GPP_A16 Individual Voltage Sel... | 3.3Volts | This setting controls the VCCIO voltage for the GPP_ |
| GPP_A17 Individual Voltage Sel... | 3.3Volts | This setting controls the VCCIO voltage for the GPP_ |
| GPP_A18 Individual Voltage Sel... | 3.3Volts | This setting controls the VCCIO voltage for the GPP_ |
| GPP_A19 Individual Voltage Sel... | 3.3Volts | This setting controls the VCCIO voltage for the GPP_ |
| GPP_A20 Individual Voltage Sel... | 3.3Volts | This setting controls the VCCIO voltage for the GPP_ |
| GPP_A21 Individual Voltage Sel... | 3.3Volts | This setting controls the VCCIO voltage for the GPP_ |
| GPP_A22 Individual Voltage Sel... | 3.3Volts | This setting controls the VCCIO voltage for the GPP_ |
| GPP_A23 Individual Voltage Sel... | 3.3Volts | This setting controls the VCCIO voltage for the GPP_ |

| # | Parameter | Platform | Settings |
|---|---|---|---|
| 3 | **GPIO VCCIO Voltage Control**<br>***Warning:*** Incorrectly configuring GPIO voltages may result in MCP damage. The voltage settings below are for the specific RVPs noted under the Platform column. Customers should check their schematics to verify that the appropriate voltages are configured. | | |
| **#** | **Parameter** | **Platform** | **Settings** |
| | **GPP_A0 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_A0 GPIO pin. | UP4<br>UP3 | 1.8 Volts<br>1.8 Volts |

## Table 2-17. - GPIO (Sheet 3 of 20)

| # | Parameter | Platform | Settings |
|---|---|---|---|
| | **GPP_A1 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_A1 GPIO pin. | UP4<br>UP3 | 1.8 Volts<br>1.8 Volts |
| | **GPP_A2 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_A2 GPIO pin. | UP4<br>UP3 | 1.8 Volts<br>1.8 Volts |
| | **GPP_A3 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_A3 GPIO pin. | UP4<br>UP3 | 1.8 Volts<br>1.8 Volts |
| | **GPP_A4 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_A4 GPIO pin. | UP4<br>UP3 | 1.8 Volts<br>1.8 Volts |
| | **GPP_A5 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_A5 GPIO pin. | UP4<br>UP3 | 1.8 Volts<br>1.8 Volts |
| | **GPP_A6 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_A6 GPIO pin. | UP4<br>UP3 | 1.8 Volts<br>1.8 Volts |
| | **GPP_A7 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_A7 GPIO pin. | UP4<br>UP3 | 1.8 Volts<br>1.8 Volts |
| | **GPP_A8 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_A8 GPIO pin. | UP4<br>UP3 | 1.8 Volts<br>1.8 Volts |
| | **GPP_A9 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_A9 GPIO pin. | UP4<br>UP3 | 1.8 Volts<br>1.8 Volts |
| | **GPP_A10 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_A10 GPIO pin. | UP4<br>UP3 | 1.8 Volts<br>1.8 Volts |
| | **GPP_A11 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_A11 GPIO pin. | UP4<br>UP3 | 3.3 Volts<br>3.3 Volts |
| | **GPP_A12 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_A12 GPIO pin. | UP4<br>UP3 | 3.3 Volts<br>3.3 Volts |
| | **GPP_A13 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_A13 GPIO pin. | UP4<br>UP3 | 3.3 Volts<br>3.3 Volts |
| | **GPP_A14 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_A14 GPIO pin. | UP4<br>UP3 | 3.3 Volts<br>3.3 Volts |
| | **GPP_A15 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_A15 GPIO pin. | UP4<br>UP3 | 3.3 Volts<br>3.3 Volts |
| | **GPP_A16 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_A16 GPIO pin. | UP4<br>UP3 | 3.3 Volts<br>3.3 Volts |
| | **GPP_A17 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_A17 GPIO pin. | UP4<br>UP3 | 3.3 Volts<br>3.3 Volts |
| | **GPP_A18 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_A18 GPIO pin. | UP4<br>UP3 | 3.3 Volts<br>3.3 Volts |

## Table 2-17. - GPIO (Sheet 4 of 20)

| # | Parameter | Platform | Settings |
|---|---|---|---|
| | **GPP_A19 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_A19 GPIO pin. | UP4<br>UP3 | 3.3 Volts<br>3.3 Volts |
| | **GPP_A20 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_A20 GPIO pin. | UP4<br>UP3 | 3.3 Volts<br>3.3 Volts |
| | **GPP_A21 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_A21 GPIO pin. | UP4<br>UP3 | 3.3 Volts<br>3.3 Volts |
| | **GPP_A22 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_A22 GPIO pin. | UP4<br>UP3 | 3.3 Volts<br>3.3 Volts |
| | **GPP_A23 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_A23 GPIO pin. | UP4<br>UP3 | 3.3 Volts<br>3.3 Volts |

## Table 2-17. - GPIO (Sheet 5 of 20)

| | | |
|---|---|---|
| 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**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_B0 GPIO pin. | UP4<br>UP3 | 1.8 Volts<br>1.8 Volts |
| | **GPP_B1 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_B1 GPIO pin. | UP4<br>UP3 | 1.8 Volts<br>1.8 Volts |
| | **GPP_B2 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_B2 GPIO pin. | UP4<br>UP3 | 3.3 Volts<br>3.3 Volts |

## Table 2-17. - GPIO (Sheet 6 of 20)

| # | Parameter | Platform | Settings |
|---|---|---|---|
| | **GPP_B3 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_B3 GPIO pin. | UP4<br>UP3 | 1.8 Volts<br>1.8 Volts |
| | **GPP_B4 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_B4 GPIO pin. | UP4<br>UP3 | 1.8 Volts<br>1.8 Volts |
| | **GPP_B5 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_B5 GPIO pin. | UP4<br>UP3 | 1.8 Volts<br>1.8 Volts |
| | **GPP_B6 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_B6 GPIO pin. | UP4<br>UP3 | 1.8 Volts<br>1.8 Volts |
| | **GPP_B7 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_B7 GPIO pin. | UP4<br>UP3 | 1.8 Volts<br>1.8 Volts |
| | **GPP_B8 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_B8 GPIO pin. | UP4<br>UP3 | 1.8 Volts<br>1.8 Volts |
| | **GPP_B9 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_B9 GPIO pin. | UP4<br>UP3 | 1.8 Volts<br>1.8 Volts |
| | **GPP_B10 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_B10 GPIO pin. | UP4<br>UP3 | 1.8 Volts<br>1.8 Volts |
| | **GPP_B11 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_B11 GPIO pin. | UP4<br>UP3 | 3.3 Volts<br>3.3 Volts |
| | **GPP_B12 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_B12 GPIO pin. | UP4<br>UP3 | 3.3 Volts<br>3.3 Volts |
| | **GPP_B13 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_B13 GPIO pin. | UP4<br>UP3 | 3.3 Volts<br>3.3 Volts |
| | **GPP_B14 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_B14 GPIO pin. | UP4<br>UP3 | 1.8 Volts<br>1.8 Volts |
| | **GPP_B15 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_B15 GPIO pin. | UP4<br>UP3 | 3.3 Volts<br>3.3 Volts |
| | **GPP_B16 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_B16 GPIO pin. | UP4<br>UP3 | 3.3 Volts<br>3.3 Volts |
| | **GPP_B17 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_B17 GPIO pin. | UP4<br>UP3 | 3.3 Volts<br>3.3 Volts |
| | **GPP_B18 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_B18 GPIO pin. | UP4<br>UP3 | 3.3 Volts<br>3.3 Volts |
| | **GPP_B19 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_B19 GPIO pin. | UP4<br>UP3 | 3.3 Volts<br>3.3 Volts |
| | **GPP_B20 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_B20 GPIO pin. | UP4<br>UP3 | 3.3 Volts<br>3.3 Volts |

## Table 2-17. - GPIO (Sheet 7 of 20)

| # | Parameter | Platform | Settings |
|---|---|---|---|
| | **GPP_B21 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_B21 GPIO pin. | UP4<br>UP3 | 3.3 Volts<br>3.3 Volts |
| | **GPP_B22 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_B22 GPIO pin. | UP4<br>UP3 | 3.3 Volts<br>3.3 Volts |
| | **GPP_B23 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_B23 GPIO pin. | UP4<br>UP3 | 1.8 Volts<br>1.8 Volts |

| | | |
|---|---|---|
| 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 2-17. - GPIO (Sheet 8 of 20)

| # | Parameter | Platform | Settings |
|---|---|---|---|
| | **GPP_C0 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_C0 GPIO pin. | UP4<br>UP3 | 3.3 Volts<br>3.3 Volts |
| | **GPP_C1 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_C1 GPIO pin. | UP4<br>UP3 | 3.3 Volts<br>1.8 Volts |
| | **GPP_C2 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_C2 GPIO pin. | UP4<br>UP3 | 1.8 Volts<br>3.3 Volts |
| | **GPP_C3 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_C3 GPIO pin. | UP4<br>UP3 | 3.3 Volts<br>3.3 Volts |
| | **GPP_C4 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_C4 GPIO pin. | UP4<br>UP3 | 3.3 Volts<br>3.3 Volts |
| | **GPP_C5 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_C5 GPIO pin. | UP4<br>UP3 | 1.8 Volts<br>1.8 Volts |
| | **GPP_C6 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_C6 GPIO pin. | UP4<br>UP3 | 3.3 Volts<br>3.3 Volts |
| | **GPP_C7 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_C7 GPIO pin. | UP4<br>UP3 | 3.3 Volts<br>3.3 Volts |
| | **GPP_C8 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_C8 GPIO pin. | UP4<br>UP3 | 1.8 Volts<br>1.8 Volts |
| | **GPP_C9 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_C9 GPIO pin. | UP4<br>UP3 | 3.3 Volts<br>3.3 Volts |
| | **GPP_C10 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_C10 GPIO pin. | UP4<br>UP3 | 1.8 Volts<br>1.8 Volts |
| | **GPP_C11 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_C11 GPIO pin. | UP4<br>UP3 | 3.3 Volts<br>3.3 Volts |
| | **GPP_C12 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_C12 GPIO pin. | UP4<br>UP3 | 1.8 Volts<br>1.8 Volts |
| | **GPP_C13 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_C13 GPIO pin. | UP4<br>UP3 | 3.3 Volts<br>3.3 Volts |
| | **GPP_C14 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_C14 GPIO pin. | UP4<br>UP3 | 3.3 Volts<br>3.3 Volts |
| | **GPP_C15 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_C15 GPIO pin. | UP4<br>UP3 | 1.8 Volts<br>1.8 Volts |
| | **GPP_C16 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_C16 GPIO pin. | UP4<br>UP3 | 1.8 Volts<br>1.8 Volts |
| | **GPP_C17 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_C17 GPIO pin. | UP4<br>UP3 | 1.8 Volts<br>1.8 Volts |

## Table 2-17. - GPIO (Sheet 9 of 20)

| # | Parameter | Platform | Settings |
|---|---|---|---|
| | **GPP_C18 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_C18 GPIO pin. | UP4<br>UP3 | 1.8 Volts<br>1.8 Volts |
| | **GPP_C19 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_C19 GPIO pin. | UP4<br>UP3 | 1.8 Volts<br>1.8 Volts |
| | **GPP_C20 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_C20 GPIO pin. | UP4<br>UP3 | 3.3 Volts<br>3.3 Volts |
| | **GPP_C21 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_C21 GPIO pin. | UP4<br>UP3 | 3.3 Volts<br>3.3 Volts |
| | **GPP_C22 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_C22 GPIO pin. | UP4<br>UP3 | 3.3 Volts<br>3.3 Volts |
| | **GPP_C23 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_C23 GPIO pin. | UP4<br>UP3 | 3.3 Volts<br>3.3 Volts |

## Table 2-17. - GPIO (Sheet 10 of 20)

| | | |
|---|---|---|
| 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 |

| # | Parameter | Platform | Settings |
|---|---|---|---|
| | **GPP_D0 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_D0 GPIO pin. | UP4<br>UP3 | 1.8 Volts<br>1.8 Volts |
| | **GPP_D1 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_D1 GPIO pin. | UP4<br>UP3 | 1.8 Volts<br>1.8 Volts |
| | **GPP_D2 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_D2 GPIO pin. | UP4<br>UP3 | 1.8 Volts<br>1.8 Volts |
| | **GPP_D3 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_D3 GPIO pin. | UP4<br>UP3 | 1.8 Volts<br>1.8 Volts |
| | **GPP_D4 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_D4 GPIO pin. | UP4<br>UP3 | 1.8 Volts<br>1.8 Volts |

## Table 2-17. - GPIO (Sheet 11 of 20)

| # | Parameter | Platform | Settings |
|---|---|---|---|
| | **GPP_D5 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_D5 GPIO pin. | UP4<br>UP3 | 3.3 Volts<br>3.3 Volts |
| | **GPP_D6 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_D6 GPIO pin. | UP4<br>UP3 | 3.3 Volts<br>3.3 Volts |
| | **GPP_D7 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_D7 GPIO pin. | UP4<br>UP3 | 3.3 Volts<br>3.3 Volts |
| | **GPP_D8 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_D8 GPIO pin. | UP4<br>UP3 | 3.3 Volts<br>3.3 Volts |
| | **GPP_D9 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_D9 GPIO pin. | UP4<br>UP3 | 3.3 Volts<br>3.3 Volts |
| | **GPP_D10 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_D10 GPIO pin. | UP4<br>UP3 | 3.3 Volts<br>3.3 Volts |
| | **GPP_D11 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_D11 GPIO pin. | UP4<br>UP3 | 3.3 Volts<br>3.3 Volts |
| | **GPP_D12 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_D12 GPIO pin. | UP4<br>UP3 | 1.8 Volts<br>3.3 Volts |
| | **GPP_D13 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_D13 GPIO pin. | UP4<br>UP3 | 3.3 Volts<br>3.3 Volts |
| | **GPP_D14 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_D14 GPIO pin. | UP4<br>UP3 | 3.3 Volts<br>3.3 Volts |
| | **GPP_D15 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_D15 GPIO pin. | UP4<br>UP3 | 3.3 Volts<br>3.3 Volts |
| | **GPP_D16 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_D16 GPIO pin. | UP4<br>UP3 | 3.3 Volts<br>3.3 Volts |
| | **GPP_D17 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_D17 GPIO pin. | UP4<br>UP3 | 1.8 Volts<br>1.8 Volts |
| | **GPP_D18 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_D18 GPIO pin. | UP4<br>UP3 | 1.8 Volts<br>1.8 Volts |
| | **GPP_D19 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_D19 GPIO pin. | UP4<br>UP3 | 1.8 Volts<br>1.8 Volts |

## Table 2-17. - GPIO (Sheet 12 of 20)

| | | |
|---|---|---|
| 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 |

| # | Parameter | Platform | Settings |
|---|---|---|---|
| | **GPP_E0 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_E0 GPIO pin. | UP4<br>UP3 | 1.8 Volts<br>1.8 Volts |
| | **GPP_E1 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_E1 GPIO pin. | UP4<br>UP3 | 1.8 Volts<br>1.8 Volts |
| | **GPP_E2 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_E2 GPIO pin. | UP4<br>UP3 | 1.8 Volts<br>1.8 Volts |

## Table 2-17. - GPIO (Sheet 13 of 20)

| # | Parameter | Platform | Settings |
|---|---|---|---|
| | **GPP_E3 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_E3 GPIO pin. | UP4<br>UP3 | 1.8 Volts<br>1.8 Volts |
| | **GPP_E4 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_E4 GPIO pin. | UP4<br>UP3 | 3.3 Volts<br>3.3 Volts |
| | **GPP_E5 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_E5 GPIO pin. | UP4<br>UP3 | 3.3 Volts<br>3.3 Volts |
| | **GPP_E6 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_E6 GPIO pin. | UP4<br>UP3 | 1.8 Volts<br>1.8 Volts |
| | **GPP_E7 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_E7 GPIO pin. | UP4<br>UP3 | 3.3 Volts<br>3.3 Volts |
| | **GPP_E8 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_E8 GPIO pin. | UP4<br>UP3 | 3.3 Volts<br>3.3 Volts |
| | **GPP_E9 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_E9 GPIO pin. | UP4<br>UP3 | 3.3 Volts<br>3.3 Volts |
| | **GPP_E10 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_E10 GPIO pin. | UP4<br>UP3 | 1.8 Volts<br>1.8 Volts |
| | **GPP_E11 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_E11 GPIO pin. | UP4<br>UP3 | 1.8 Volts<br>1.8 Volts |
| | **GPP_E12 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_E12 GPIO pin. | UP4<br>UP3 | 1.8 Volts<br>1.8 Volts |
| | **GPP_E13 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_E13 GPIO pin. | UP4<br>UP3 | 1.8 Volts<br>1.8 Volts |
| | **GPP_E14 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_E14 GPIO pin. | UP4<br>UP3 | 3.3 Volts<br>3.3 Volts |
| | **GPP_E15 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_E15 GPIO pin. | UP4<br>UP3 | 1.8 Volts<br>1.8 Volts |
| | **GPP_E16 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_E16 GPIO pin. | UP4<br>UP3 | 1.8 Volts<br>1.8 Volts |
| | **GPP_E17 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_E17 GPIO pin. | UP4<br>UP3 | 1.8 Volts<br>1.8 Volts |
| | **GPP_E18 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_E18 GPIO pin. | UP4<br>UP3 | 3.3 Volts<br>3.3 Volts |
| | **GPP_E19 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_E19 GPIO pin. | UP4<br>UP3 | 3.3 Volts<br>3.3 Volts |
| | **GPP_E20 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_E20 GPIO pin. | UP4<br>UP3 | 3.3 Volts<br>3.3 Volts |

## Table 2-17. - GPIO (Sheet 14 of 20)

| # | Parameter | Platform | Settings |
|---|---|---|---|
| | **GPP_E21 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_E21 GPIO pin. | UP4<br>UP3 | 3.3 Volts<br>3.3 Volts |
| | **GPP_E22 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_E22 GPIO pin. | UP4<br>UP3 | 1.8 Volts<br>3.3 Volts |
| | **GPP_E23 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_E23 GPIO pin. | UP4<br>UP3 | 1.8 Volts<br>3.3 Volts |

| | | |
|---|---|---|
| GPP_F0 Individual Voltage Select | 3.3Volts | This setting controls the VCCIO voltage for |
| GPP_F1 Individual Voltage Select | 3.3Volts | This setting controls the VCCIO voltage for |
| GPP_F2 Individual Voltage Select | 3.3Volts | This setting controls the VCCIO voltage for |
| GPP_F3 Individual Voltage Select | 3.3Volts | This setting controls the VCCIO voltage for |
| GPP_F4 Individual Voltage Select | 3.3Volts | This setting controls the VCCIO voltage for |
| GPP_F5 Individual Voltage Select | 3.3Volts | This setting controls the VCCIO voltage for |
| GPP_F6 Individual Voltage Select | 3.3Volts | This setting controls the VCCIO voltage for |
| GPP_F7 Individual Voltage Select | 3.3Volts | This setting controls the VCCIO voltage for |
| GPP_F8 Individual Voltage Select | 3.3Volts | This setting controls the VCCIO voltage for |
| GPP_F9 Individual Voltage Select | 3.3Volts | This setting controls the VCCIO voltage for |
| GPP_F10 Individual Voltage Select | 3.3Volts | This setting controls the VCCIO voltage for |
| GPP_F11 Individual Voltage Select | 3.3Volts | This setting controls the VCCIO voltage for |
| GPP_F12 Individual Voltage Select | 3.3Volts | This setting controls the VCCIO voltage for |
| GPP_F13 Individual Voltage Select | 3.3Volts | This setting controls the VCCIO voltage for |
| GPP_F14 Individual Voltage Select | 3.3Volts | This setting controls the VCCIO voltage for |
| GPP_F15 Individual Voltage Select | 3.3Volts | This setting controls the VCCIO voltage for |
| GPP_F16 Individual Voltage Select | 3.3Volts | This setting controls the VCCIO voltage for |
| GPP_F17 Individual Voltage Select | 3.3Volts | This setting controls the VCCIO voltage for |
| GPP_F18 Individual Voltage Select | 3.3Volts | This setting controls the VCCIO voltage for |
| GPP_F19 Individual Voltage Select | 3.3Volts | This setting controls the VCCIO voltage for |
| GPP_F20 Individual Voltage Select | 3.3Volts | This setting controls the VCCIO voltage for |
| GPP_F21 Individual Voltage Select | 3.3Volts | This setting controls the VCCIO voltage for |
| GPP_F22 Individual Voltage Select | 3.3Volts | This setting controls the VCCIO voltage for |
| GPP_F23 Individual Voltage Select | 3.3Volts | This setting controls the VCCIO voltage for |

## Table 2-17. - GPIO (Sheet 15 of 20)

| # | Parameter | Platform | Settings |
|---|---|---|---|
| | **GPP_F0 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_F0 GPIO pin. | UP4<br>UP3 | 1.8 Volts<br>1.8 Volts |
| | **GPP_F1 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_F1 GPIO pin. | UP4<br>UP3 | 1.8 Volts<br>1.8 Volts |
| | **GPP_F2 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_F2 GPIO pin. | UP4<br>UP3 | 1.8 Volts<br>1.8 Volts |
| | **GPP_F3 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_F3 GPIO pin. | UP4<br>UP3 | 1.8 Volts<br>1.8 Volts |
| | **GPP_F4 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_F4 GPIO pin. | UP4<br>UP3 | 1.8 Volts<br>1.8 Volts |
| | **GPP_F5 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_F5 GPIO pin. | UP4<br>UP3 | 3.3 Volts<br>3.3 Volts |
| | **GPP_F6 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_F6 GPIO pin. | UP4<br>UP3 | 1.8 Volts<br>1.8 Volts |
| | **GPP_F7 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_F7 GPIO pin. | UP4<br>UP3 | 3.3 Volts<br>3.3 Volts |
| | **GPP_F8 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_F8 GPIO pin. | UP4<br>UP3 | 1.8 Volts<br>1.8 Volts |
| | **GPP_F9 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_F9 GPIO pin. | UP4<br>UP3 | 3.3 Volts<br>3.3 Volts |
| | **GPP_F10 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_F10 GPIO pin. | UP4<br>UP3 | 3.3 Volts<br>3.3 Volts |
| | **GPP_F11 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_F11 GPIO pin. | UP4<br>UP3 | 1.8 Volts<br>1.8 Volts |
| | **GPP_F12 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_F12 GPIO pin. | UP4<br>UP3 | 1.8 Volts<br>1.8 Volts |
| | **GPP_F13 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_F13 GPIO pin. | UP4<br>UP3 | 1.8 Volts<br>1.8 Volts |
| | **GPP_F14 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_F14 GPIO pin. | UP4<br>UP3 | 1.8 Volts<br>1.8 Volts |
| | **GPP_F15 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_F15 GPIO pin. | UP4<br>UP3 | 1.8 Volts<br>1.8 Volts |
| | **GPP_F16 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_F16 GPIO pin. | UP4<br>UP3 | 1.8 Volts<br>1.8 Volts |
| | **GPP_F17 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_F17 GPIO pin. | UP4<br>UP3 | 1.8 Volts<br>1.8 Volts |

## Table 2-17. - GPIO (Sheet 16 of 20)

| # | Parameter | Platform | Settings |
|---|---|---|---|
| | **GPP_F18 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_F18 GPIO pin. | UP4<br>UP3 | 1.8 Volts<br>1.8 Volts |
| | **GPP_F19 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_F19 GPIO pin. | UP4<br>UP3 | 3.3 Volts<br>3.3 Volts |
| | **GPP_F20 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_F20 GPIO pin. | UP4<br>UP3 | 3.3 Volts<br>3.3 Volts |
| | **GPP_F21 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_F21 GPIO pin. | UP4<br>UP3 | 3.3 Volts<br>3.3 Volts |
| | **GPP_F22 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_F22 GPIO pin. | UP4<br>UP3 | 3.3 Volts<br>3.3 Volts |
| | **GPP_F23 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_F23 GPIO pin. | UP4<br>UP3 | 3.3 Volts<br>3.3 Volts |

## Table 2-17. - GPIO (Sheet 17 of 20)

| | | |
|---|---|---|
| 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 |

| # | Parameter | Platform | Settings |
|---|---|---|---|
| | **GPP_H0 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_H1 GPIO pin. | UP4<br>UP3 | 3.3 Volts<br>3.3 Volts |
| | **GPP_H1 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_H2 GPIO pin. | UP4<br>UP3 | 3.3 Volts<br>3.3 Volts |
| | **GPP_H2 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_H3 GPIO pin. | UP4<br>UP3 | 3.3 Volts<br>3.3 Volts |

## Table 2-17. - GPIO (Sheet 18 of 20)

| # | Parameter | Platform | Settings |
|---|---|---|---|
| | **GPP_H3 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_H4 GPIO pin. | UP4<br>UP3 | 3.3 Volts<br>3.3 Volts |
| | **GPP_H4 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_H5 GPIO pin. | UP4<br>UP3 | 1.8 Volts<br>1.8 Volts |
| | **GPP_H5 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_H5 GPIO pin. | UP4<br>UP3 | 1.8 Volts<br>1.8 Volts |
| | **GPP_H6 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_H6 GPIO pin. | UP4<br>UP3 | 1.8 Volts<br>1.8 Volts |
| | **GPP_H7 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_H7 GPIO pin. | UP4<br>UP3 | 1.8 Volts<br>1.8 Volts |
| | **GPP_H8 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_H8 GPIO pin. | UP4<br>UP3 | 1.8 Volts<br>1.8 Volts |
| | **GPP_H9 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_H9 GPIO pin. | UP4<br>UP3 | 1.8 Volts<br>1.8 Volts |
| | **GPP_H10 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_H10 GPIO pin. | UP4<br>UP3 | 3.3 Volts<br>3.3 Volts |
| | **GPP_H11 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_H11 GPIO pin. | UP4<br>UP3 | 3.3 Volts<br>3.3 Volts |
| | **GPP_H12 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_H12 GPIO pin. | UP4<br>UP3 | 1.8 Volts<br>1.8 Volts |
| | **GPP_H13 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_H13 GPIO pin. | UP4<br>UP3 | 1.8 Volts<br>1.8 Volts |
| | **GPP_H14 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_H14 GPIO pin. | UP4<br>UP3 | 3.3 Volts<br>3.3 Volts |
| | **GPP_H15 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_H15 GPIO pin. | UP4<br>UP3 | 3.3 Volts<br>3.3 Volts |
| | **GPP_H16 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_H16 GPIO pin. | UP4<br>UP3 | 3.3 Volts<br>3.3 Volts |
| | **GPP_H17 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_H17 GPIO pin. | UP4<br>UP3 | 3.3 Volts<br>3.3 Volts |
| | **GPP_H18 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_H18 GPIO pin. | UP4<br>UP3 | 3.3 Volts<br>3.3 Volts |
| | **GPP_H19 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_H19 GPIO pin. | UP4<br>UP3 | 3.3 Volts<br>3.3 Volts |
| | **GPP_H20 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_H20 GPIO pin. | UP4<br>UP3 | 1.8 Volts<br>1.8 Volts |

## Table 2-17. - GPIO (Sheet 19 of 20)

| # | Parameter | Platform | Settings |
|---|---|---|---|
| | **GPP_H21 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_H21 GPIO pin. | UP4<br>UP3 | 1.8 Volts<br>1.8 Volts |
| | **GPP_H22 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_H22 GPIO pin. | UP4<br>UP3 | 1.8 Volts<br>1.8 Volts |
| | **GPP_H23 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_H23 GPIO pin. | UP4<br>UP3 | 3.3 Volts<br>3.3 Volts |

| | | |
|---|---|---|
| GPP_T2 Individual Voltage Select | 3.3Volts | This setting controls the VCCIO voltage for |
| GPP_T3 Individual Voltage Select | 3.3Volts | This setting controls the VCCIO voltage for |

| # | Parameter | Platform | Settings |
|---|---|---|---|
| | **GPP_T2 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_T2 GPIO pin. | UP4<br>UP3 | 3.3 Volts<br>3.3 Volts |
| | **GPP_T3 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_T3 GPIO pin. | UP4<br>UP3 | 3.3 Volts<br>3.3 Volts |

| | | |
|---|---|---|
| GPP_U4 Individual Voltage Select | 3.3Volts | This setting controls the VCCIO voltage for |
| GPP_U5 Individual Voltage Select | 3.3Volts | This setting controls the VCCIO voltage for |
| Intel(R) HD Audio Voltage Select | 1.8Volts | This setting controls configures the VCCIO |

| # | Parameter | Platform | Settings |
|---|---|---|---|
| | **GPP_U4 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_U4 GPIO pin. | UP4<br>UP3 | 3.3 Volts<br>3.3 Volts |
| | **GPP_U5 Individual Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for the GPP_U5 GPIO pin. | UP4<br>UP3 | 3.3 Volts<br>3.3 Volts |
| | **Intel® HD Audio Voltage Select**<br>**Values: 3.3Volts / 1.8Volts**<br>This setting configures the VCCIO voltage for all of the Intel® HD Audio GPIO pins. | UP4<br>UP3 | 1.8 Volts<br>1.8 Volts |

### Thunderbolt LSx/BSSB-LS Configuration

4

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

## Table 2-17. - GPIO (Sheet 20 of 20)

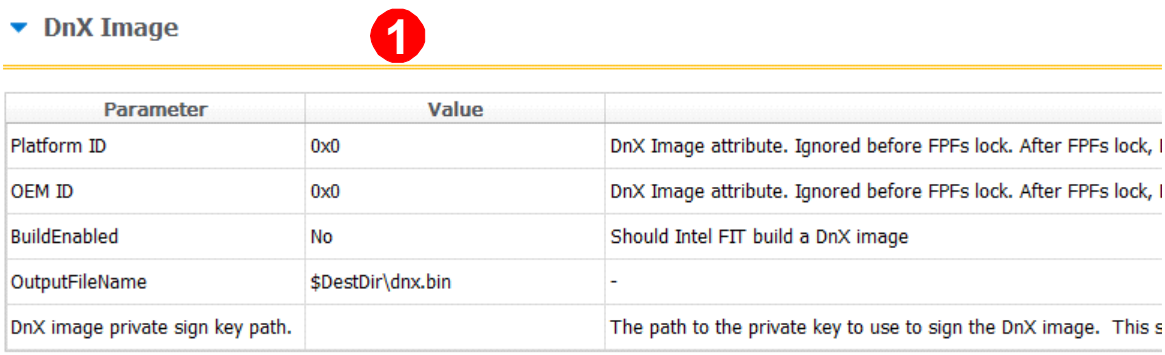
| # | Parameter | Platform | Settings |
|---|---|---|---|
| 4 | **Thunderbolt LSx/BSSB-LS Configuration** | | |
| | **Thunderbolt LSx/BSSB-LS 0 VCCIO**<br>**Values: TX VCCIO / Legacy VCCIO**<br>This setting configured Thunderbolt LSx/BSSB-LS 0 VCCIO. | UP4<br>UP3 | TX VCCIO<br>TX VCCIO |
| | **Thunderbolt LSx/BSSB-LS 1 VCCIO**<br>**Values: TX VCCIO / Legacy VCCIO**<br>This setting configured Thunderbolt LSx/BSSB-LS 0 VCCIO. | UP4<br>UP3 | TX VCCIO<br>TX VCCIO |
| | **Thunderbolt LSx/BSSB-LS 2 VCCIO**<br>**Values: TX VCCIO / Legacy VCCIO**<br>This setting configured Thunderbolt LSx/BSSB-LS 0 VCCIO. | UP4<br>UP3 | TX VCCIO<br>TX VCCIO |
| | **Thunderbolt LSx/BSSB-LS 3 VCCIO**<br>**Values: TX VCCIO / Legacy VCCIO**<br>This setting configured Thunderbolt LSx/BSSB-LS 0 VCCIO. | UP4<br>UP3 | TX VCCIO<br>TX VCCIO |

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

| | | | |
|---|---|---|---|
| **Click on Intel® Precise Touch and Stylus in the left tabs menu> Intel® Integrated Touch and Stylus Configuration is expanded by default:** | | | |
| | | | |
| **#** | **Parameter** | **Platform** | **Settings** |
| 1 | **IntegratedTouchConfiguration** | | |
| | **Intel® Precise Touch and Stylus Controller 1 Maximum Frequency**<br>**Values: 17MHz, 30MHz, 48MHz**<br>This setting allows customers to set an upper limit on the frequency for Intel® Precise Touch and Stylus transactions for the Touch Controller 1 interface. | UP4<br>UP3 | 30MHz<br>30MHz |
| | **Intel® Precise Touch and Stylus Enabled**<br>**Values: Yes / No**<br>This setting enables the Intel® Precise Touch and Stylus feature. | UP4<br>UP3 | No<br>No |

## Table 2-19. - Download and Execute

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



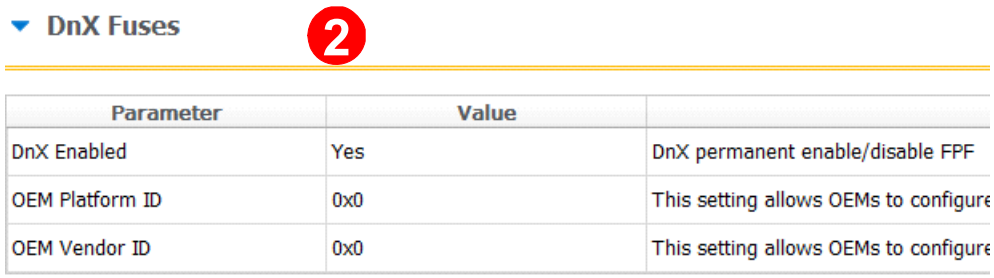
DnX Image

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

| # | Parameter | Platform | Settings |
|---|---|---|---|
| 1 | **Dnx Image** | | |
| | **Platform ID**<br>**Value: Hex**<br>This configures the Platform ID that DnX uses to verify the image is correct for the platform. Before FPFs are fused, this field is ignored and DnX will accept any image. After FPS lock, only images with this Platform ID will be accepted by DnX.<br>***Caution:*** Ensure that the Platform ID value is correctly populated prior to close of manufacturing on the platform. | UP4<br>UP3 | 0<br>0 |
| | **OEM ID**<br>**Value: Hex**<br>This configures the OEM ID that DnX uses to verify the image is correct for the platform. Before FPFs fused, this field is ignored and DnX will accept any image. After FPF lock, only images with this OEM ID will be accepted by DnX.<br>***Caution:*** Ensure that the OEM ID value is correctly populated prior to close of manufacturing on the platform. | UP4<br>UP3 | 0<br>0 |
| | **BuildEnabled**<br>**Value:Binary Yes / No**<br>This setting determines if the Intel® FIT tool should build a DnX image | UP4<br>UP3 | No<br>No |
| | **OutputFileName**<br>**Value:Binary File**<br>This setting allow the OEM to designate the DnX binary name for the output file. | UP4<br>UP3 | dnx.bin<br>dnx.bin |
| | **DnX image private sign key path**<br>This designates the path to the private key to use to sign the DnX image. This setting is only configurable when OEM signing is enabled (See Platform Integrity / OemPublicKeyHash). | UP4<br>UP3 | -<br>- |

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

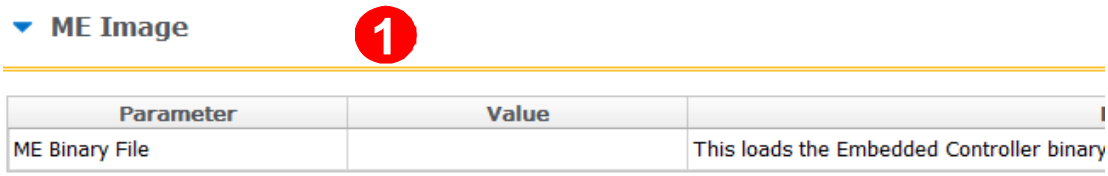
## Table 2-19. - Download and Execute




| | | | |
|---|---|---|---|
| 2 | **DnX Fuses** | | |
| | **DnX Enabled**<br>**Value: Yes / No**<br>This setting enables / disables DnX.<br>***Caution:*** Setting this option to No will permanently DnX on the platform hardware. | UP4<br>UP3 | Yes<br>Yes |
| | **Platform ID**<br>**Value: Hex**<br>This configures the Platform ID that DnX uses to verify the image is correct for the platform. Before FPFs are fused, this field is ignored and DnX will accept any image. After FPS lock, only images with this Platform ID will be accepted by DnX.<br>***Caution:*** Ensure that the Platform ID value is correctly populated prior to close of manufacturing on the platform. | UP4<br>UP3 | 0<br>0 |
| | **OEM ID**<br>**Value: Hex**<br>This configures the OEM ID that DnX uses to verify the image is correct for the platform. Before FPFs fused, this field is ignored and DnX will accept any image. After FPF lock, only images with this OEM ID will be accepted by DnX.<br>***Caution:*** Ensure that the OEM ID value is correctly populated prior to close of manufacturing on the platform. | UP4<br>UP3 | 0<br>0 |

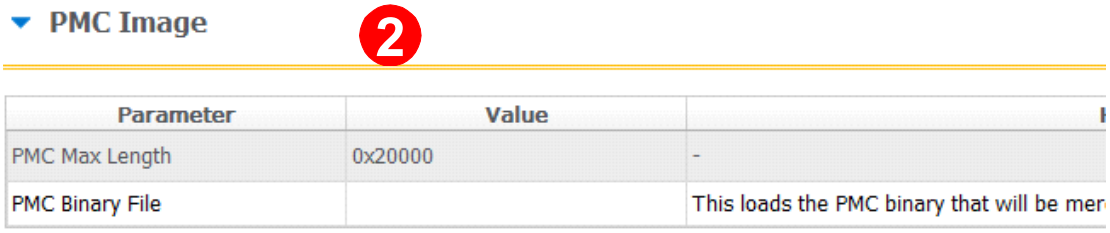
## Table 2-20. - FW Update Image Build

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



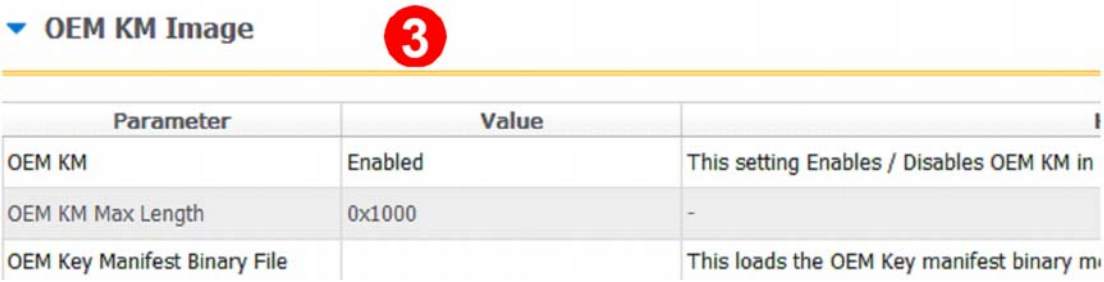

| # | Parameter | Platform | Settings |
|---|---|---|---|
| | **The FW Update Image Build tab allows users to build firmware update image binaries based on one or several of the following elements combined together:**<br><br>**Intel® ME, PMC, OEM KM, IOM, MG, TBT, ISH, iUnit, PCHC and GBST** | | |
| 1 | **ME Image** | | |
| | **ME Binary Image**<br>**Values: Binary File**<br>This loads the Embedded Controller binary that will be merged into the FWUpdate image generated by the Intel® FIT tool. | UP4<br>UP3 | ME Binary<br>ME Binary |

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

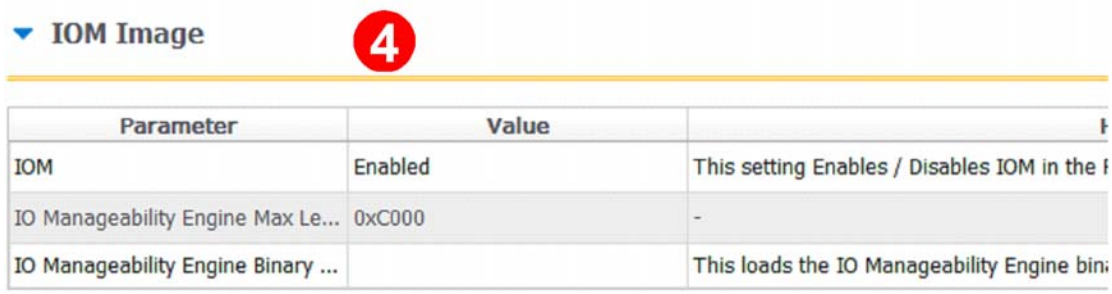
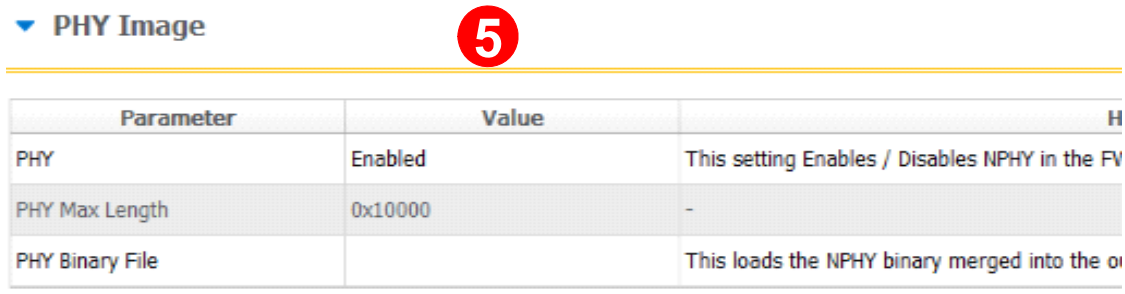



| # | Parameter | Platform | Settings |
|---|---|---|---|
| 2 | **PMC Image** | | |
| | **PMC Max Length** | | |
| | **PMC Binary Image**<br>**Values: Binary File**<br>This loads the PMC binary that will be merged into the FWUpdate image generated by the Intel® FIT tool. | UP4<br>UP3 | PMC Binary<br>PMC Binary |

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

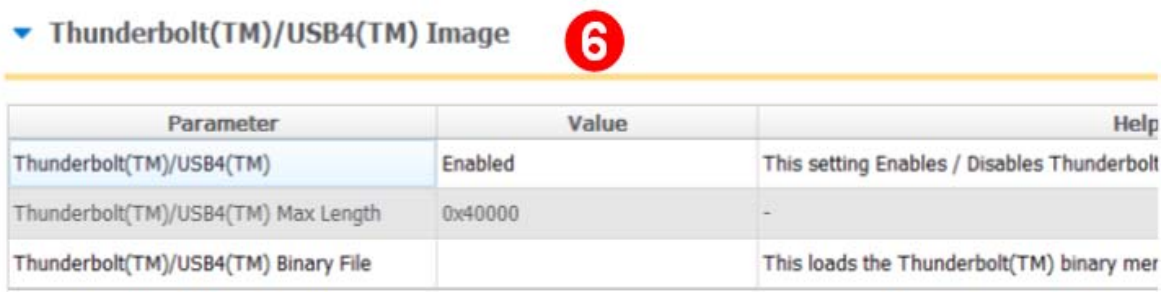


## Table 2-20. - FW Update Image Build

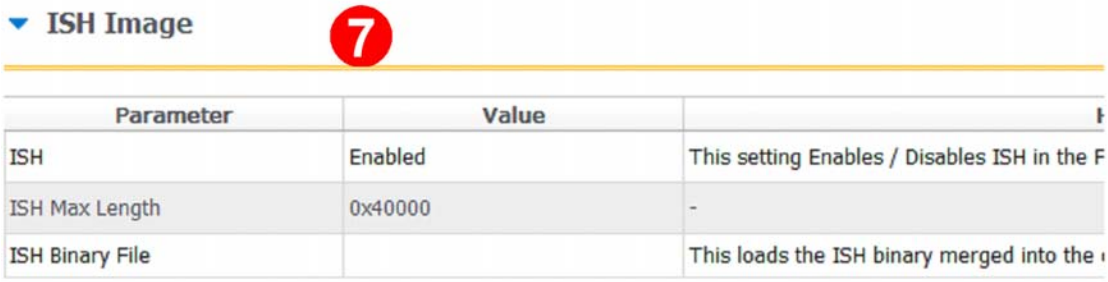
| # | Parameter | Platform | Settings |
|---|---|---|---|
| 3 | **OEM KM Image** | | |
| | **OEM KM**<br>**Values: Enabled / Disabled**<br>This setting Enables / Disables OEM KM in the FWUpdate image. | UP4<br>UP3 | Enabled<br>Enabled |
| | **OEM KM Max Length** | | |
| | **OEM Key Manifest Binary File**<br>**Values: Binary File**<br>This loads the OEM Key manifest binary merged into the output image generated by the Intel® FIT tool. | UP4<br>UP3 | OEM KM Binary<br>OEM KM Binary |
| **Click on FW Update Image Build in the left tabs menu> IOM Image is expanded by default:** | | | |
|  | | | |
| **#** | **Parameter** | **Platform** | **Settings** |
| 4 | **IOM Image** | | |
| | **IOM**<br>**Values: Enabled / Disabled**<br>This setting Enables / Disables IOM in the FWUpdate image. | UP4<br>UP3 | Enabled<br>Enabled |
| | **IO Manageability Engine Max Length** | | |
| | **IO Manageability Engine Binary File**<br>**Values: Binary File**<br>This loads the IO Manageability binary merged into the output image generated by the Intel® FIT tool. | UP4<br>UP3 | IOM Binary<br>IOM Binary |
| **Click on FW Update Image Build in the left tabs menu> MG Image is expanded by default:** | | | |
|  | | | |
| **#** | **Parameter** | **Platform** | **Settings** |

## Table 2-20. - FW Update Image Build

| | | | |
|---|---|---|---|
| 5 | **PHY Image** | | |
| | **PHY**<br>**Values: Enabled / Disabled**<br>This setting Enables / Disables NPHY in the FWUpdate image. | UP4<br>UP3 | Enabled<br>Enabled |
| | **PHY Max Length** | | |
| | **PHY Binary File**<br>**Values: Binary File**<br>This loads the NPHY binary merged into the output image generated by the Intel® FIT tool. | UP4<br>UP3 | NPHY Binary<br>NPHY Binary |
| **Click on FW Update Image Build in the left tabs menu> TBT Image is expanded by default:** | | | |



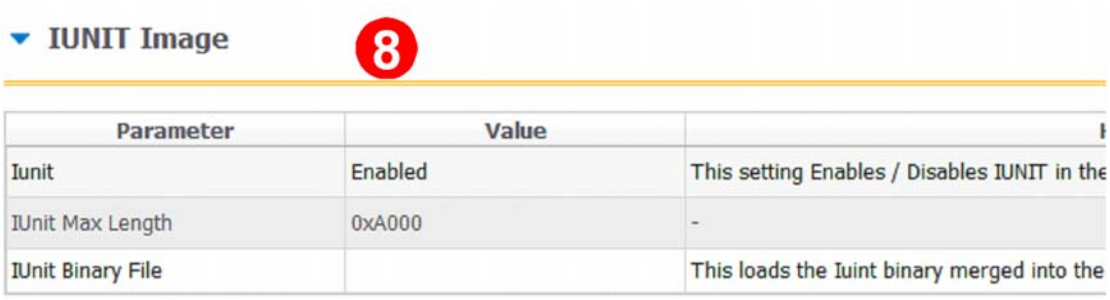

| # | Parameter | Platform | Settings |
|---|---|---|---|
| 6 | **TBT Image** | | |
| | **Thunderbolt(TM) / USB4(TM)**<br>**Values: Enabled / Disabled**<br>This setting Enables / Disables Thunderbolt(TM)/USB4(TM) in the FWUpdate image. | UP4<br>UP3 | Enabled<br>Enabled |
| | **Thunderbolt(TM) / USB4(TM) Max Length** | | |
| | **Thunderbolt(TM) / USB4(TM) Binary File**<br>**Values: Binary File**<br>This loads the Thunderbolt(TM)/USB4(TM) binary merged into the output image generated by the Intel® FIT tool. | UP4<br>UP3 | TBT Binary<br>TBT Binary |
| **Click on FW Update Image Build in the left tabs menu> ISH Image is expanded by default:** | | | |




| # | Parameter | Platform | Settings |
|---|---|---|---|
| 7 | **ISH Image** | | |

## Table 2-20. - FW Update Image Build

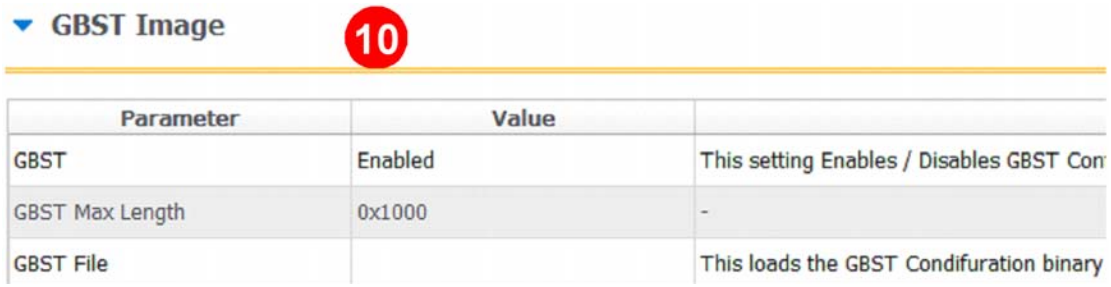
| | | | |
|---|---|---|---|
| | **ISH**<br>**Values: Enabled / Disabled**<br>This setting Enables / Disables ISH in the FWUpdate image. | UP4<br>UP3 | Enabled<br>Enabled |
| | **ISH Max Length** | | |
| | **ISH Binary File**<br>**Values: Binary File**<br>This loads the ISH binary merged into the output image generated by the Intel® FIT tool. | UP4<br>UP3 | ISH Binary<br>ISH Binary |
| **Click on FW Update Image Build in the left tabs menu> IUNIT Image is expanded by default:** | | | |




| # | Parameter | Platform | Settings |
|---|---|---|---|
| 8 | **IUNIT Image** | | |
| | **IUnit**<br>**Values: Enabled / Disabled**<br>This setting Enables / Disables IUNIT in the FWUpdate image. | UP4<br>UP3 | Enabled<br>Enabled |
| | **IUnit Max Length** | | |
| | **IUnit Binary File**<br>**Values: Binary File**<br>This loads the IUnit binary merged into the output image generated by the Intel® FIT tool. | UP4<br>UP3 | IUnit Binary<br>IUnit Binary |
| **Click on FW Update Image Build in the left tabs menu> PCHC Image is expanded by default:** | | | |

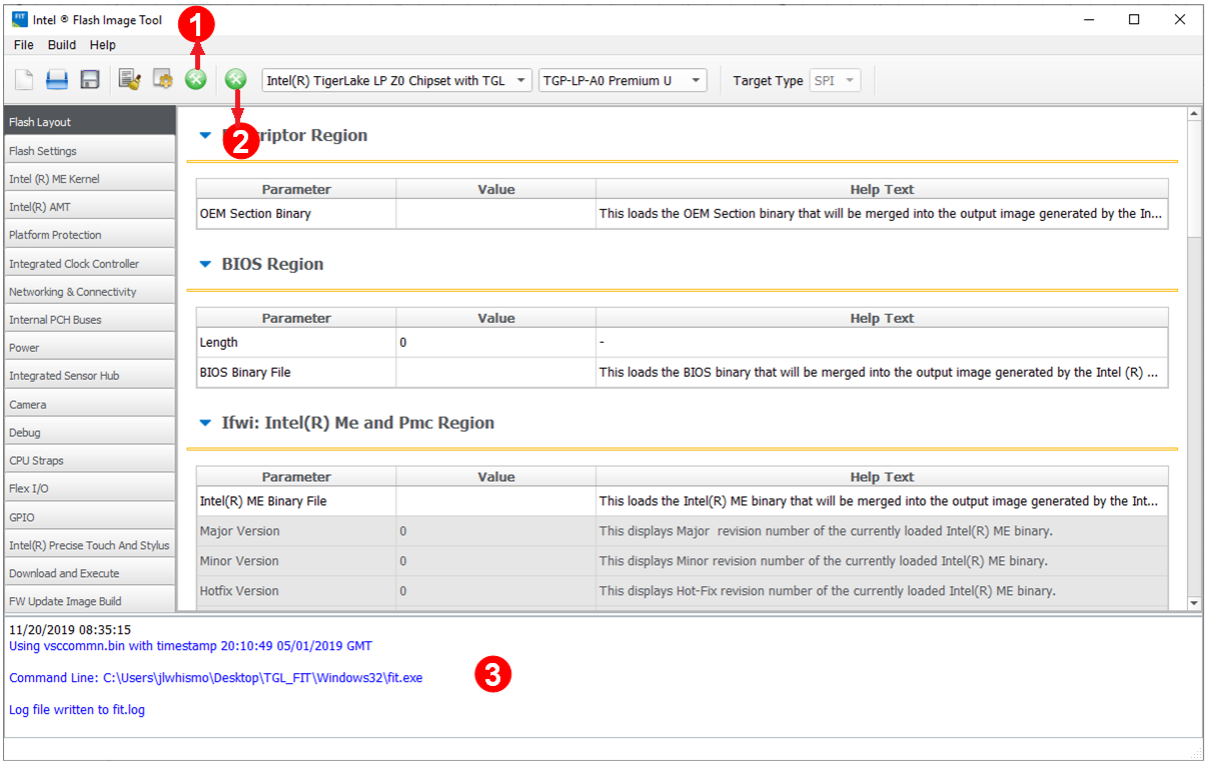
| # | Parameter | Platform | Settings |
|---|---|---|---|
| 9 | **PCHC Image** | | |
| | **PCH Configuration Max Length** | | |
| | **Values: Binary File**<br>This loads the PCHC binary merged into the output image generated by the Intel® FIT tool. | UP4<br>UP3 | PCHC Binary<br>PCHC Binary |
| **Click on FW Update Image Build in the left tabs menu> GBST Image is expanded by default:** | | | |

## Table 2-20. - FW Update Image Build




| # | Parameter | Platform | Settings |
|---|---|---|---|
| 10 | **GBST Image** | | |
| | **GBST Configuration Enable**<br>**Values: Enabled / Disabled**<br>This setting Enables / Disables GBST in the FWUpdate image. | UP4<br>UP3 | Disabled<br>Disabled |
| | **GBST Configuration Max Length** | | |
| | **Values: Binary File**<br>This loads the GBST binary merged into the output image generated by the Intel® FIT tool.<br><br>***Note:*** The GBST sub-partition is used to enabling FuSa safety standards and is not applicable for client platforms. | UP4<br>UP3 | GBST Binary (Optional)<br>GBST Binary (Optional) |

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




| | |
|---|---|
| 1 | **Green Build button**<br>Can also select CTRL+B, or Build> Build Image from the menu bar along the top of the screen |
| 2 | **Console shows status of build and path where saved** |
| 3 | **Console shows status of build and path where saved** |

# 3 Programming SPI Flash Devices and Checking Firmware Status

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

## 3.1 Flash Burner/Programmer

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

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

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

### 3.1.1 In-Circuit SPI Flash Programming for CRB

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

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

## 3.2 Flash Programming Tool (Intel® FPT)

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

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

### 3.2.1 Intel® FPT Windows* Version

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

Use the following steps to program the SPI Flash devices,

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

```
fptw.exe -i
```

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

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

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

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

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

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

```
FPT Operation Passed
```

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

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

## 3.3 Checking Intel® ME Firmware Status

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

1. Copy the file **MEInfo.exe** in the "(root)\Tools\System Tools\MEInfo\DOS" directory to the root directory of a bootable USB key.

2. Boot the target system and use F2 or Del to enter the BIOS setup menu. Load default values for BIOS (on Intel® CRBs press F3 to load default values). Save and reboot (on Intel® CRBs press F4 and select Yes).
3. Boot the target system to DOS and change to the root directory of the bootable USB key. At the DOS prompt type:

```
MEInfo.exe -fwsts
```

The system should respond with a message similar to below.

```
Intel® MEInfo Version: 15.0.0.xxxx

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

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

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

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

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

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

## 3.4 Common Bring Up Issues and Troubleshooting Table

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

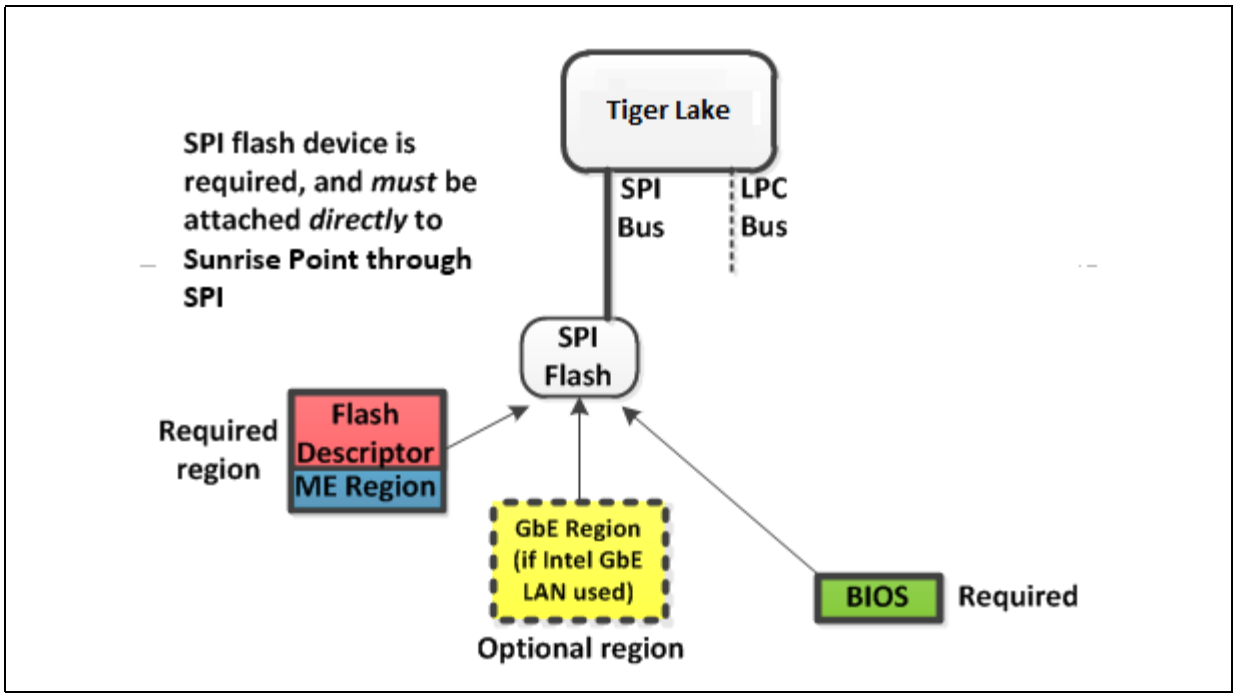
| Problem / Issue | Solution / Workaround |
|---|---|
| System does not boot to DOS | By default, the system will boot to EFI Shell. To boot to DOS,<br>1. Enter BIOS menu, then go to the 'Boot' screen<br>2. Change 'Boot Option #1' to be your USB key (ensure USB key is formatted to be DOS bootable)<br>3. Press 'F4' to save settings and reboot |
| Hear 3 beeps when platform powers on | Possible device is disconnected or device not found, check<br>• platform power and MCP fan power connectors<br>• DIMM memory modules (if applicable for memory down modules<br>• USB devices (keyboard, mouse, USB key) may be plugged into inactive USB port<br>• missing/incorrect jumpers<br>• 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:<br>• wrong FW selected during Flash image build process<br>• wrong Flash size selected<br>Re-build image with correct settings and re-flash using Flash burner. |

§ §

# A Appendix — Flash Configurations

This chapter covers only the basic information needed for clock control parameter programming. For a more detailed treatment of Mainstream - Mobile Family clocks, see Intel® *Tiger Lake PCH-H / LP Clocks* and *Intel® Converged Security and Management Engine — Platform Compliancy Guide for ME Hardware*.

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




§ §

# B Appendix — Intel® ICCS SKU Support Matrix

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

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

In below tables,

Min = Clock Div Max (minimum allowed frequency)

Max = Clock Div Min (maximum allowed frequency)

## B.1 Intel® ICCS SKU Matrix - TGP-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 - TGP-LP**

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

# C Appendix — Boot Guard Configuration

## C.1 Boot Guard Profiles

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

### Table C-1. Profile Description

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

## C.2 Enforcement Policies

### Table C-2. Enforcement Policy Description

| Error Enforcement Policy (ENF) | Enforcement Mode Name | Description |
|---|---|---|
| 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)<br><br>**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)<br><br>**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)<br><br>**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)<br><br>**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,<br>• Allowing platform to continue to boot<br>• Immediate Shutdown<br>• Shutdown with Timeout intervals<br>When the ENF logic is invoked, PTT or TPM also disconnects. | See Section C-2 for details. |

# D Appendix — Intel® Platform Trust Technology

## D.1 Intel® Platform Trust Technology

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

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

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

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

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

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

PV = Production Version

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

**Table E-1. ISH Public Key Settings**

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

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

# F Appendix — RVP Platform Specific Settings

The following table describes the configuration matrix of RVP specific settings in the Intel® FIT XML.

### Table F-1. RVP Settings

| RVP Type | Intel® FIT XML setting in StrapsDifferences section | Value |
|---|---|---|
| UP4 | PCH_Strap_SPI_ClockGateEnable_Diff | 0x1 |
| | PCH_Strap_SPI_PowerGateEnable_Diff | 0x1 |
| | PCH_Strap_DMI_DMI_CAUM_Diff | 0x1 |
| | PCH_Strap_DMI_DMI_TLPFTM_Diff | 0x1 |
| | PCH_Strap_DMI_OPDMI_PAD_Diff | 0x5 |
| | PCH_Strap_thc0_fuse_ClockGateEnable_Diff | 0x1 |
| | PCH_Strap_thc0_fuse_PowerGateEnable_Diff | 0x1 |
| | PCH_Strap_thc1_fuse_ClockGateEnable_Diff | 0x1 |
| | PCH_Strap_thc1_fuse_PowerGateEnable_Diff | 0x1 |
| | PCH_Strap_FIA_LOSL5_Diff | 0x0 |
| | PCH_Strap_FIA_LOSL4_Diff | 0x0 |
| | PCH_Strap_GBE_Xtal_clk_frequency_Diff | 0x1 |
| | PMC_Strap_pmc_smip_CPWRG_RST_WTDIS_Diff | 0x1 |
| | PMC_Strap_pmc_smip_SPE_DIS_STRAP_Diff | 0x1 |
| | PMC_Strap_pmc_smip_SPD_DIS_STRAP_Diff | 0x1 |
| | PMC_Strap_pmc_smip_TRSB_DIS_STRAP_Diff | 0x1 |
| | PMC_Strap_pmc_smip_PNCRA5_DIS_STRAP_Diff | 0x1 |
| | PMC_Strap_pmc_smip_PNCRA4_DIS_STRAP_Diff | 0x1 |
| | PMC_Strap_pmc_smip_ADC_DIS_STRAP_Diff | 0x1 |
| | PMC_Strap_pmc_smip_RTC1_DIS_STRAP_Diff | 0x1 |
| | PMC_Strap_pmc_smip_SMT6_DIS_STRAP_Diff | 0x1 |
| | PMC_Strap_pmc_smip_SMT5_DIS_STRAP_Diff | 0x1 |
| | PMC_Strap_pmc_smip_SMT4_DIS_STRAP_Diff | 0x1 |
| | PMC_Strap_pmc_smip_DTS1_DIS_STRAP_Diff | 0x1 |
| | PMC_Strap_pmc_smip_WI_SSTRAP_IVR_ENABLE_Diff | 0x1 |
| | PMC_Strap_pmc_smip_VCCIO_FIVR_DIS_Diff | 0x1 |
| | PMC_Strap_pmc_smip_DEF_CPU_BCLK_CFG_Diff | 0x2 |
| | PMC_Strap_pmc_smip_PHY_VID_Diff | 0x7 |
| | PMC_Strap_pmc_smip_vPro_Host_Enabled_Diff | 0x0 |
| | CPU_Strap_DTI_Diff | 0x28 |