

# Coffee Lake-H

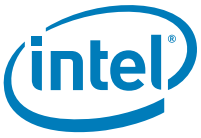
# Intel® Management Engine Firmware 12.0

## Consumer Firmware Bring Up Guide

***September 2018***

**Revision 1.6**

**Intel Confidential**



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

INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH Intel® PRODUCTS. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN INTEL'S TERMS AND CONDITIONS OF SALE FOR SUCH PRODUCTS, INTEL ASSUMES NO LIABILITY WHATSOEVER, AND 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, OFFICERS, AND EMPLOYEES OF EACH, HARMLESS AGAINST ALL CLAIMS COSTS, DAMAGES, AND EXPENSES AND REASONABLE ATTORNEYS' FEES ARISING OUT OF, DIRECTLY OR INDIRECTLY, ANY CLAIM OF PRODUCT LIABILITY, PERSONAL INJURY, OR DEATH ARISING IN ANY WAY OUT OF SUCH MISSION CRITICAL APPLICATION, WHETHER OR NOT INTEL OR ITS SUBCONTRACTOR WAS NEGLIGENT IN THE DESIGN, MANUFACTURE, OR WARNING OF THE INTEL PRODUCT OR ANY OF ITS PARTS.

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

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

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

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

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

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

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

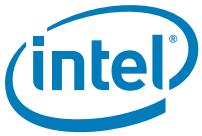
Intel processor numbers are not a measure of performance. Processor numbers differentiate features within each processor family, not across different processor families. See http://www.intel.com/products/processor_number for details. I2C is a two-wire communications bus/protocol developed by Philips.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

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

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

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

Copyright © 2014-2018, Intel Corporation. All rights reserved.



# Contents


**1 Introduction** ..... 6
- 1.1 Related Documentation ..... 6
- 1.2 Intel® ME FW Features ..... 6
- 1.3 Prerequisites ..... 6
- 1.4 Acronyms and Definitions ..... 7
  - 1.4.1 General ..... 7
  - 1.4.2 Intel® Management Engine ..... 8
  - 1.4.3 System States and Power Management ..... 9
- 1.5 Reference Documents ..... 9
- 1.6 Format and Notation ..... 9
- 1.7 Kit Contents ..... 11
- 1.8 External Hardware Requirements for Bring Up ..... 15

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

**3 Programming SPI Flash Devices and Checking Firmware Status** ..... 107
- 3.1 Flash Burner/Programmer ..... 107
  - 3.1.1 In-Circuit SPI Flash Programming for CRB ..... 107
- 3.2 Flash Programming Tool (Intel® FPT) ..... 107
  - 3.2.1 Intel® FPT Windows* Version ..... 108
- 3.3 Checking Intel® ME Firmware Status ..... 109
- 3.4 Common Bring Up Issues and Troubleshooting Table ..... 111

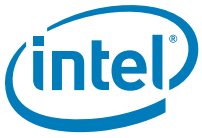
**A Appendix — Flash Configurations** ..... 112

**B Appendix — Intel® ICCS SKU Support Matrix** ..... 115
- B.1 Intel® ICCS SKU Matrix - CNP-H ..... 115
- B.2 How to configure CLKREQ# parameters ..... 116

**C Appendix — Boot Guard Configuration** ..... 117
- C.1 Boot Guard Profiles ..... 117
- C.2 Enforcement Policies ..... 117
- C.3 OEM Profile Parameters ..... 118

**D Appendix — Intel® Platform Trust Technology** ..... 119
- D.1 Intel® Platform Trust Technology ..... 119

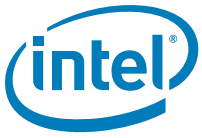
**E Appendix — Integrated Sensor Hub (ISH) Public Key Settings** ..... 120



## Figures

## Tables

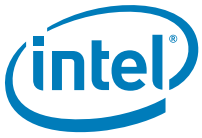

1-1 Number Format Notation ..... 10
1-2 Data Format Notation ..... 10
1-3 Kit Contents ..... 11
2-1 - Initial Screen Layout ..... 17
2-2 - Build Settings ..... 26
2-3 - Flash Layout ..... 28
2-4 - Flash Settings ..... 33
2-5 - Intel® ME Kernel ..... 42
2-6 - Intel® AMT ..... 45
2-7 - Platform Protection ..... 53
2-8 - Integrated Clock Controller ..... 58
2-9 - Networking & Connectivity ..... 68
2-10- Internal PCH Buses ..... 70
2-11- Power ..... 75
2-12- Integrated Sensor Hub ..... 77
2-13- Debug ..... 79
2-14- CPU Straps ..... 85
2-15- Flex I/O Straps ..... 88
2-16- GPIO ..... 100
2-17- Intel® Precise Touch and Stylus ..... 105
2-20- Intel® FIT - Build Image ..... 106
3-1 Common Bring Up Issues and Troubleshooting Table ..... 111



# Revision History

| Document Number | Revision Number | Description | Revision Date |
|---|---|---|---|
| | 0.8 | Pre-Alpha Release: See change bars on the left side of the page. | June 2017 |
| | 0.81 | Alpha Release: See change bars on the left side of the page | August 2017 |
| | 0.9 | Beta Release: See change bars on the left side of the page | September 2017 |
| | 0.91 | Beta Release Update: See change bars on the left of the page | October 2017 |
| | 1.0 | PC Release: See change bars on the left side of the page | December 2017 |
| | 1.1 | PC Release Update: See Change bars on the left side of the page | January 2018 |
| | 1.2 | PC Release Update 2:See change bars on left side of the page | January 2018 |
| | 1.3 | PC Release Update 3:See change bars on left side of the page | February 2018 |
| | 1.4 | PV Release: See change bars on left side of the page | May 2018 |
| | 1.5 | Added CLKOUT_CPUNSSC_P/N Clock Path Generation setting | June 2018 |
| | 1.6 | Removed Cannon Lake-H entries | September 2018 |

§ §



# 1 Introduction

This document covers the Intel® Management Engine Firmware (Intel® ME) 12.0 - 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® ME FW region — Contains firmware for the Intel® Management Engine.
- **[optional]** GbE region — Contains firmware for Intel LAN solution.

For more details on SPI Flash layout, see the document **Cannon 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# 106913 - Intel® Ethernet Network Connections (20.1 OEM Gen) - LAN Software Production Candidate 20.1

CDI # 559465 Intel® Ethernet Connection i219 [Jacksonville]

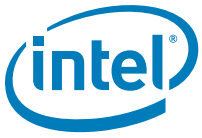
## 1.2 Intel® ME FW Features

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 customizability and soft control of “Third generation” clock solution and makes clocks available before CPU powers up.
- Silicon Workaround Capability – Intel® ME FW will have limited capabilities to perform targeted workarounds for silicon issues. **Benefit:** Allows Intel® ME FW to address some issues that otherwise would require a new silicon stepping.

## 1.3 Prerequisites

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

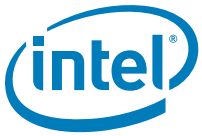
This document makes only the following limited assumptions regarding hardware:

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

## 1.4 Acronyms and Definitions

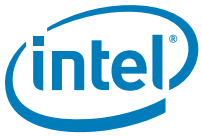
### 1.4.1 General

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



### 1.4.2 Intel® 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® Management Engine Firmware. |
| Host Service/Application | An application that is running on the host CPU |
| INF | An information file (.inf) used by Microsoft* operating systems that supports the Plug & Play feature. When installing a driver, this file provides the OS the necessary information about driver filenames, driver components, and supported hardware. |
| Intel® Management Engine Interface (Intel® MEI) | Interface between the Management Engine and the Host system |
| Intel® MEI driver | Intel® ME host driver that runs on the host and interfaces between ISV Agents and the Intel® ME HW. |
| IT User | Information Technology User. Typically very technical and uses a management console to ensure functionality of multiple PCs on a network. |
| LMS | Local Management Service: A SW application which runs on the host machine and provide a secured communication between the ISV agent and the Intel® Management Engine Firmware. |
| Intel® ME | Intel® Management Engine: The embedded processor residing in the chipset MCP |
| MECI | ME-VE Communication Interface |
| NVM | Non-Volatile Memory: A type of memory that will retain its contents even if power is removed. In the Intel® AMT current implementation, this is achieved using a FLASH memory device. |
| OOB Interface | Out Of Band interface: This is WSMAN interface over secure or non-secure TCP protocol. |
| OS not Functional | The Host OS is considered non-functional in Sx power state and any one of the following cases when system is in S0 power state:<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. |



### 1.4.3 System States and Power Management

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

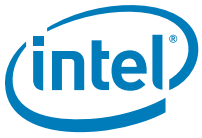
## 1.5 Reference Documents

| Document | Doc Number/ Location* |
|---|---|
| *Cannon Lake Intel® Management Engine (Intel® ME) and Embedded Controller Interaction Product Specification Revision 0.5* | 549024 / CDI |
| *Intel® Management Engine BIOS Writers Guide* | TBD / * |
| *Intel® Management Engine (Intel® ME) 11 SKU Firmware* Consumer *Compliance Guide for Cannon Lake PCH-H/LP Chipset Family - Cannon Lake Platform Compliancy and Testing Guide - Revision 1.1* | TBD / CDI |

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

## 1.6 Format and Notation

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



### Table 1-1. Number Format Notation

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

### Table 1-2. Data Format Notation

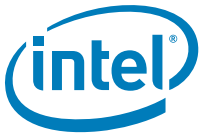
| Data Type | Notation | Size |
|---|---|---|
| Bit | b | Smallest unit, 0 or 1 |
| Byte | B | 8 bits |
| Word | W | 16 bits or 2 bytes |
| Double-word | DW | 32 bits or 4 bytes |
| Quad-word | QW | 8 bytes or 4 words |
| Kilobyte | KB | 1024 bytes |
| Megabit | Mb | 1,048,576 bits or 128 KB |
| Megabyte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

## 1.7 Kit Contents

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

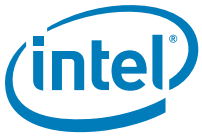
**Table 1-3. Kit Contents (Sheet 1 of 4)**

| File or [Directory] | Content Description |
|---|---|
| [root] | Root directory |
| [CNP-H] | |
| CNL-H Corporate Bring Up Guide.pdf | Firmware Bring-up for Cannon / Coffee Lake-H. |
| Coffeelake-H Client SPI Programming Guide.pdf | How to program SPI device parameters and descriptor region details. Also contains a complete SPI Flash softstrap reference. |
| [Image Components] | |
| [CSME] | |
| CSME_FW_Consumer_CNP-LP_B0_PCH.bin<br>CSME_FW_Consumer_CNP-H_A0_PCH.bin | Intel® ME firmware image (**Non Production FW**) - supports **unfused** Canonlake PCH-H Platform steppings:<br>• Unfused (Super SKU)<br><br>**Note: For PAVP Testing**, you must match Production FW with Production Part and Non Production FW with Non Production Parts. |
| [CNP-LP] | |
| Cannon Lake-LP Client SPI Programming Guide.pdf | How to program SPI device parameters and descriptor region details. Also contains a complete SPI Flash softstrap reference. |
| CNL-LP Corporate Bring Up Guide.pdf | Firmware Bring-up for Cannon / Coffee Lake-LP. |
| [Image Components] | |
| [CSME] | |
| [CNP-LP_B0] | |
| CSME_FW_Corporate_CNP-LP_B0_PCH.bin | Intel® ME firmware image (**Non Production FW Rom Bypass**) - supports **unfused** Kabylake PCH-LP Platform I/O MCP steppings:<br>• Unfused (Super SKU)<br><br>**Note: For PAVP Testing**, you must match Production FW with Production Part and Non Production FW with Non Production Parts. |
| CNPLP_B0_PMC_FW_PATCH_V6.pmc.bin | PMC patch FW that goes with the Intel® ME firmware image binary for Cannon / Coffee Lake-LP Platforms. |
| [Installers] | |
| Intel®_ME SW Installation Guide.pdf | Intel® ME Software installation Guide. |
| [ME_SW_MSI] | |
| IntelMEFWVer.dll | |
| MUP | XML file |
| SetupME | |
| [MEI-Only Installer MSI] | |
| IntelMEFWVer.dll | |



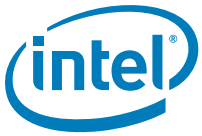
## Table 1-3. Kit Contents (Sheet 2 of 4)

| File or [Directory] | Content Description |
|---|---|
| MEISetup | |
| MUP | XML file |
| [WindowsDriverPackages] | |
| [MEI] | |
| win10 | |
| [x64] | |
| TeeDriverW8x64.sys | |
| [x86] | |
| TeeDriverW8.sys | |
| heci.cat | |
| heci.inf | |
| [SOL] | |
| mesrl.cat | |
| mesrl.inf | |
| [Tools] | |
| [ICC_Tools] | |
| Intel® ME Firmware ICC Tools User Guide.pdf | ICC Tools User Guide |
| [CCT] | |
| cct | Exe file |
| cct | Ini file |
| cctDll.dll | |
| cctWin | Exe file |
| [EFI] | |
| cct.efi | CCT for EFI |
| [System Tools] | |
| Open Watcom Public License.pdf | Sybase Open Watcom Public License version 1.0 document. |
| System Tools User Guide.pdf | System Tools User Guide |
| [Flash Image Tool] | |
| [WINDOWS] | |
| fit.exe | |
| vsccommn.bin | Binary containing the supported SPI parts |
| VSCCommn_bin Content.pdf | Documentation listing the SPI parts supported by vscccommn.bin |
| [Flash Programming Tool] | |
| [DOS] | |
| fparts.txt | List of supported SPI Flash devices with specific Flash parameters |
| fpt.exe | Intel® FPT for DOS |
| [EFI64] | |



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

| File or [Directory] | Content Description |
|---|---|
| fparts.txt | List of supported SPI Flash devices with specific Flash parameters |
| fpt.efi | Intel® FPT for EFI |
| [Windows] | |
| fparts.txt | List of supported SPI Flash devices with specific Flash parameters |
| fptw.exe | Intel® FPT for Windows* |
| Idrvdll.dll | |
| Pmxdll.dll | |
| [Windows64] | |
| fparts.txt | List of supported SPI Flash devices with specific Flash parameters |
| fptw64.exe | Intel® FPT for Windows* (64-bit) OS |
| Idrvdll32e.dll | |
| Pmxdll32e.dll | |
| [FWUpdate] | |
| [EFI64] | |
| FWUpdLcl.efi | FW Update Tool (EFI version) |
| [DOS] | |
| FWUpdLcl.exe | FW Update Tool (DOS version) |
| [Win] | |
| FWUpdLcl.exe | FW Update Tool (Windows* version 32bit) |
| [Win64] | |
| FWUpdLcl64.exe | FW Update Tool (Windows* version 64bit) |
| [Manifest Extension Utility] | |
| [Win] | |
| meu.exe | Intel® Manifest Extension Utility (MEU) executable file that allows input of FW binary and outputs and independent updatable partition that is compressed and signed. |
| [MEInfo] | |
| [DOS] | |
| MEInfo.exe | Intel® ME Information Tool (DOS version) |
| [EFI64] | |
| MEInfo.efi | Intel® ME Information Tool (EFI version) |
| [Windows] | |
| MEInfoWin.exe | Intel® ME Information Tool (Windows* version 32bit) |
| Idrvdll.dll | |
| Pmxdll.dll | |
| ISHLib.dll | |
| [Windows64] | |



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

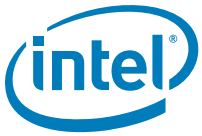
| File or [Directory] | Content Description |
|---|---|
| MEInfoWin64.exe | Intel® ME Information Tool (Windows* version 64bit) |
| Idrvdll32e.dll | |
| ISHLib.dll | |
| Pmxdll32e.dll | |
| [MEManuf] | |
| [DOS] | |
| MEManuf.exe | Intel® ME Manufacturing Tool (DOS version) |
| vsccommn.bin | Binary containing the supported SPI parts |
| VSCCommn_bin Content.pdf | Documentation listing the SPI parts supported by vscccommn.bin |
| [EFI64] | |
| VSCCommn_bin Content.pdf | Documentation listing the SPI parts supported by vscccommn.bin |
| MEManuf.efi | Intel® ME Manufacturing Tool (EFI version) |
| vsccommn.bin | Binary containing the supported SPI parts |
| [Windows] | |
| Idrvdll.dll | |
| MEManufWin.exe | Intel® ME Manufacturing Tool (Windows* version 32bit) |
| Pmxdll.dll | |
| ISHLib.dll | |
| vsccommn.bin | Binary containing the supported SPI parts |
| VSCCommn_bin Content.pdf | Documentation listing the SPI parts supported by vscccommn.bin |
| [Windows64] | |
| Idrvdll32e.dll | |
| ISHLib.dll | |
| MEManufWin64.exe | Intel® ME Manufacturing Tool (Windows* version 64bit) |
| Pmxdll32e.dll | |
| vsccommn.bin | Binary containing the supported SPI parts |
| VSCCommn_bin Content.pdf | Documentation listing the SPI parts supported by vscccommn.bin |

## 1.8 External Hardware Requirements for Bring Up

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

| Windows* OS System | Flash Burner | DOS Bootable USB Key |
|---|---|---|
|  |  |  |
| **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.

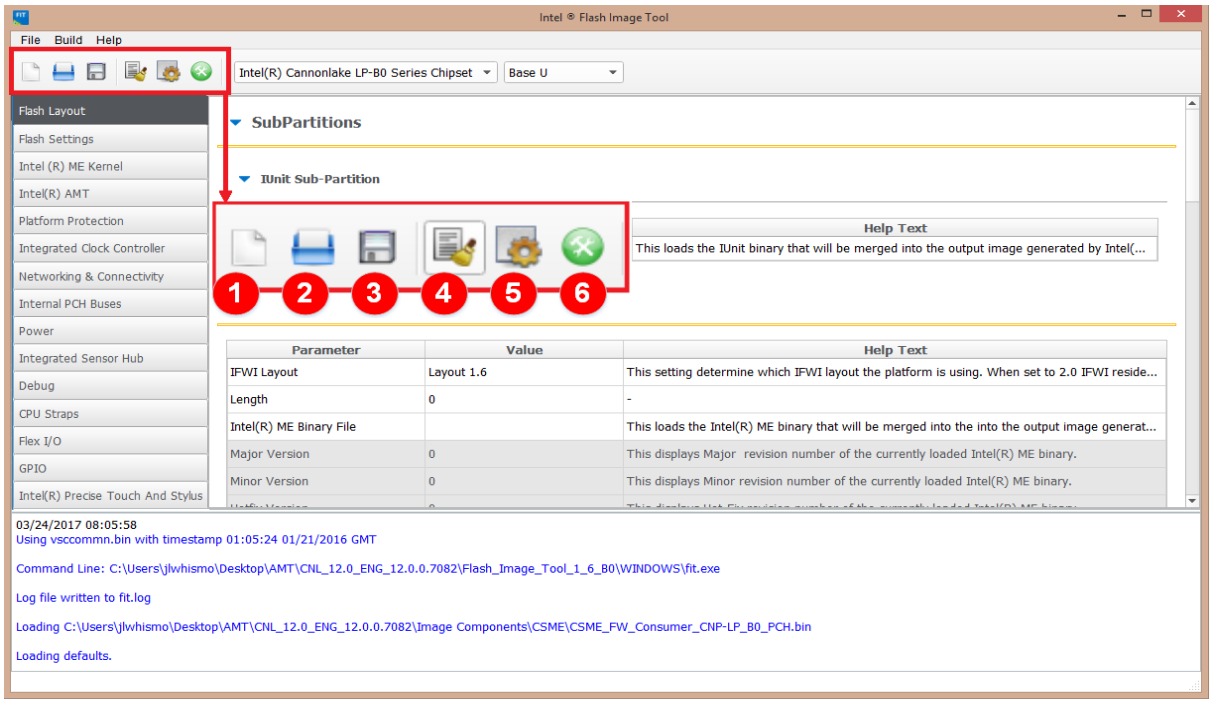
***Note:*** The Flash Image Tool may be updated throughout the release cycles. As a general rule, please ensure you use the tools, images and other content from the same kit and refrain from using different version tools.

## 2.1 Start Intel®FIT

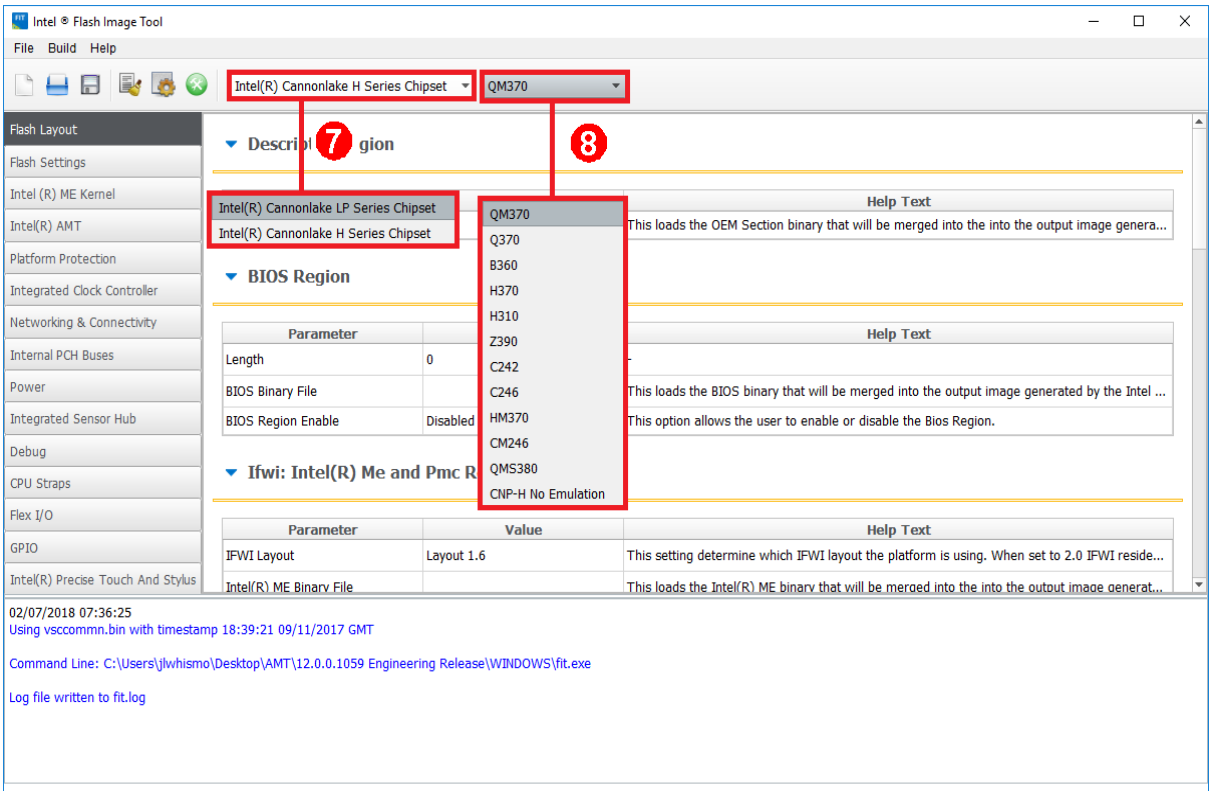
1. Invoke Intel® Flash Image Tool. Using Explorer*, navigate to **[root]\Tools\System Tools\Flash Image Tool**. Verify that the directory contents are correct (see Section 1.7). Double-click **FIT.exe**.
2. **NOTE:** In the tables below, where default settings are listed for CNL LP/H, if the value is 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

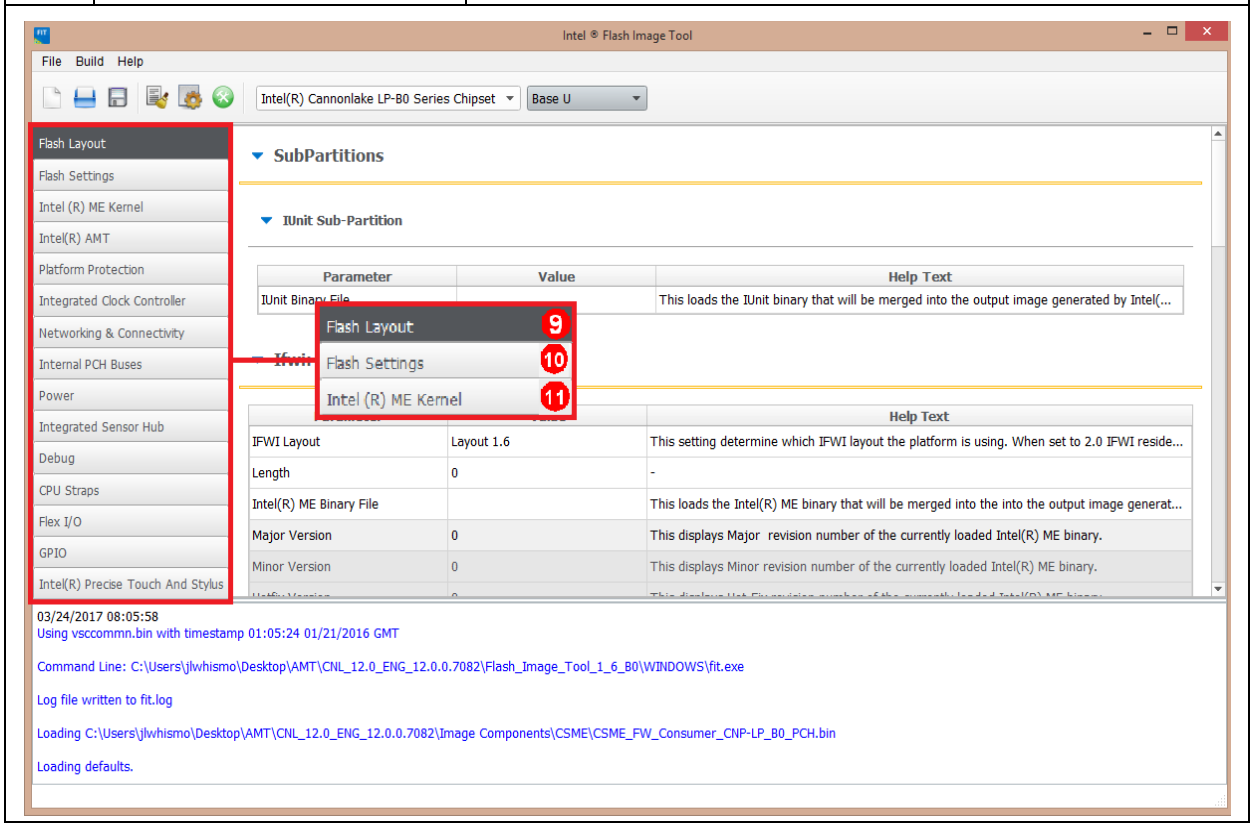
## Table 2-1. - Initial Screen Layout (Sheet 1 of 9)

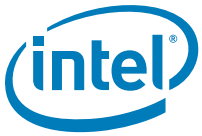
| # | Label | Contents |
|---|---|---|
|  | | |
| 1 | **New** | This button labeled ‘New’ on rollover allows opening of a new session with default values |
| 2 | **Open** | This button labeled ‘Open’ on rollover allows opening of an xml or bin file |
| 3 | **Save** | This button labeled ‘Save’ on rollover 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 |

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

| # | Label | Contents |
|---|---|---|
|  | | |
| 7 | **Drop Down Selector** | This drop down allows selection of platform |
| 8 | **Drop Down Selector** | This drop down allows selection of SKU within platform selected |

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

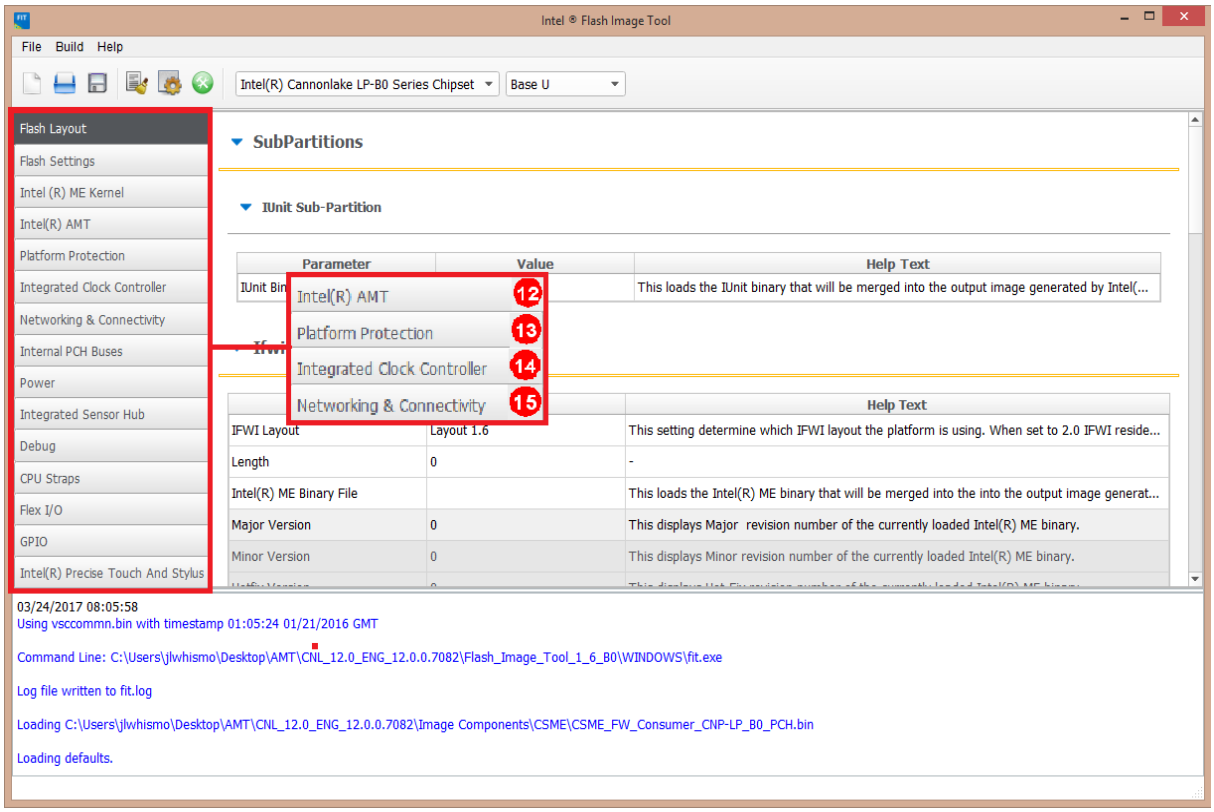
| # | Label | Contents |
|---|---|---|
| | |  |

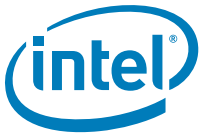


## Table 2-1. - Initial Screen Layout (Sheet 4 of 9)

| # | Label | Contents |
|---|---|---|
| 9 | **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 |
| 10 | **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>• VSCC Table - VSCC Entry<br>• BIOS Configuration |
| 11 | **Intel® ME Kernel Tab** | Intel® ME Kernel which contains (see Table 2-5):<br>• Processor<br>• Intel® ME Firmware Update<br>• Intel® Services Configuration<br>• Image Identification<br>• Firmware Diagnostics<br>• Post Manufacturing Lock<br>• MCTP Configuration<br>• Intel® ME Boot Configuration<br>• Reserved |

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

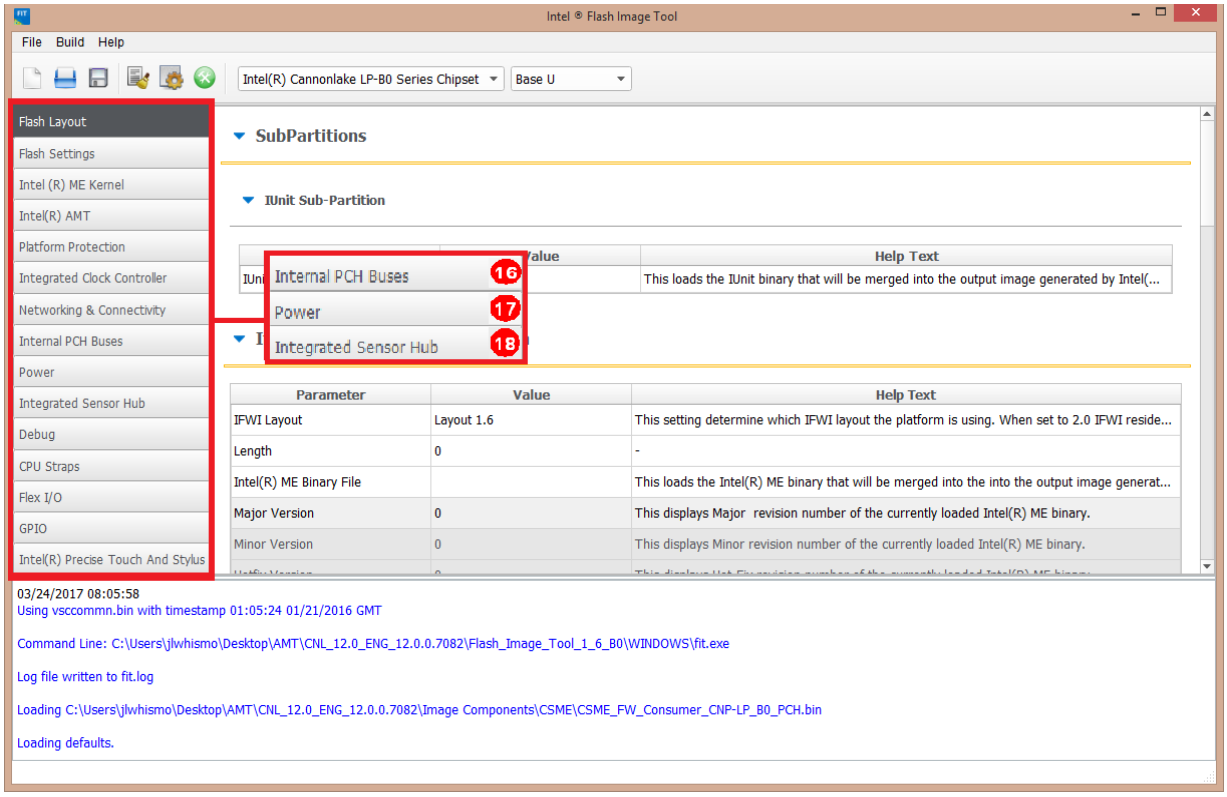
| # | Label | Contents |
|---|---|---|
|  | | |
| 12 | **Intel® AMT Tab** | Intel® AMT which contains (see Table 2-6):<br>• Intel® AMT Configuration<br>• KVM Configuration<br>• Provisioning Configuration<br>• OEM Customizable Certificates (1, 2, 3)<br>• OEM Default Certificates (1, 2, 3, 4, 5)<br>• Redirection Configuration<br>• TLS Configuration |
| 13 | **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>• Intel® PTT Configuration<br>• TPM Over SPI Bus Configuration<br>• BIOS Guard Configuration<br>• TXT Configuration |
| 14 | **Integrated Clock Controller Tab** | Integrated Clock Controller which contains (see Table 2-8):<br>• Integrated Clock Controller Policies<br>• Profiles |



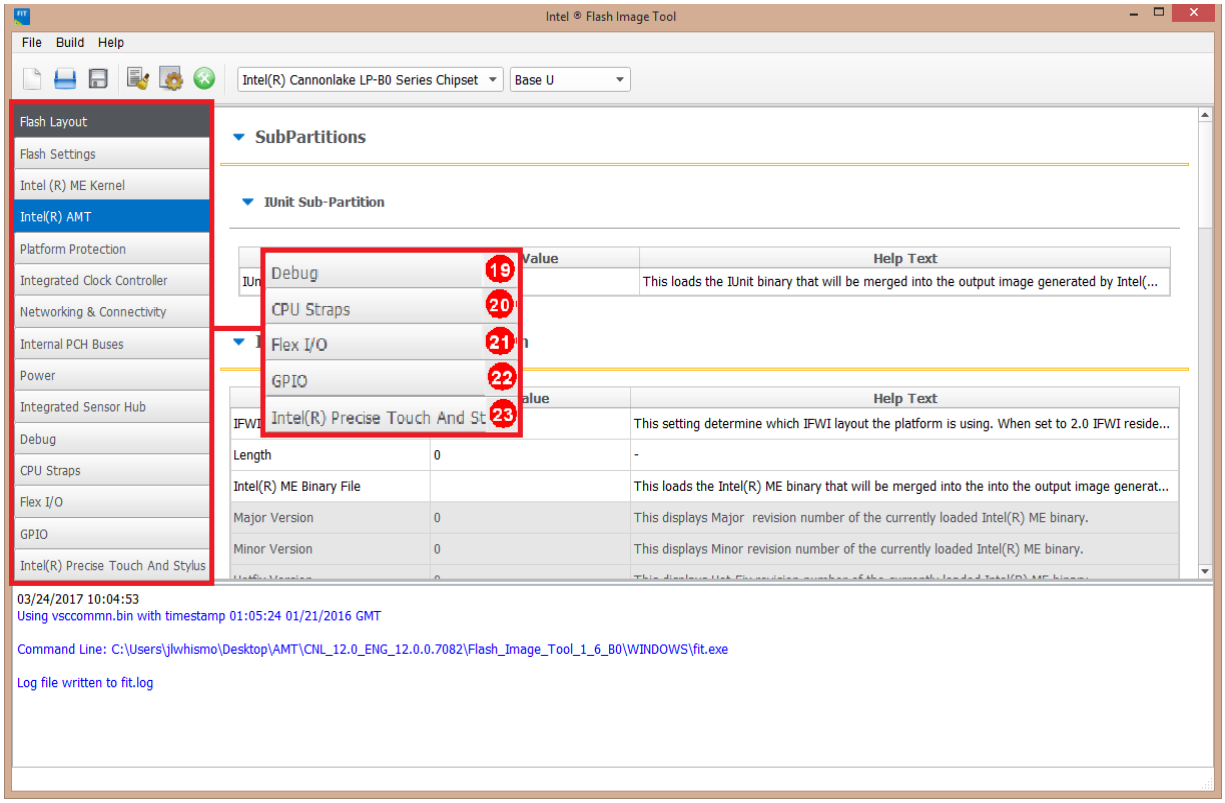
## Table 2-1. - Initial Screen Layout (Sheet 6 of 9)

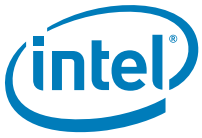
| # | Label | Contents |
|---|---|---|
| 15 | **Networking & Connectivity Tab** | Networking & Connectivity which contains (see Table 2-9):<br>• Wired LAN Configuration<br>• Wireless LAN Configuration |

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

| # | Label | Contents |
|---|---|---|
|  | | |
| 16 | **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 Configuration<br>• eSPI Configuration |
| 17 | **Power Tab** | Power which contains (see Table 2-11):<br>• Platform Power<br>• Deep Sx<br>• PCH Thermal Reporting |
| 18 | **Integrated Sensor Hub Tab** | Integrated Sensor Hub which contains (see Table 2-12):<br>• Integrated Sensor Hub<br>• ISH Image<br>• ISH Data |

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

| # | Label | Contents |
|---|---|---|
|  | | |
| 19 | **Debug Tab** | Debug which contains (see Table 2-13):<br>• IDLM<br>• Intel® Trace Hub Technology<br>• Intel® ME Firmware Debugging Overrides<br>• Direct Connection Interface Configuration<br>• Early USB DBC over Type-A Configuration<br>• eSPI Feature Overrides |
| 20 | **CPU Straps Tab** | CPU Straps which contain a detailed list of parameters (see Table 2-14)<br>• CPU Straps |
| 21 | **Flex I/O Tab** | Flex I/O which contains (see Table 2-15):<br>• Intel® RST for PCIe Configuration<br>• PCIe Lane Reversal Configuration<br>• PCIe Port Configuration<br>• SATA / PCIe Combo Port Configuration<br>• SATA / PCIe Combo Port Select Polarity<br>• USB3 Port Configuration<br>• USB2 Port Configuration |

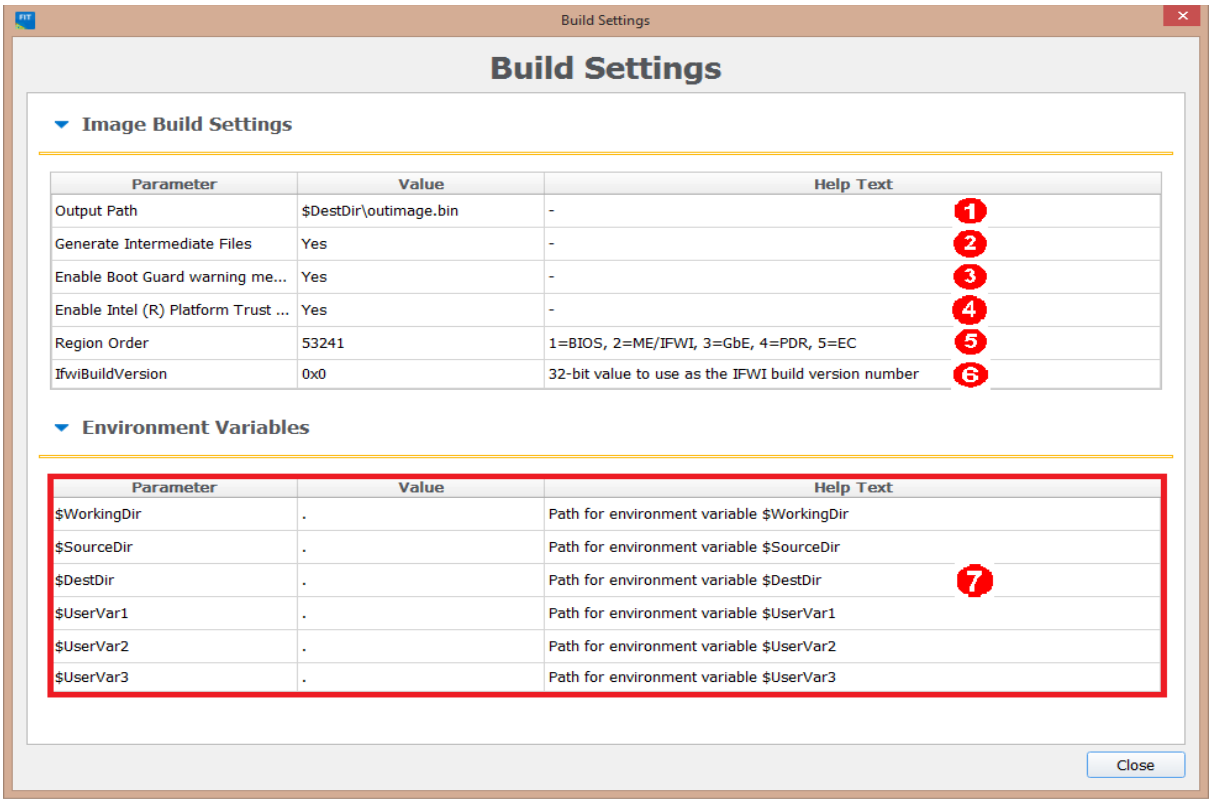


## Table 2-1. - Initial Screen Layout (Sheet 9 of 9)

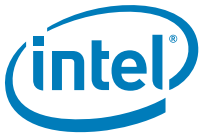
| # | Label | Contents |
|---|---|---|
| 22 | **GPIO Tab** | GPIO which contains (see Table 2-16):<br>• LAN / GPIO Select<br>• WLAN / GPIO Select<br>• Platform Power / GPIO<br>• ME Feature Pins<br>• Touch Controller Pins<br>• GPIO VCCIO Voltage Control |
| 23 | **Intel® Precise Touch and Stylus** | Intel® Precise Touch and Stylus which contains (see Table 2-17):<br>• Integrated Touch Configuration<br>• Intel® Integrated Touch and Stylus Configuration |
| | **Console Window Area** | Displays opening messages, log file entries, and build activity messages |

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

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




| # | Parameter | CRB | Values |
|---|---|---|---|
| 1 | **Output Path** | | Double click to the right of outimage.bin and click to get browse button to specify path and name of file to create for the build - default is outimage.bin in the same folder as Intel® FIT tool |
| 2 | **Generate Intermediate Files** | Yes | Yes/No - Yes is default |
| 3 | **Enable Boot Guard warning message at build time** | Yes | Yes/No - Yes is default |
| 4 | **Enable Intel(R) Platform Trust Technology warning message at build time** | Yes | Yes/No - Yes is default |

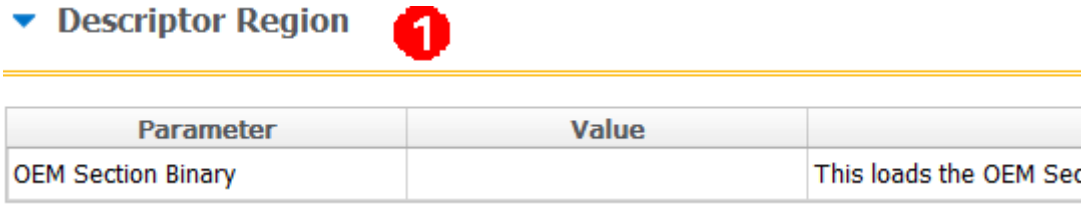


## Table 2-2. - Build Settings (Sheet 2 of 2)

| Click on Build Button in the top menu bar> Build Settings window pop up is displayed: | | | |
|---|---|---|---|
| # | Parameter | CRB | Values |
| 5 | **Region Order** | Yes | 53241 - is default |
| 6 | IFWI Build Version | Yes | 0x0 is default |
| 7 | | | $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 |

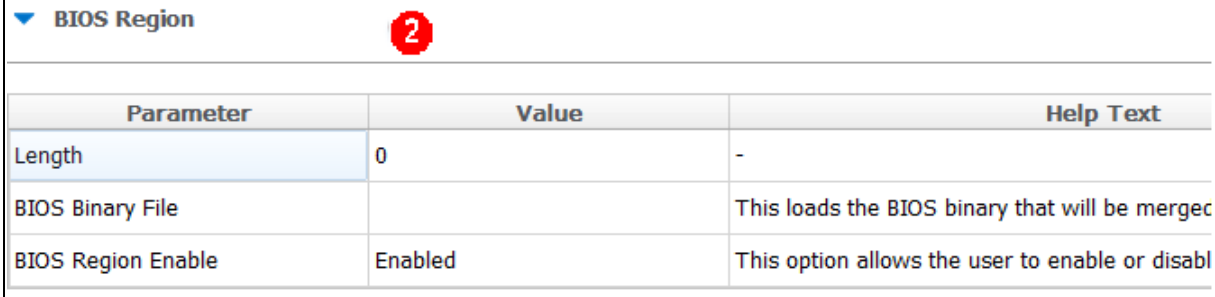
## Table 2-3. - Flash Layout (Sheet 1 of 5)

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




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

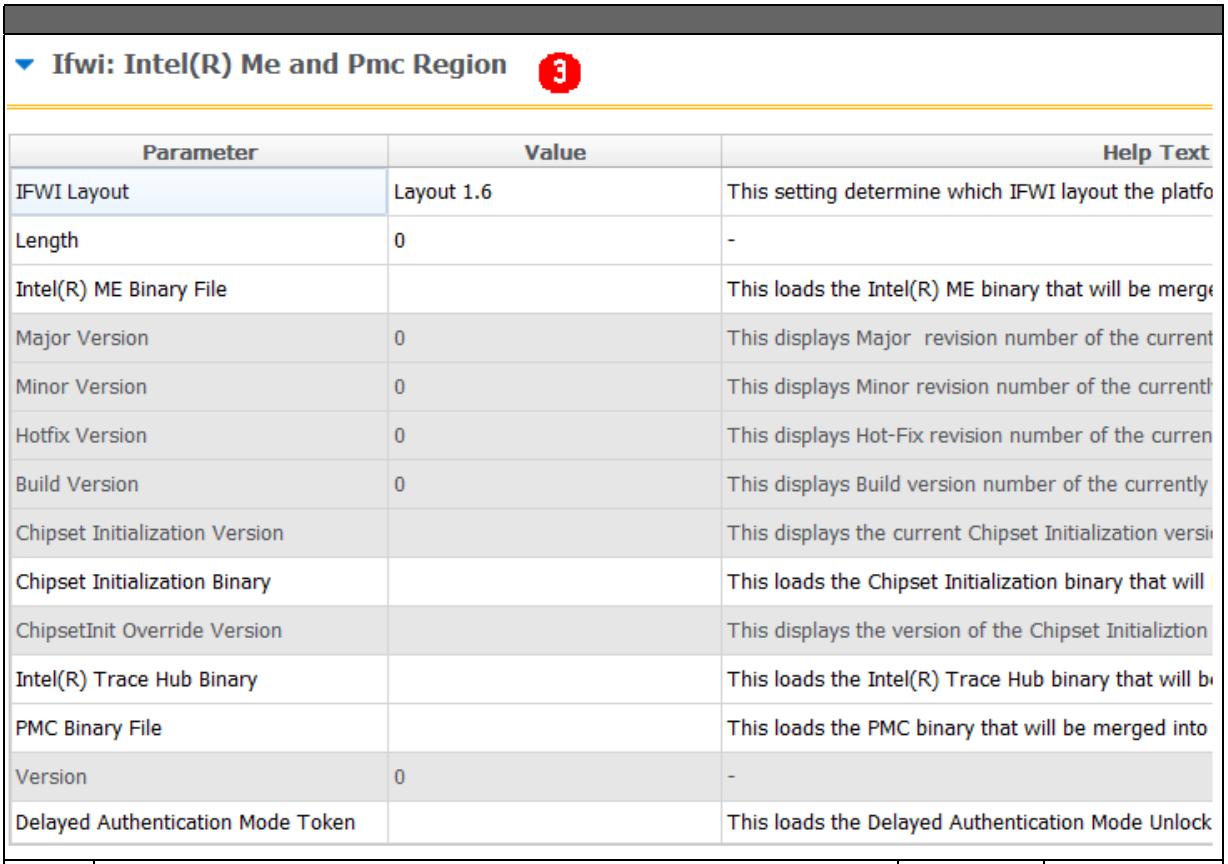
**Click on Flash Layout in the left tabs menu> BIOS Region is expanded by default:**




| # | Parameter | Platform | Settings |
|---|---|---|---|
| 2 | **BIOS Region - Length** | CFL-S<br>CFL-H | 0<br>0 |
| | **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. | CFL-S<br>CFL-H | biosimage.bin<br>biosimage.bin |
| | **BIOS Region Enable**<br>**Values: Enabled / Disabled**<br>This option allows the user to enable or disable the BIOS region.<br>**Note:** After loading bios.rom file, check that the BIOS region is enabled in tool before building image. | CFL-S<br>CFL-H | Enabled<br>Enabled |

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

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



Ifwi: Intel(R) Me and Pmc Region 3

| Parameter | Value | Help Text |
|---|---|---|
| IFWI Layout | Layout 1.6 | This setting determine which IFWI layout the platfo |
| Length | 0 | - |
| Intel(R) ME Binary File | | This loads the Intel(R) ME binary that will be merge |
| Major Version | 0 | This displays Major revision number of the current |
| Minor Version | 0 | This displays Minor revision number of the currentl |
| Hotfix Version | 0 | This displays Hot-Fix revision number of the curren |
| Build Version | 0 | This displays Build version number of the currently |
| Chipset Initialization Version | | This displays the current Chipset Initialization versi |
| Chipset Initialization Binary | | This loads the Chipset Initialization binary that will |
| ChipsetInit Override Version | | This displays the version of the Chipset Initializtion |
| Intel(R) Trace Hub Binary | | This loads the Intel(R) Trace Hub binary that will b |
| PMC Binary File | | This loads the PMC binary that will be merged into |
| Version | 0 | - |
| Delayed Authentication Mode Token | | This loads the Delayed Authentication Mode Unlock |

| | | | |
|---|---|---|---|
| 3 | **IFWI Layout** | All | Layout 1.6 |
| | **Intel® ME Binary File**<br>Navigate to your **Source Directory** (as specified in Table 2-2) and switch to the ME subdirectory. Choose the appropriate Intel **ME** Firmware binary image. This loads the Intel® ME 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® ME 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. | CFL-S<br>CFL-H | meimage.bin<br>meimage.bin |
| | **Major Version -** This displays Major revision number of the currently loaded Intel® ME binary. | | |
| | **Minor Version -** This displays Minor revision number of the currently loaded Intel® ME binary. | | |
| | **Hotfix Version -** This displays Hot-Fix revision number of the currently loaded Intel® ME binary. | | |
| | **Build Version -** This displays Build version number of the currently loaded Intel® ME binary. | | |
| | **Chipset Initialization Version -** This displays the current Chipset Initialization version contained in the currently loaded Intel® ME binary. | | |

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

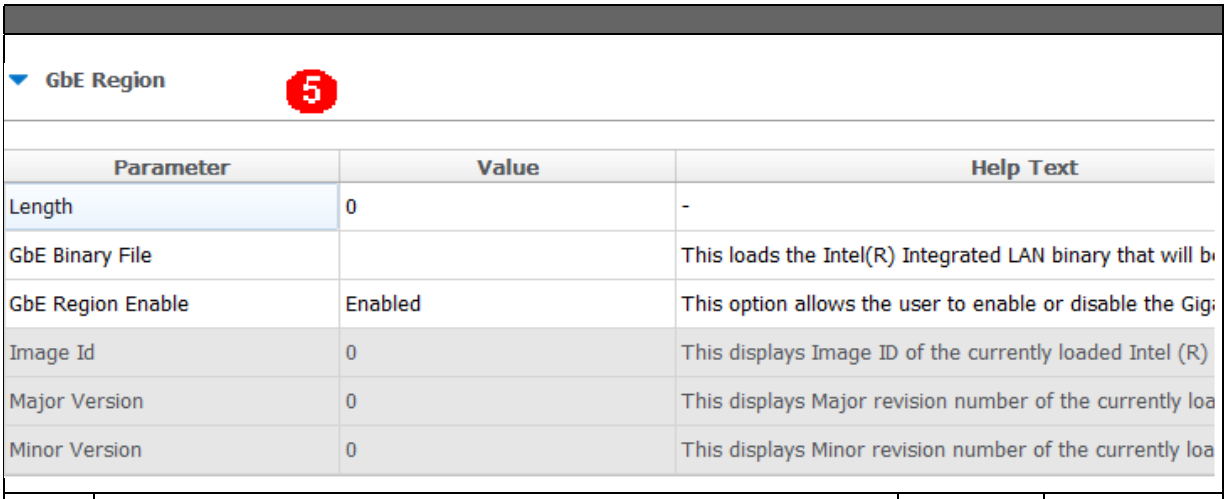
| | | | |
|---|---|---|---|
| | **Chipset Initialization Binary -** This loads the Chipset Initialization binary that will be merged into the output image generated by the Intel® FIT. If specified, this will override the version contained in the Intel® ME binary to align with the values programmed by 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. | CFL-S<br>CFL-H | 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. | CFL-S<br>CFL-H | PMC.bin<br>PMC.bin |
| | **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 - Length** | CFL-S<br>CFL-H | 0<br>0 |
| | **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. | CFL-S<br>CFL-H | 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. | CFL-S<br>CFL-H | 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 | CFL-S<br>CFL-H | Pointer Binary<br>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 5)



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 - Length**<br>**Note:** This value will be automatically populated by Intel® FIT during image build. | CFL-S<br>CFL-H | 0<br>0 |
| | **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. | CFL-S<br>CFL-H | 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><br>**NOTE:** If choosing a configuration that **does not include the GbE LAN the following settings need to be adjusted**:<br><br>**LAN Power Well: Core Well**<br>**Intel® Integrated Wired LAN Enabled: No**<br>**GbE MAC SMBus Address: No**<br>**Intel® PHY over PCIe Enabled: No**<br>**LAN PHY Power Control GDP11 Signal Configuration: Enable as GDP11** | CFL-S<br>CFL-H | Enabled<br>Enabled |

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



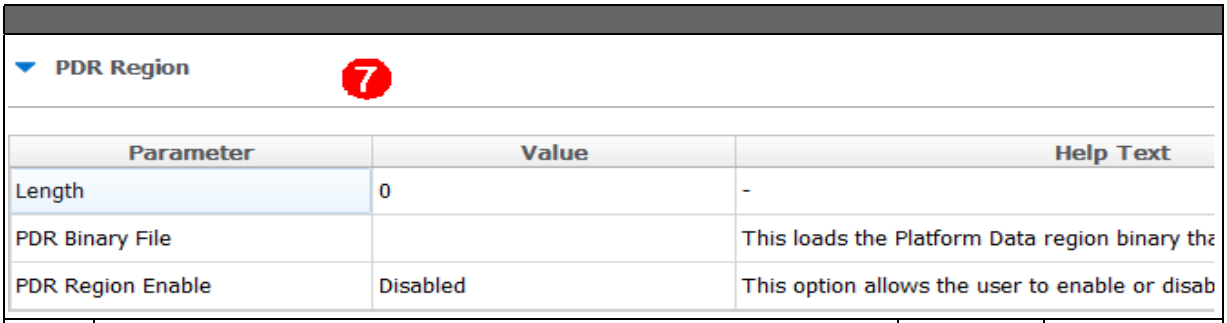
IUnit Sub-Partition 6

| Parameter | Value | Help Text |
|---|---|---|
| IUnit Binary File | | This loads the IUnit binary that will be merged into t |

| # | 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. | CFL-S<br>CFL-H | Iunit.bin (Optional)<br>Iunit.bin (Optional) |

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

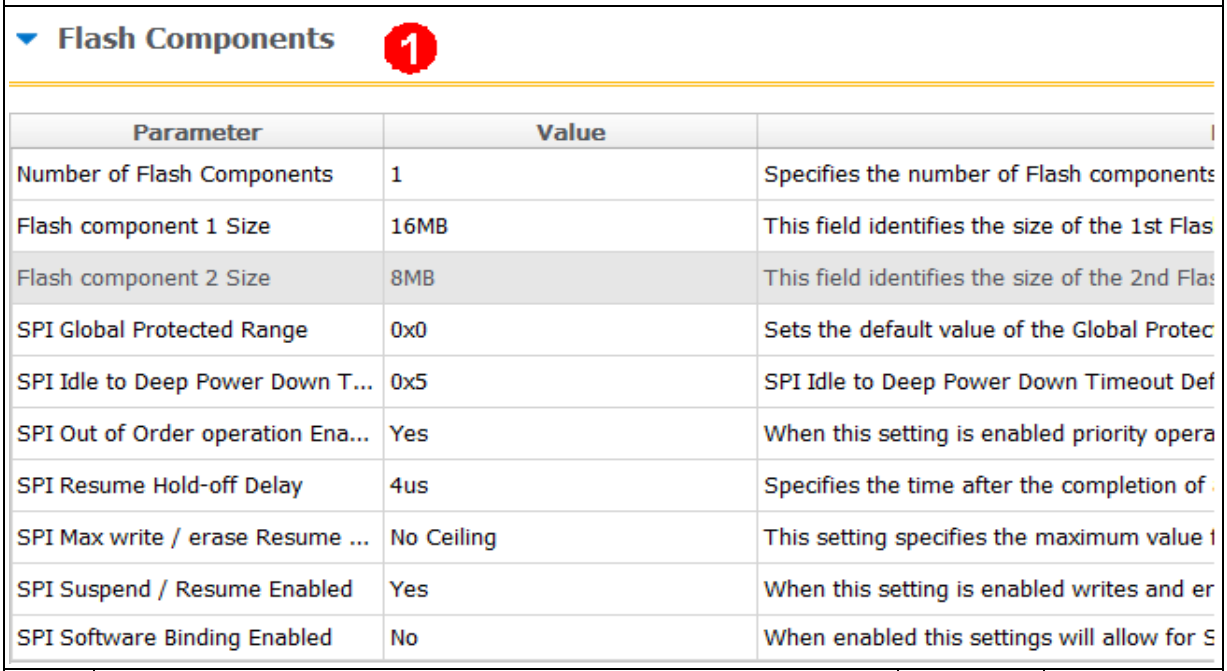
## Table 2-3. - Flash Layout (Sheet 5 of 5)




| # | Parameter | Platform | Settings |
|---|---|---|---|
| 7 | **PDR Region - Length**<br>Region is disabled by default. Displays Region size information when **Binary input file** is specified. | CFL-S<br>CFL-H | 0<br>0 |
| | **PDR Binary File**<br>Navigate to path to load pdrimage.bin file if required and available. This loads the Platform Data region binary that will be merged into the output image generated by the Intel® FIT tool. | CFL-S<br>CFL-H | 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. | CFL-S<br>CFL-H | Disabled<br>Disabled |

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

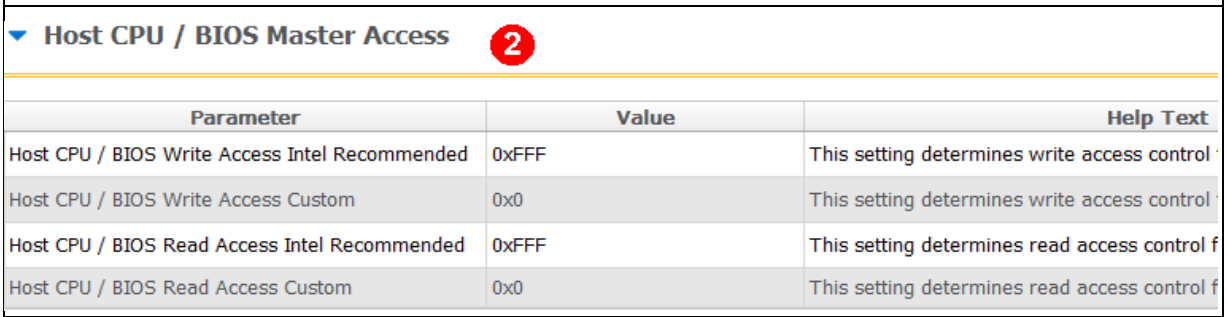
**Click on Flash Settings in the left tabs menu> Flash Components is expanded by default:**




| # | Parameter | 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. | CFL-S<br>CFL-H | 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. | CFL-S<br>CFL-H | 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'. | CFL-S<br>CFL-H | 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. | CFL-S<br>CFL-H | 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. | CFL-S<br>CFL-H | 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. | CFL-S<br>CFL-H | 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. | CFL-S<br>CFL-H | 4us<br>4us |
| | **SPI Max write / erase Resume to Suspend intervals** - This setting specifies the maximum value for the write and erase Resume to Suspend intervals. | CFL-S<br>CFL-H | No Ceiling<br>No Ceiling |

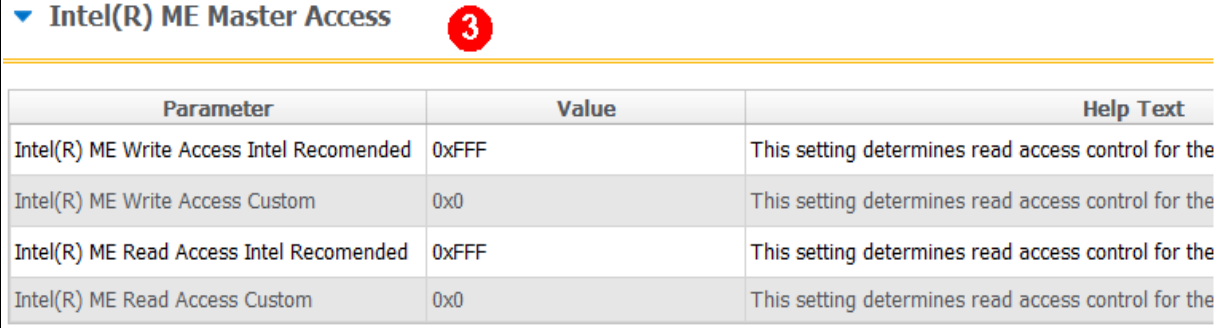
## Table 2-4. - Flash Settings (Sheet 2 of 9)

| | | | |
|---|---|---|---|
| | **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. | CFL-S<br>CFL-H | Yes<br>Yes |
| | **SPI Software Binding Enabled -** When enabled this settings will allow for SPI re-binding to a new PCH during re-manufacturing flows. | CFL-S<br>CFL-H | No<br>No |
| **Click on Flash Layout in the left tabs menu> BIOS Region is expanded by default:** | | | |



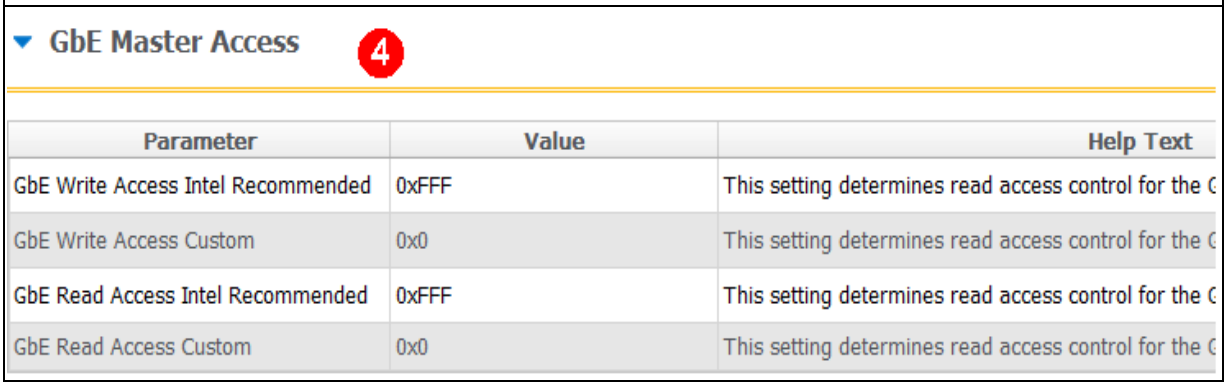

| # | Parameter | Platform | Settings |
|---|---|---|---|
| 2 | **Host CPU / BIOS Master Access** | | |
| | **Host CPU / BIOS Write Access Intel Recommended**<br>**Values: 0xFFF, 0x00A, 0x01A, 0x10A, 0x11A** - This setting determines write access control for the BIOS region.<br>**0xFFF** = Debug/Manufacturing<br>**0x00A** = Production<br>**0x01A** = Production with access to PDR (should ONLY be used if PDR region is implemented).<br>**0x10A** = Production with access to EC<br>**0x11A** = 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 Cannon Lake H SPI Programming guide further details. | CFL-S<br>CFL-H | 0xFFF<br>0xFFF |
| | **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** | CFL-S<br>CFL-H | Hex Input |
| | **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 Cannon Lake H SPI Programming guide. | CFL-S<br>CFL-H | 0xFFF<br>0xFFF |

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

| | | | |
|---|---|---|---|
| | **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** | CFL-S<br>CFL-H | Hex Input |
| **Click on Flash Settings in the left tabs menu> Intel® ME Master Access is expanded by default:** | | | |
|  | | |
| **#** | **Parameter** | **Platform** | **Settings** |
| 3 | **Intel® ME Master Access** | | |
| | **Intel® ME Write Access Intel Recommended**<br>**Values: 0xFFF, 0x004** - This setting determines write access control for the ME region.<br>**0xFFF** = Debug/Manufacturing<br>**0x004** = Production<br>**0x00C** = Production<br>**Custom** = User custom Intel® ME Write Access values<br><br>For further details on Region Access Control see Cannon Lake H SPI Programming guide further details. | CFL-S<br>CFL-H | 0xFFF<br>0xFFF |
| | **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** | CFL-S<br>CFL-H | Hex Input |
| | **Intel® ME Read Access Intel Recommended**<br>**Values: 0xFFF, 0x00D** - This setting determines read access control for the ME region.<br>**0xFFF** = Debug/Manufacturing<br>**0x00D** = Production<br>**Custom** = User custom Intel® ME Read Access values<br><br>For further details on Region Access Control see Cannon Lake H SPI Programming guide further details. | CFL-S<br>CFL-H | 0xFFF<br>0xFFF |

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

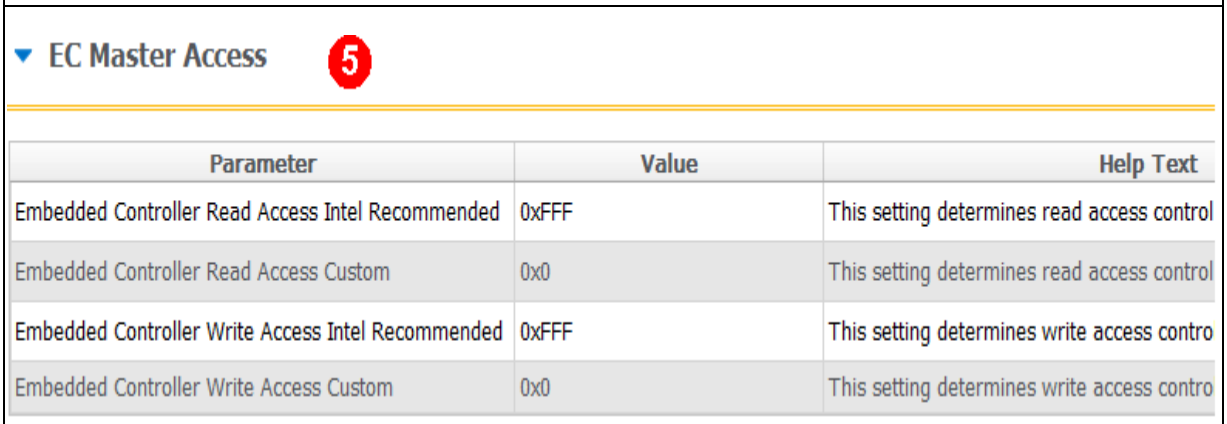
| | | | |
|---|---|---|---|
| | **Intel® ME Read Access Custom** - This setting allows free form user customized Intel® ME Read Access regions permissions<br><br>***Note:*** This setting is grayed out unless Custom is selected under the Intel® ME Read Access Intel Recommended drop down menu.<br><br>***Warning:*** **Setting region access permission values outside of Intel recommendation could result in compromised platform security** | CFL-S<br>CFL-H | Hex Input |
| **Click on Flash Settings in the left tabs menu> GbE Master Access is expanded by default:** | | | |




| # | Parameter | Platform | Settings |
|---|---|---|---|
| 4 | **GbE Master Access** | | |
| | **GbE Write Access Intel Recommended**<br>**Values: 0xFFF, 0x008** - This setting determines write access control for the Gigabit Ethernet Region.<br>**0xFFF** = Debug/Manufacturing<br>**0x008** = Production<br>**Custom** = User custom GbE Write Access values<br><br>For further details on Region Access Control see Cannon Lake H SPI Programming guide further details. | CFL-S<br>CFL-H | 0xFFF<br>0xFFF |
| | **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** | CFL-S<br>CFL-H | Hex Input |
| | **GbE Read Access Intel Recommended**<br>**Values: 0xFFF, 0x009** - This setting determines read access control for the Gigabit Ethernet Region.<br>**0xFFF** = Debug/Manufacturing<br>**0x009** = Production<br>**Custom** = User custom GbE Read Access values<br><br>For further details on Region Access Control see Cannon Lake H SPI Programming guide further details. | CFL-S<br>CFL-H | 0xFFF<br>0xFFF |

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

| | | | |
|---|---|---|---|
| | **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** | CFL-S<br>CFL-H | Hex Input |
| **Click on Flash Settings in the left tabs menu> EC Master Access is expanded by default:** | | | |

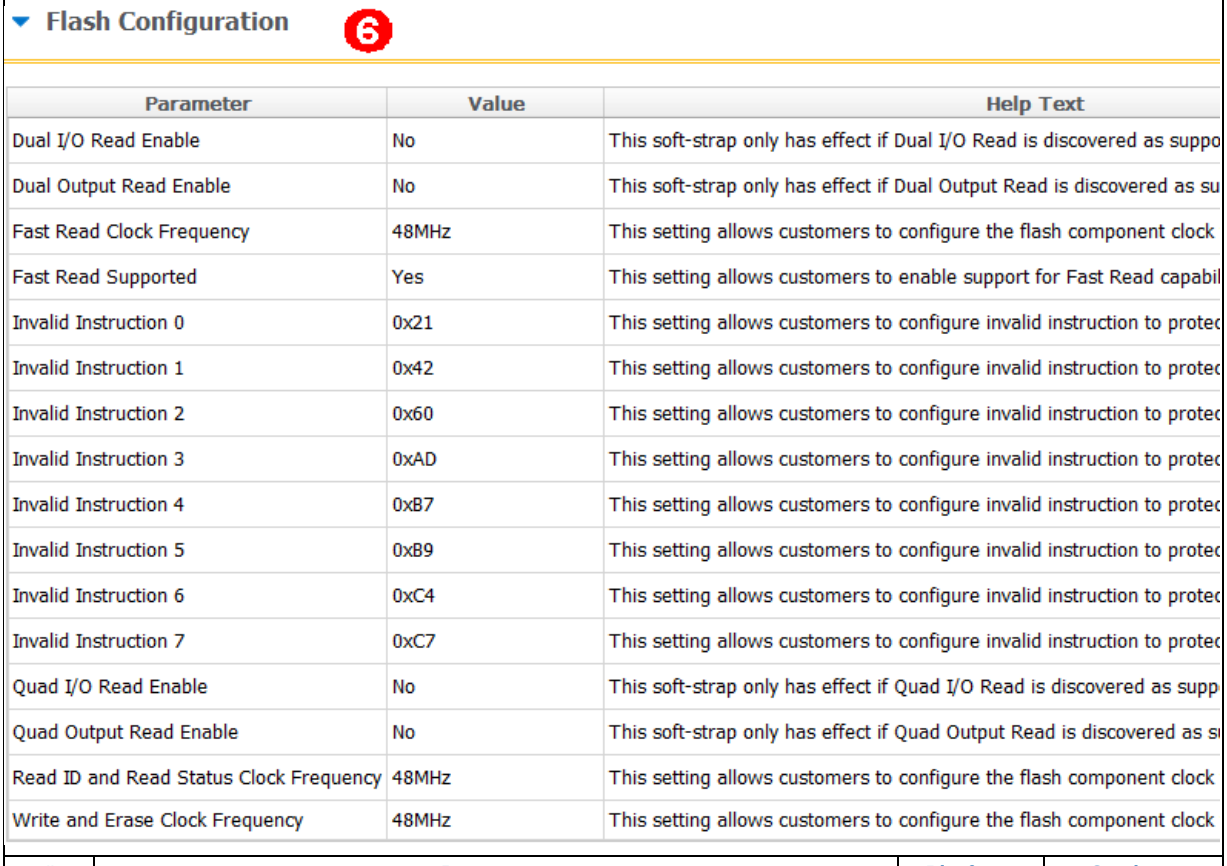



| # | Parameter | Platform | Settings |
|---|---|---|---|
| 5 | **EC Master Access** | | |
| | **EC Write Access Intel Recommended**<br>**Values: 0xFFF, 0x100** - This setting determines write access control for the Embedded Controller Region.<br>**0xFFF** = Debug/Manufacturing<br>**0x100** = Production<br>**Custom** = User custom EC Write Access values<br><br>For further details on Region Access Control see Cannon Lake H SPI Programming guide further details. | CFL-S<br>CFL-H | 0xFFF<br>0xFFF |
| | **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** | CFL-S<br>CFL-H | Hex Input |
| | **EC Read Access Intel Recommended**<br>**Values: 0xFFF, 0x101, 0x103** - This setting determines read access control for the Embedded Controller Region.<br>**0xFFF** = Debug/Manufacturing<br>**0x101 =** Production<br>**0x103** = Production with EC BIOS Read Access<br>**Custom** = User custom EC Read Access values<br><br>For further details on Region Access Control see Cannon Lake H SPI Programming guide further details. | CFL-S<br>CFL-H | 0xFFF<br>0xFFF |

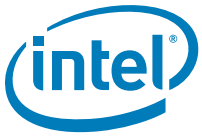
## Table 2-4. - Flash Settings (Sheet 6 of 9)

| | | | |
|---|---|---|---|
| | **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** | CFL-S<br>CFL-H | Hex Input |

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



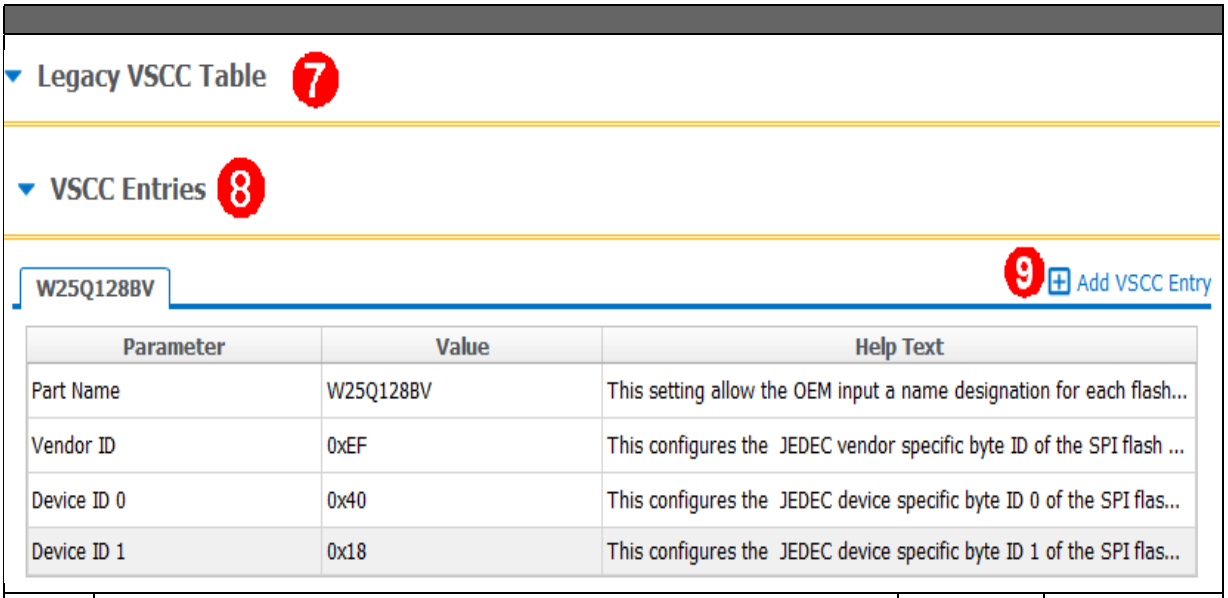

| # | Parameter | Platform | Settings |
|---|---|---|---|
| 6 | **Flash Configuration** | | |
| | **Dual I/O Read Enabled**<br>**Values: Yes/No** - This setting allows the customer to enable support for Dual I/O Read capabilities for flash components. See Cannon Lake H SPI Programming guide for further details. | CFL-S<br>CFL-H | 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 Cannon Lake H SPI Programming guide for further details. | CFL-S<br>CFL-H | Yes<br>Yes |
| | **Fast Read Clock Frequency**<br>**Values: 17MHz, 30MHz, 48MHz** - This setting allows the customer to configure the flash component clock frequency setting for Fast Read. See Cannon Lake H SPI Programming guide for further details. | CFL-S<br>CFL-H | 48MHz<br>48MHz |



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

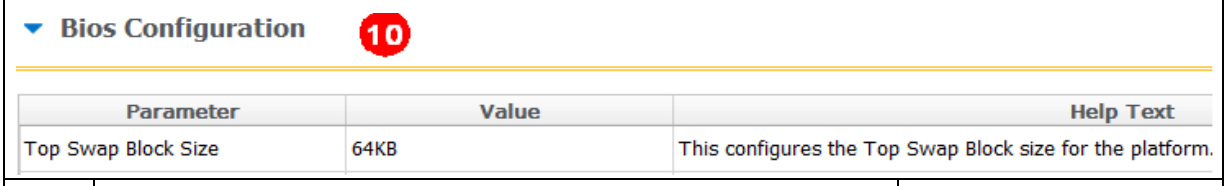
| | | | |
|---|---|---|---|
| | **Fast Read Supported**<br>**Values: Yes/No** - This setting allows the customer to enable support for Fast Read capabilities for flash components. See Cannon Lake H SPI Programming guide for further details.<br>**Note:** If fast read supported is set to **"No"** any changes 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. | CFL-S<br>CFL-H | Yes<br>Yes |
| | **Invalid Instruction 0** - This setting allows the customer to configure invalid instruction to protect against Chip Erase. See Cannon Lake H SPI Programming guide for further details. **Note:** This setting should be set to '0' if there are not Invalid instructions. | CFL-S<br>CFL-H | 0x00000021<br>0x00000021 |
| | **Invalid Instruction 1** - This setting allows the customer to configure invalid instruction to protect against Chip Erase. See Cannon Lake H SPI Programming guide for further details. **Note:** This setting should be set to '0' if there are not Invalid instructions. | CFL-S<br>CFL-H | 0x00000042<br>0x00000042 |
| | **Invalid Instruction 2** - This setting allows the customer to configure invalid instruction to protect against Chip Erase. See Cannon Lake H SPI Programming guide for further details. **Note:** This setting should be set to '0' if there are not Invalid instructions. | CFL-S<br>CFL-H | 0x00000060<br>0x00000060 |
| | **Invalid Instruction 3** - This setting allows the customer to configure invalid instruction to protect against Chip Erase. See Cannon Lake H SPI Programming guide for further details. **Note:** This setting should be set to '0' if there are not Invalid instructions. | CFL-S<br>CFL-H | 0x000000AD<br>0x000000AD |
| | **Invalid Instruction 4** - This setting allows the customer to configure invalid instruction to protect against Chip Erase. See Cannon Lake H SPI Programming guide for further details. **Note:** This setting should be set to '0' if there are not Invalid instructions. | CFL-S<br>CFL-H | 0x000000B7<br>0x000000B7 |
| | **Invalid Instruction 5** - This setting allows the customer to configure invalid instruction to protect against Chip Erase. See Cannon Lake H SPI Programming guide for further details. **Note:** This setting should be set to '0' if there are not Invalid instructions. | CFL-S<br>CFL-H | 0x000000B9<br>0x000000B9 |
| | **Invalid Instruction 6** - This setting allows the customer to configure invalid instruction to protect against Chip Erase. See Cannon Lake H SPI Programming guide for further details. **Note:** This setting should be set to '0' if there are not Invalid instructions. | CFL-S<br>CFL-H | 0x000000C4<br>0x000000C4 |
| | **Invalid Instruction 7** - This setting allows the customer to configure invalid instruction to protect against Chip Erase. See Cannon Lake H SPI Programming guide for further details. **Note:** This setting should be set to '0' if there are not Invalid instructions. | CFL-S<br>CFL-H | 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 Cannon Lake H SPI Programming guide for further details. | CFL-S<br>CFL-H | 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 Cannon Lake H SPI Programming guide for further details. | CFL-S<br>CFL-H | Yes<br>Yes |
| | **Read ID and Read Status clock frequency**<br>**Values: 17MHz, 30MHz, 48MHz** - This setting allows the customer to configure the flash component clock frequency setting for Read ID and Read Status. See Cannon Lake H SPI Programming guide for further details. | CFL-S<br>CFL-H | 48MHz<br>48MHz |
| | **Write and Erase clock frequency**<br>**Values: 17MHz, 30MHz, 48MHz** - This setting allows the customer to configure the flash component clock frequency setting for Write and Erase. See Cannon Lake / Coffee Lake H SPI Programming guide for further details. | CFL-S<br>CFL-H | 48MHz<br>48MHz |
| **Click on Flash Settings in the left tabs menu> Legacy VSCC Table is expanded by default:** | | | |

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



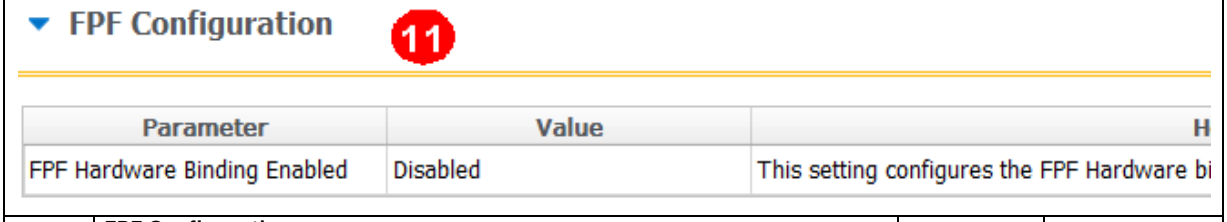

| # | Parameter | Platform | Settings |
|---|---|---|---|
| 7 | **Flash Settings - VSCC Table**<br>**VSCC Entries** | | |
| | **W25Q128BV** | | |
| 8 | **VSCC Entry** | CFL-S<br>CFL-H | |
| | **Name** - This setting allow the OEM input a name designation for each flash component being used. **Note:** This is a free form entry field it does not affect actual flash component operation. | CFL-S<br>CFL-H | Winbond<br>Winbond |
| | **Vendor ID** - This configures the JEDEC vendor specific byte ID of the SPI flash component. See Cannon Lake H SPI Programming guide for further details. | CFL-S<br>CFL-H | 0xEF<br>0xEF |
| | **Device ID 0** - This configures the JEDEC device specific byte ID 0 of the SPI flash component. See Cannon Lake H SPI Programming guide for further details. | CFL-S<br>CFL-H | 0x40<br>0x40 |
| | **Device ID 1** - This configures the JEDEC device specific byte ID 1 of the SPI flash component. See Cannon Lake H SPI Programming guide for further details. | CFL-S<br>CFL-H | 0x18<br>0x18 |
| 9 | **+ Add VSCC Entry** | | |

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



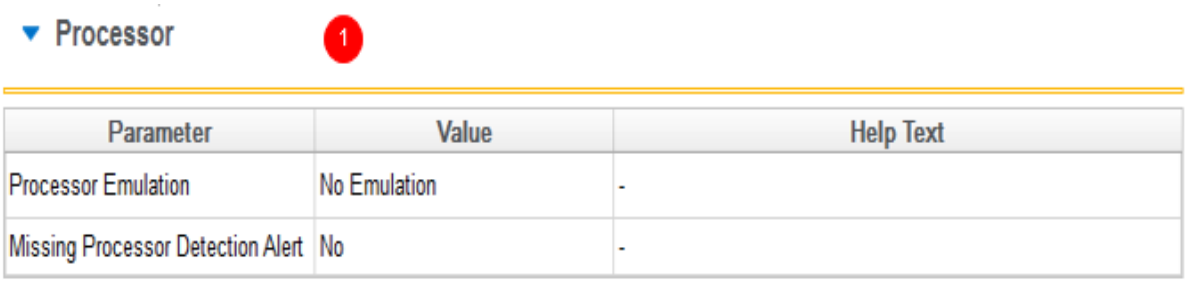

| # | Parameter | Platform |
|---|---|---|

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

| | | | |
|---|---|---|---|
| 10 | **BIOS Configuration**<br>**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 Cannon Lake H Platform Controller Hub EDS. | CFL-S<br>CFL-H | 128KB<br>128KB |
| **Click on Flash Settings in the left tabs menu> BIOS Configuration is expanded by default:** | | | |
|  | | | |
| 11 | **FPF Configuration**<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>***Note:*** For Revenue parts this setting will be ignored and FPF Hardware binding will take place when close manufacturing flow is executed. | | |
| | **FPF Hardware Binding Enabled** | CFL-S<br>CFL-H | Disabled<br>Disabled |

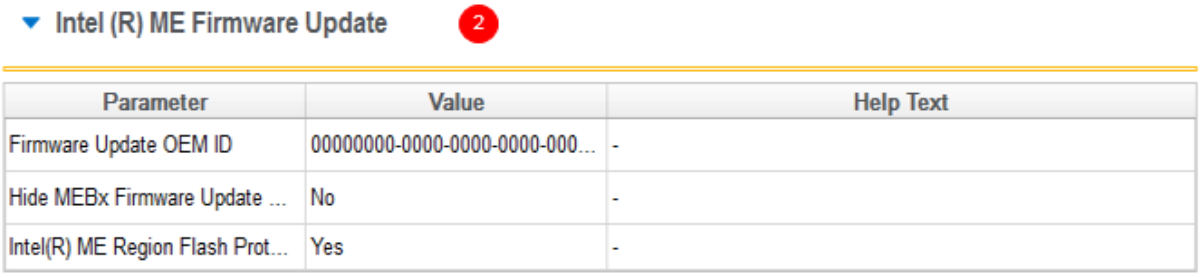
## Table 2-5. - Intel® ME Kernel (Sheet 1 of 4)

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




| # | Parameter | Platform | Settings |
|---|---|---|---|
| 1 | **Intel® ME Kernel - 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. | CFL-S<br>CFL-H | No Emulation<br>No Emulation |

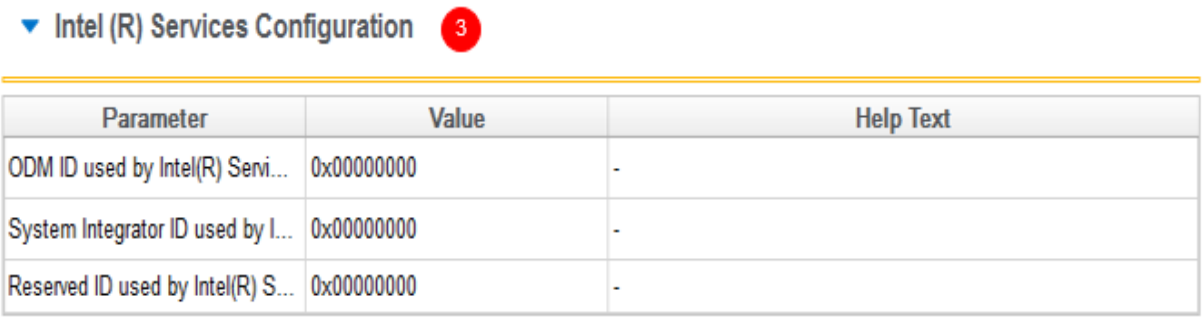
**Click on Intel® ME Kernel in the left tabs menu> Intel® ME Firmware Update is expanded by default:**




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

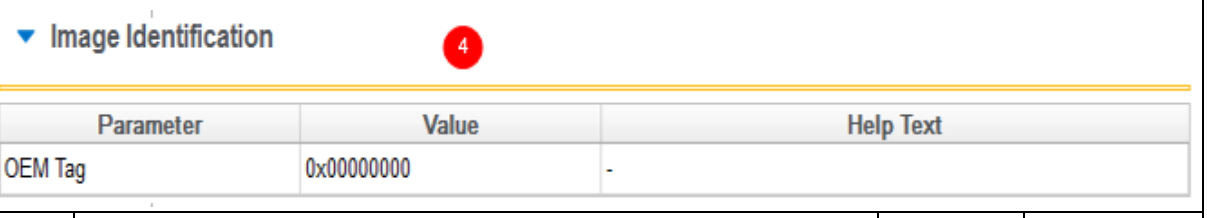
**Click on Intel® ME Kernel in the left tabs menu> Intel® ME Services Configuration is expanded by default:**

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



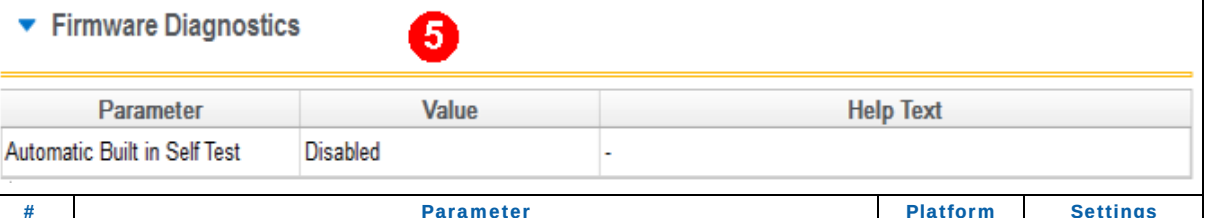

| # | Parameter | Platform | |
|---|---|---|---|
| 3 | **Intel® ME Kernel - Intel® Services Configuration** | | |
| | **ODM ID used by Intel® Services -** This setting is for entering the ODM ID for Intel® Services to identify the ODM Board builder. **Note:** This ID is either generated by or registered with Intel® Services Web servers. | CFL-S<br>CFL-H | 0x00000000<br>0x00000000 |
| | **System Integrator ID used by Intel® Services** - This setting is for entering the System Integrator ID for Intel® Services to identify the System Integrator. **Note:** This ID is either generated by or registered with Intel® Services Web servers. | CFL-S<br>CFL-H | 0x00000000<br>0x00000000 |
| | **Reserved ID used by Intel® Services** - This setting is for entering the Reserved ID for Intel® Services currently not used. | CFL-S<br>CFL-H | 0x00000000<br>0x00000000 |

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




| # | Parameter | Platform | Settings |
|---|---|---|---|
| 4 | **Intel® ME Kernel - Image Identification** | | |
| | **OEM Tag -** This is a free form 32bit field that allows the OEM to configure their own unique identifier in the firmware image. | CFL-S<br>CFL-H | 0x00000000<br>0x00000000 |

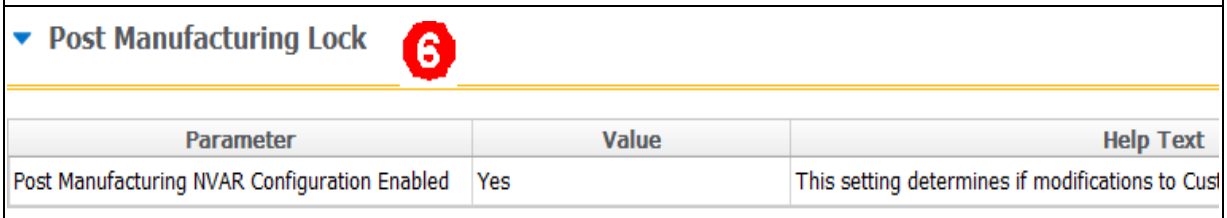
**Click on Intel® ME Kernel in the left tabs menu> Firmware Diagnostics is expanded by default:**



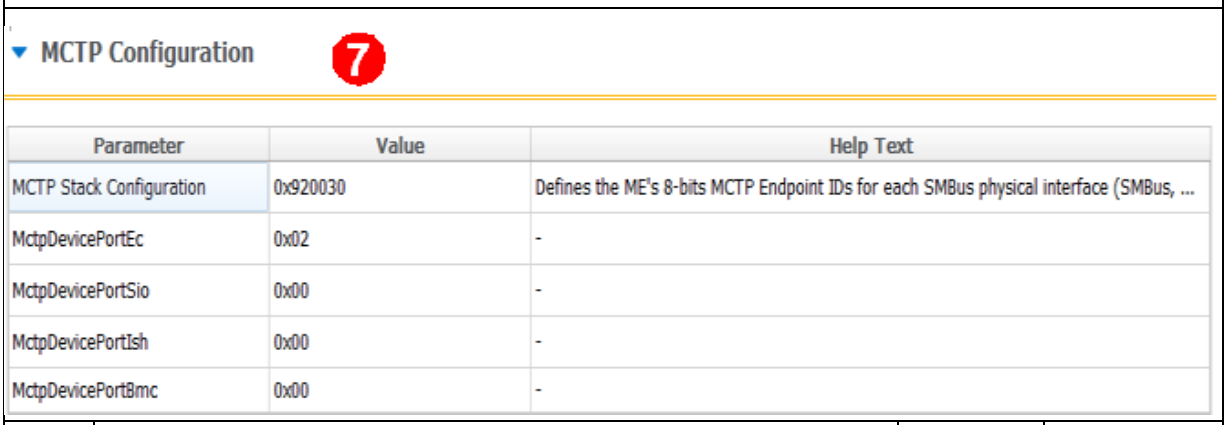

| # | Parameter | Platform | Settings |
|---|---|---|---|

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

| | | | |
|---|---|---|---|
| 5 | **Intel® ME Kernel - 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. | CFL-S<br>CFL-H | Disabled<br>Disabled |
| **Click on Intel® ME Kernel in the left tabs menu> Post Manufacturing Lock is expanded by default:** | | | |

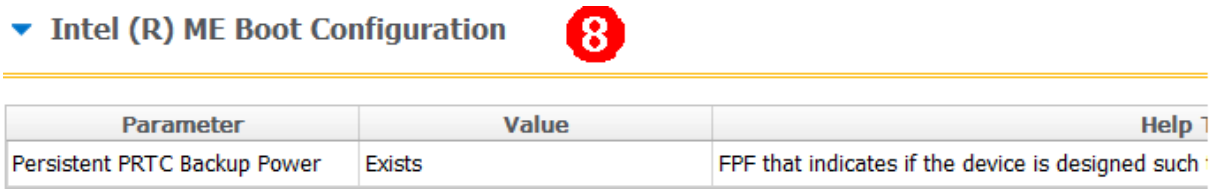
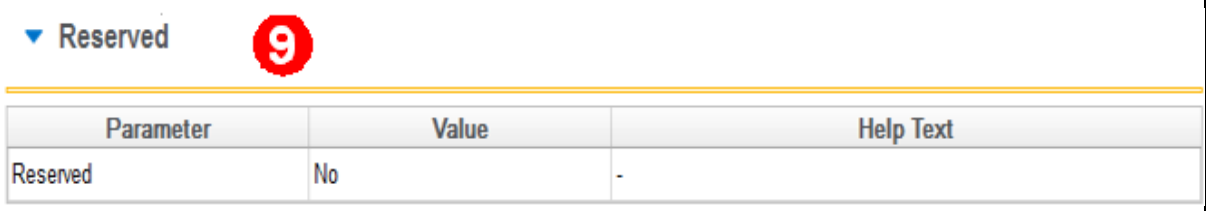



| # | Parameter | Platform | Settings |
|---|---|---|---|
| 6 | **Post Manufacturing Lock** | | |
| | **Post Manufacturing NVAR Configuration Enabled -** This setting determines if modifications to Customer configurable NVARs is to be allowed after close of manufacturing. | CFL-S<br>CFL-H | Yes<br>Yes |
| **Click on Intel® ME Kernel in the left tabs menu> MCTP Configuration is expanded by default:** | | | |




| # | Parameter | Platform | Settings |
|---|---|---|---|
| 7 | **Intel® ME Kernel - 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. | CFL-S<br>CFL-H | 0x920030<br>0x920030 |
| | **MctpDevicePortEc** | CFL-S<br>CFL-H | 0x02<br>0x02 |
| | **MctpDevicePortSio** | CFL-S<br>CFL-H | 0x00<br>0x00 |
| | **MctpDevicePortIsh** | CFL-S<br>CFL-H | 0x00<br>0x00 |

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

| | | | |
|---|---|---|---|
| | **MctpDevicePortBmc** | CFL-S<br>CFL-H | 0x00<br>0x00 |
| **Click on Intel® ME Kernel in the left tabs menu> Intel® ME Boot Configuration is expanded by default:** | | | |
|  | | | |
| **#** | **Parameter** | **Platform** | **Settings** |
| 8 | **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 | CFL-S<br>CFL-H | Exists<br>Exists |
| **Click on Intel® ME Kernel in the left tabs menu> Reserved is expanded by default:** | | | |
|  | | | |
| 9 | **Intel® ME Kernel - Reserved** | | |
| | **Reserved**<br>**Values: Yes / No** | CFL-S<br>CFL-H | No<br>No |

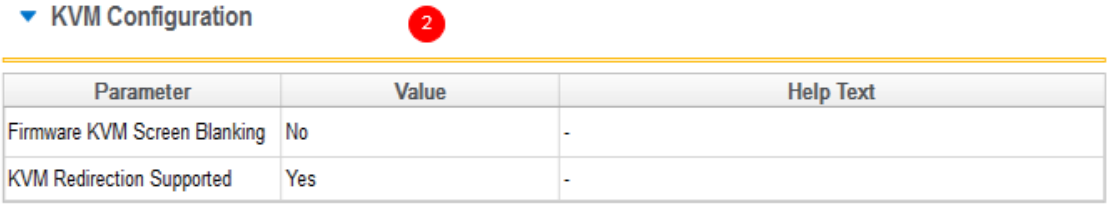
## Table 2-6. - Intel® AMT (Sheet 1 of 7)

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




| # | Parameter | Platform | Settings |
|---|---|---|---|
| 1 | **Intel® AMT - 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. **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. | CFL-S<br>CFL-H | No<br>No |
| | **Intel® ME Network Services Supported**<br>**Values: Yes / No -** This setting allows customers to enable / disable Intel® ME Network Services on the platform. **Note:** This setting and TLS needs to be enabled for proper operation of Intel® Authenticate (Corporate Only). In addition if this setting is disabled Intel® AMT will also be disabled. | CFL-S<br>CFL-H | 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. **Note:** This setting only applies to Desktop and Workstation platforms. | CFL-S<br>CFL-H | 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. **Note:** If this setting is disabled Intel® AMT or Standard Manageability can still be re-enabled through the Intel® MEBx interface. | CFL-S<br>CFL-H | Disabled<br>Disabled |
| | **Intel® AMT Idle Timeout**<br>**Values: 0xFFFF** - This setting configures the idle timeout value before Intel® AMT enters into an off state. | CFL-S<br>CFL-H | 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. **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. | CFL-S<br>CFL-H | No<br>No |

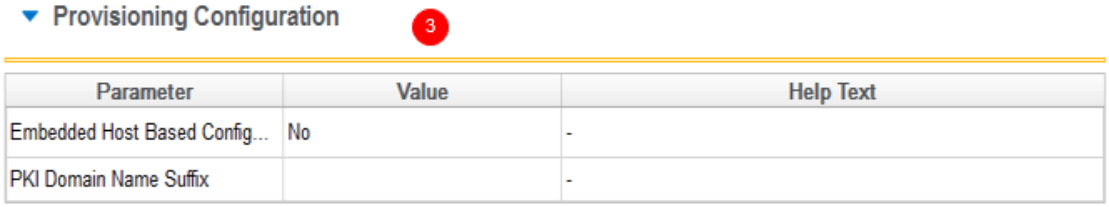
**Click on Intel® AMT in the left tabs menu> KVM Configuration is expanded by default:**



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

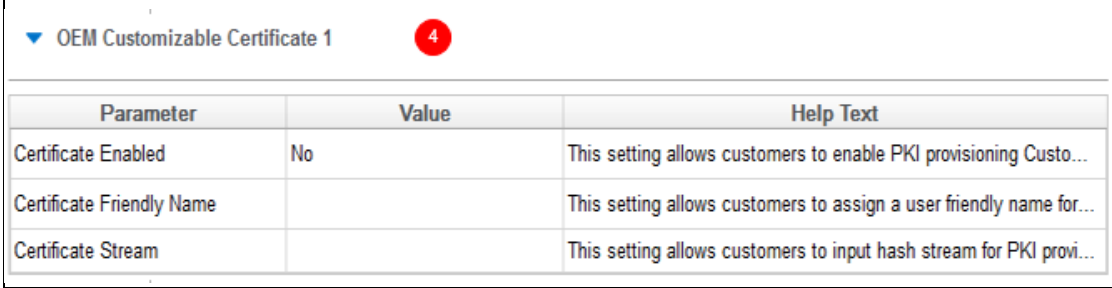
| # | Parameter | Platform | Settings |
|---|---|---|---|
| 2 | **Intel® AMT - KVM Configuration** | | |
| | **Firmware KVM Screen Blanking**<br>**Values: Yes / No -** This setting enables KVM Screen blanking capabilities in the firmware image. **Note:** This feature is dependent on processor level support.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

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




| # | Parameter | Platform | |
|---|---|---|---|
| 3 | **Intel® AMT - Provisioning Configuration** | | |
| | **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>**Note:** The Intel® FIT tool will not adjust the Redirection Privacy/Security value based on selection here. Please set security level as needed. | CFL-S<br>CFL-H | 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. **Note:** For normal out-of-box provisioning functionality this setting should be left empty. | CFL-S<br>CFL-H | -<br>- |

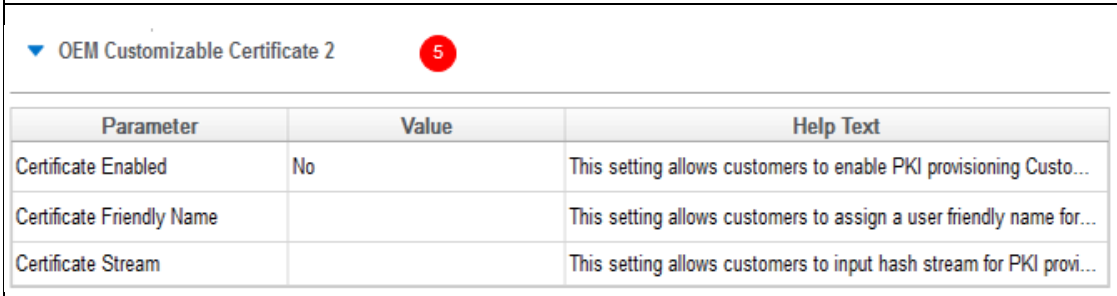
**Click on Intel® AMT in the left tabs menu> OEM Customizable Certificate 1 is expanded by default:**



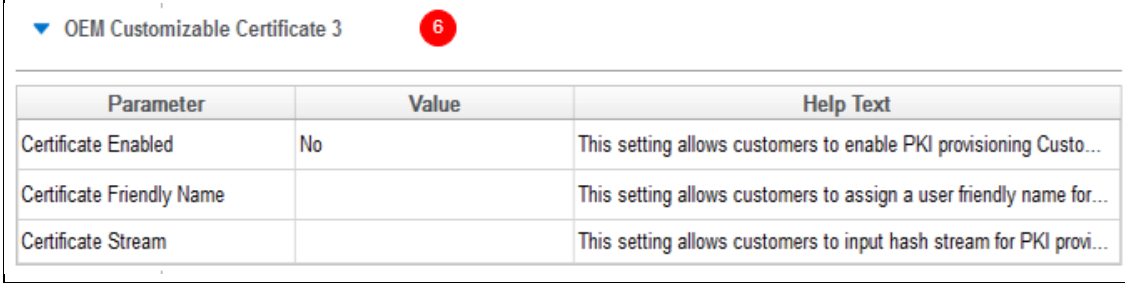

| # | Parameter | Platform | Settings |
|---|---|---|---|
| 4 | **Intel® AMT - OEM Customizable Certificate 1** | | |
| | **Certificate Enabled**<br>**Values: Yes / No** - This setting allows customers to enable PKI provisioning Custom Certificate 1. | CFL-S<br>CFL-H | No<br>No |

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

| | | | |
|---|---|---|---|
| | **Certificate Friendly Name** - This setting allows customers to assign a user friendly name for PKI provisioning Custom Certificate 1. Maximum of 32 characters. | CFL-S<br>CFL-H | -<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. **Note:** If the platform is un-configured the Custom Certificate Hash will be deleted. | CFL-S<br>CFL-H | -<br>- |
| **Click on Intel® AMT in the left tabs menu> OEM Customizable Certificate 2 is expanded by default:** | | | |



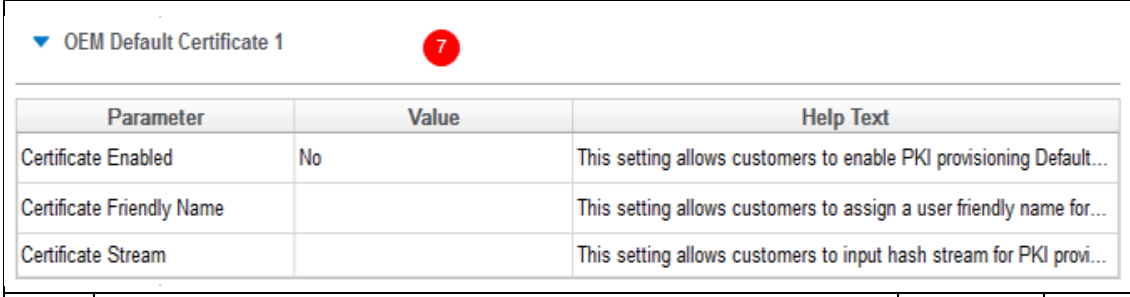

| # | Parameter | Platform | Settings |
|---|---|---|---|
| 5 | **Intel® AMT - OEM Customizable Certificate 2** | | |
| | **Certificate Enabled**<br>**Values: Yes / No** - This setting allows customers to enable PKI provisioning Custom Certificate 2. | CFL-S<br>CFL-H | No<br>No |
| | **Certificate Friendly Name** - This setting allows customers to assign a user friendly name for PKI provisioning Custom Certificate 2. Maximum of 32 characters. | CFL-S<br>CFL-H | -<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. **Note:** If the platform is un-configured the Custom Certificate Hash will be deleted. | CFL-S<br>CFL-H | -<br>- |
| **Click on Intel® AMT in the left tabs menu> OEM Customizable Certificate 3 is expanded by default:** | | | |




| # | Parameter | Platform | Settings |
|---|---|---|---|
| 6 | **Intel® AMT - OEM Customizable Certificate 3** | | |
| | **Certificate Enabled**<br>**Values: Yes / No** - This setting allows customers to enable PKI provisioning Custom Certificate 3. | CFL-S<br>CFL-H | 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. | CFL-S<br>CFL-H | -<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. **Note:** If the platform is un-configured the Custom Certificate Hash will be deleted. | CFL-S<br>CFL-H | -<br>- |

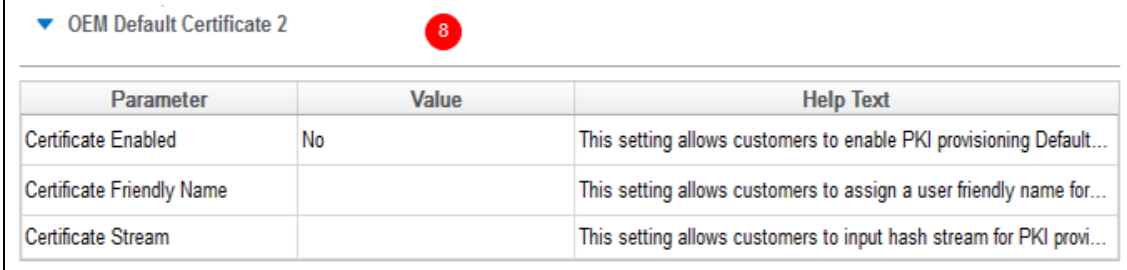
## Table 2-6. - Intel® AMT (Sheet 4 of 7)

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




| # | Parameter | Platform | Settings |
|---|---|---|---|
| 7 | **Intel® AMT - OEM Default Certificate 1** | | |
| | **Certificate Enabled**<br>**Values: Yes/No** - This setting allows customers to enable PKI provisioning Default certificate 1. | CFL-S<br>CFL-H | 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. | CFL-S<br>CFL-H | -<br>- |
| | **Certificate Stream** - This setting allows customers to input hash stream for PKI provisioning custom certificate 1. **Note:** Default Certificates if enabled will be used in addition to those already pre-loaded in firmware during provisioning. Unlike Customizable Certificates the Default Certificates are not deleted when the platform is un-provisioned. | CFL-S<br>CFL-H | -<br>- |

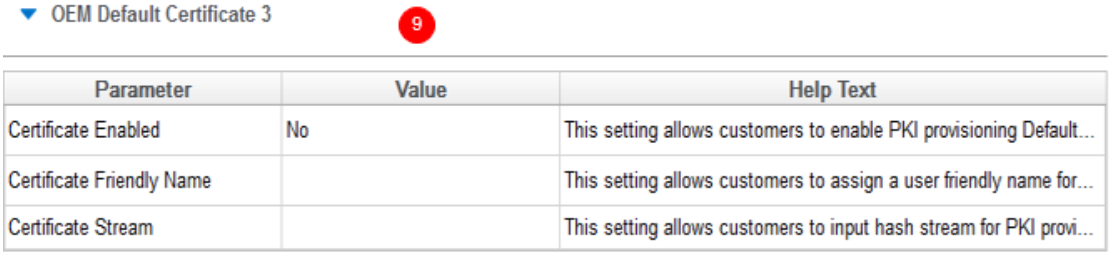
**Click on Intel® AMT in the left tabs menu> OEM Default Certificate 2 is expanded by default:**



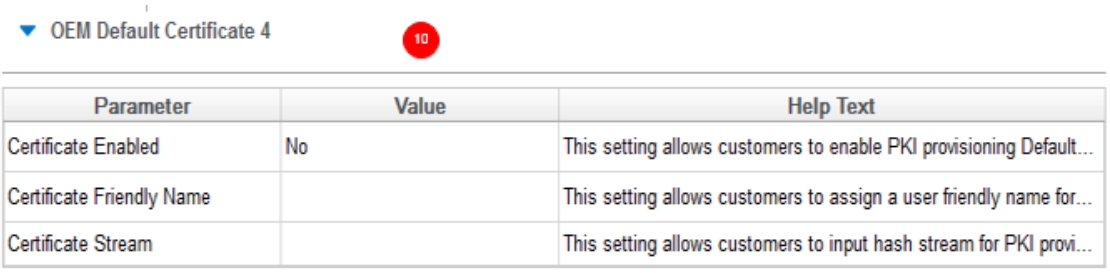

| # | Parameter | Platform | Settings |
|---|---|---|---|
| 8 | **Intel® AMT - OEM Default Certificate 2** | | |
| | **Certificate Enabled**<br>**Values: Yes/No** - This setting allows customers to enable PKI provisioning Default certificate 2. | CFL-S<br>CFL-H | No<br>No |
| | **Certificate Friendly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

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

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

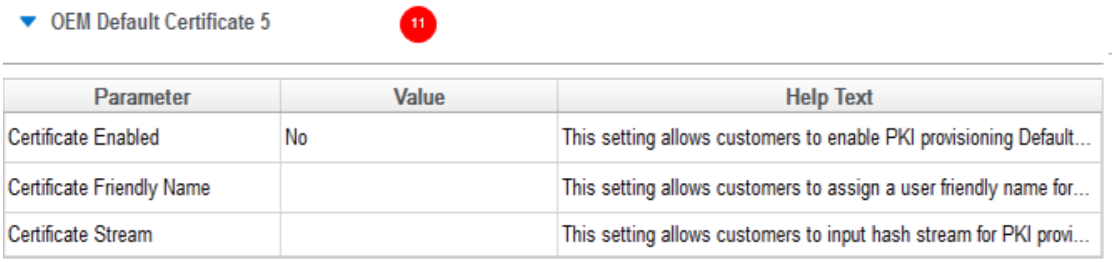



| # | Parameter | Platform | Settings |
|---|---|---|---|
| 9 | **Intel® AMT - OEM Default Certificate 3** | | |
| | **Certificate Enabled**<br>**Values: Yes / No** - This setting allows customers to enable PKI provisioning Default certificate 3. | CFL-S<br>CFL-H | No<br>No |
| | **Certificate Friendly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

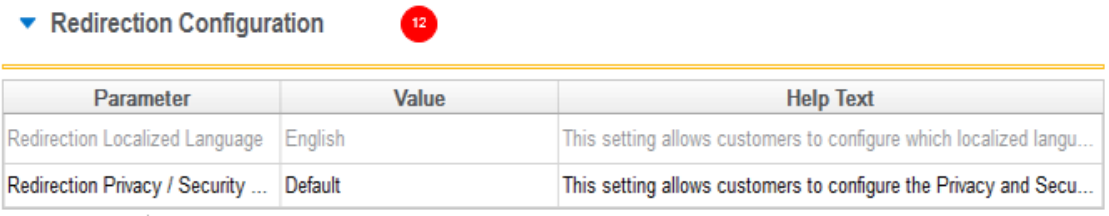



| # | Parameter | Platform | Settings |
|---|---|---|---|
| 10 | **Intel® AMT - OEM Default Certificate 4** | | |
| | **Certificate Enabled**<br>**Values: Yes / No** - This setting allows customers to enable PKI provisioning Default certificate 4. | CFL-S<br>CFL-H | No<br>No |
| | **Certificate Friendly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

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

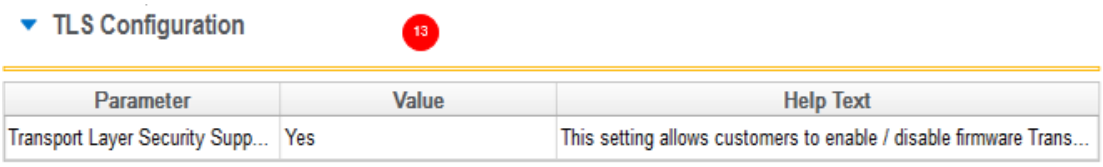



| # | Parameter | Platform | Settings |
|---|---|---|---|
| 11 | **Intel® AMT - OEM Default Certificate 5** | | |
| | **Certificate Enabled**<br>**Values: Yes / No** - This setting allows customers to enable PKI provisioning Default certificate 5. | CFL-S<br>CFL-H | No<br>No |
| | **Certificate Friendly Name** - This setting allows customers to assign a user friendly name for PKI provisioning Default Certificate 5. | CFL-S<br>CFL-H | -<br>- |
| | **Certificate Stream** - This setting allows customers to input hash stream for PKI provisioning custom certificate 5. **Note:** Default Certificates if enabled will be used in addition to those already pre-loaded in firmware during provisioning. Unlike Customizable Certificates the Default Certificates are not deleted when the platform is un-provisioned. | CFL-S<br>CFL-H | -<br>- |
| **Click on Intel® AMT in the left tabs menu> Redirection Configuration is expanded by default:** | | | |




| # | Parameter | Platform | Settings |
|---|---|---|---|
| 12 | **Intel® AMT - Redirection Configuration** | | |
| | **Redirection Localized Language -** This setting allows customers to configure which localized language will be used initially by firmware for user consent output information (Examples: May be displayed before SOL / KVM session starts). | CFL-S<br>CFL-H | 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>**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. | CFL-S<br>CFL-H | Default<br>Default |
| **Click on Intel® AMT in the left tabs menu> TLS Configuration is expanded by default:** | | | |

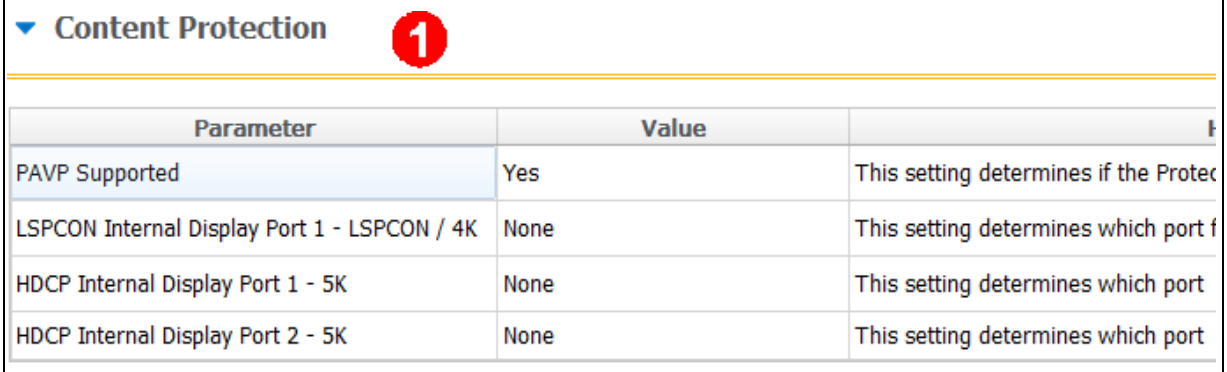
## Table 2-6. - Intel® AMT (Sheet 7 of 7)




| # | Parameter | Platform | Settings |
|---|---|---|---|
| 13 | **Intel® AMT - TLS Configuration** | | |
| | **Transport Layer Security Supported**<br>**Values: Yes / No** - This setting allows customers to enable / disable firmware Transport Layer Security support. **Note:** If this is disabled TLS will be permanently disabled in the firmware image. This setting needs to be enabled along with along with the Intel® ME Network Services Supported for proper operation of the Intel® Authenticate (Corporate Only) feature. | CFL-S<br>CFL-H | No<br>No |

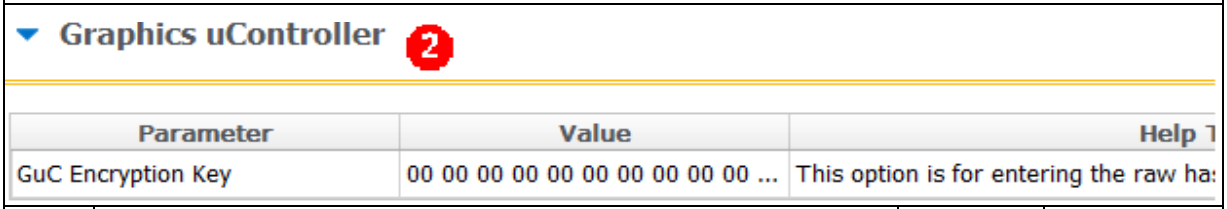
## Table 2-7. - Platform Protection (Sheet 1 of 4)

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




| # | Parameter | Platform | Settings |
|---|---|---|---|
| 1 | **Platform Protection - 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. | CFL-S<br>CFL-H | Yes<br>Yes |
| | **LSPCON Internal Display Port 1 - LSPCON / 4K**<br>**Values: None, Port B, Port C, Port D**<br>This setting determines which port for LSPCON will be connected to HDCP 2.2 Bridge adapter Display 1. | CFL-S<br>CFL-H | None<br>None |
| | **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>**Note:**<br>Both Display Port 1 & 2 need to be configured for proper operation. | CFL-S<br>CFL-H | None<br>None |
| | **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>**Note:**<br>Both Display Port 1 & 2 need to be configured for proper operation. | CFL-S<br>CFL-H | None<br>None |

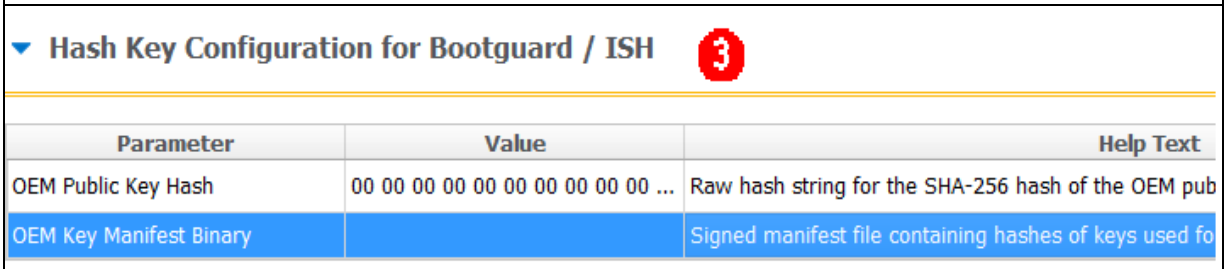
**Click on Platform Protection in the left tabs menu> Graphics uController is expanded by default:**




| # | Parameter | Platform | Settings |
|---|---|---|---|
| 2 | **Platform Protection - 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. | CFL-S<br>CFL-H | 0x00000000<br>0x00000000 |

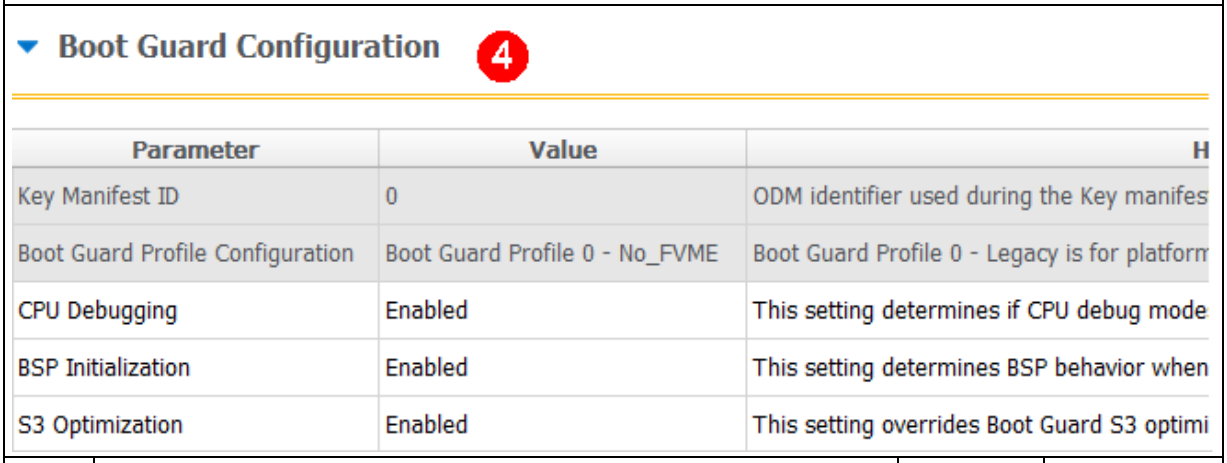
## Table 2-7. - Platform Protection (Sheet 2 of 4)

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




| # | Parameter | Platform | |
|---|---|---|---|
| 3 | **Platform Protection - 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 256-bit field represents the SHA-256 hash of the OEM public key corresponding to the private key used to sign the BIOS-SM or ISH image. Please see Appendix E for further details. | CFL-S<br>CFL-H | 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). | CFL-S<br>CFL-H | |

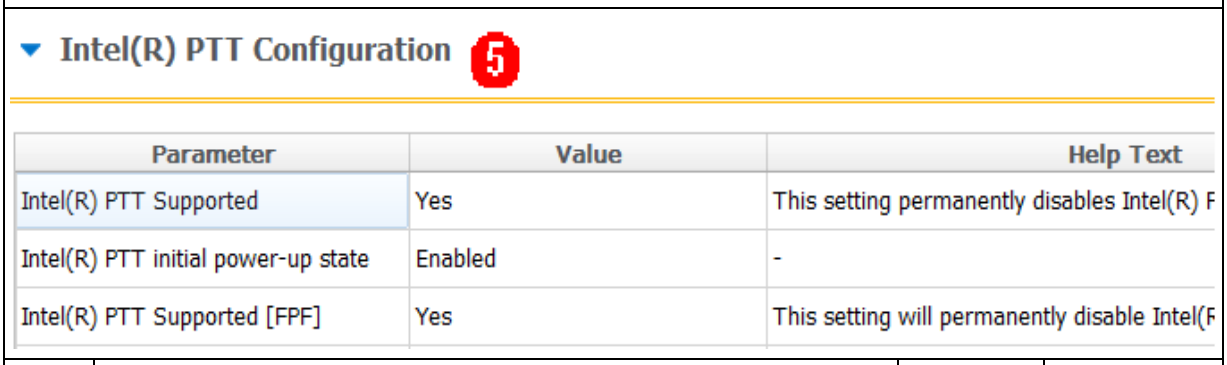
**Click on Platform Protection in the left tabs menu> Boot Guard Configuration is expanded by default:**




| # | Parameter | Platform | Settings |
|---|---|---|---|
| 4 | **Platform Protection - 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. | CFL-S<br>CFL-H | 0x0<br>0x0 |

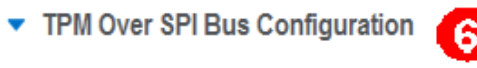
## Table 2-7. - Platform Protection (Sheet 3 of 4)

| | | | |
|---|---|---|---|
| | **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. | CFL-S<br>CFL-H | 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. | CFL-S<br>CFL-H | 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). | CFL-S<br>CFL-H | Enabled<br>Enabled |
| | **S3 Optimization**<br>**Values: Enabled / Disabled**<br>This setting overrides Boot Guard S3 optimization.<br><br>***Note:*** Used for testing only. | CFL-S<br>CFL-H | Enabled<br>Enabled |
| **Click on Platform Protection in the left tabs menu> Intel® PTT Configuration is expanded by default:** | | | |




| # | Parameter | Platform | Settings |
|---|---|---|---|
| 5 | **Platform Protection - Intel® PTT Configuration** | | |
| | **Intel® PTT Supported**<br>**Values: Yes / No** - This setting permanently disables Intel® PTT in the firmware image. | CFL-S<br>CFL-H | 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. | CFL-S<br>CFL-H | Enabled<br>Enabled |
| | **Intel® PTT Supported [FPF]**<br>**Values: Yes / No** - This setting will permanently disable Intel® PTT through platform FPFs. **Caution:** Using this option will permanently disable Intel® PTT on the platform hardware. | CFL-S<br>CFL-H | Yes<br>Yes |
| **Click on Platform Protection in the left tabs menu> TPM Over SPI Bus Configuration is expanded by default:** | | | |

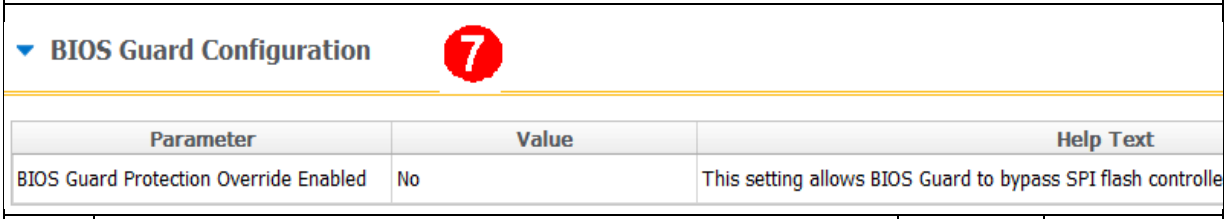
## Table 2-7. - Platform Protection (Sheet 4 of 4)




| Parameter | Value | Help Text |
|---|---|---|
| TPM Clock Frequency | 17MHz | This setting determines the clock frequency setting to be used fo... |
| TPM Over SPI Bus Enabled | No | This setting determines if TPM over SPI bus is enabled on the pl... |

| # | Parameter | Platform | Settings |
|---|---|---|---|
| 6 | **Platform Protection - TPM Over SPI Bus Configuration** | | |
| | **TPM Clock Frequency**<br>**Values: 17MHz, 30MHz, 48MHz** - This setting determines the clock frequency setting to be used for the TPM over SPI bus. | CFL-S<br>CFL-H | 17MHz<br>17MHz |
| | **TPM Over SPI Bus Enabled**<br>**Values: Yes/No** - This setting determines if TPM over SPI bus is enabled on the platform. | CFL-S<br>CFL-H | Yes<br>Yes |

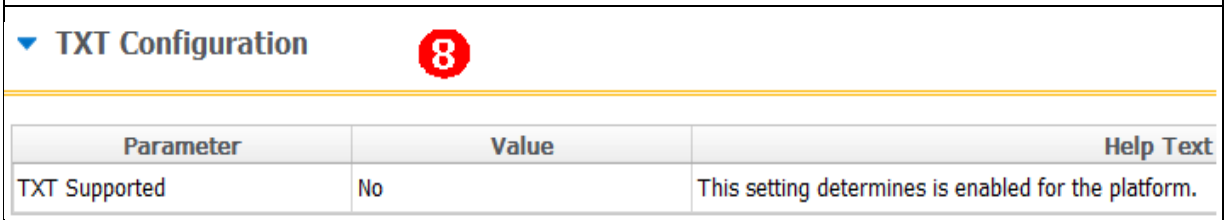
**Click on Platform Protection in the left tabs menu> BIOS Guard Configuration is expanded by default:**




| Parameter | Value | Help Text |
|---|---|---|
| BIOS Guard Protection Override Enabled | No | This setting allows BIOS Guard to bypass SPI flash controlle |

| # | Parameter | Platform | Settings |
|---|---|---|---|
| 7 | **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). | CFL-S<br>CFL-H | Yes<br>Yes |

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

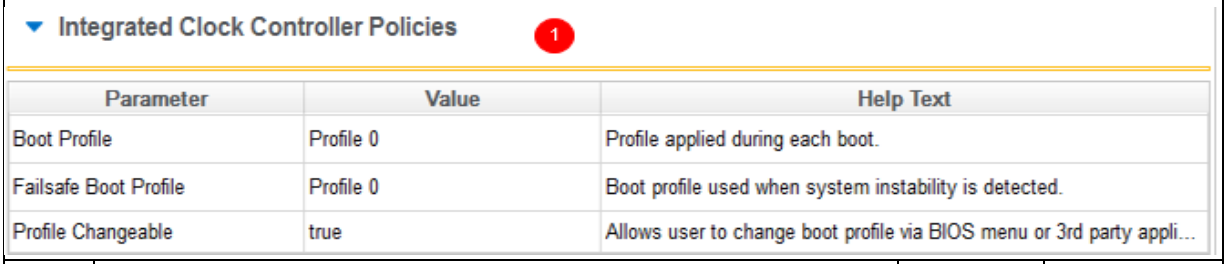



| Parameter | Value | Help Text |
|---|---|---|
| TXT Supported | No | This setting determines is enabled for the platform. |

| # | Parameter | Platform | Settings |
|---|---|---|---|
| 8 | **TXT Configuration** | | |
| | **TXT Supported**<br>This setting determines if enabled for the platform. | CFL-S<br>CFL-H | No<br>No |

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

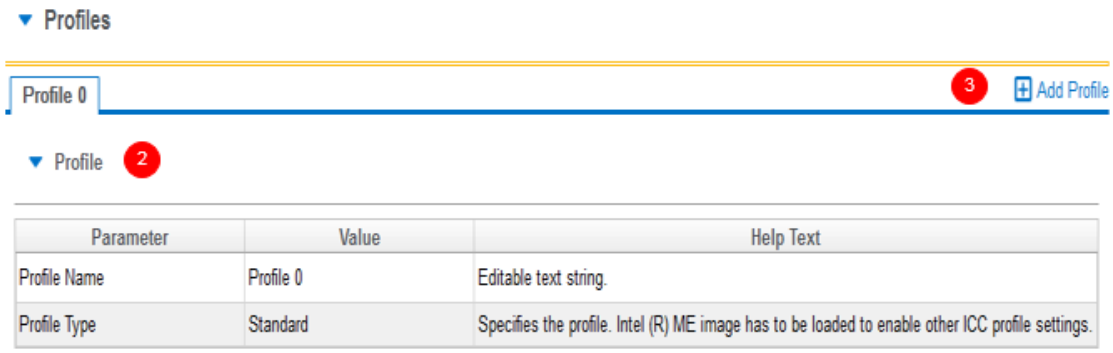
**Click on Integrated Clock Controller in the left tabs menu> Integrated Clock Controller Policies are expanded by default:**




| # | Parameter | Platform | Settings |
|---|---|---|---|
| 1 | **Integrated Clock Controller - 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. | CFL-S<br>CFL-H | 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. | CFL-S<br>CFL-H | 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. | CFL-S<br>CFL-H | True<br>True |

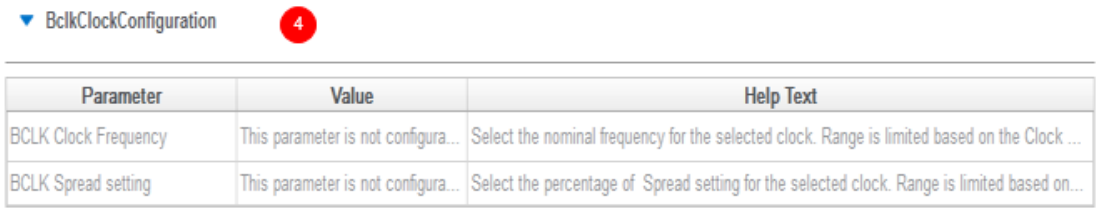
**Click on Integrated Clock Controller in the left tabs menu> Profiles are expanded by default:**

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



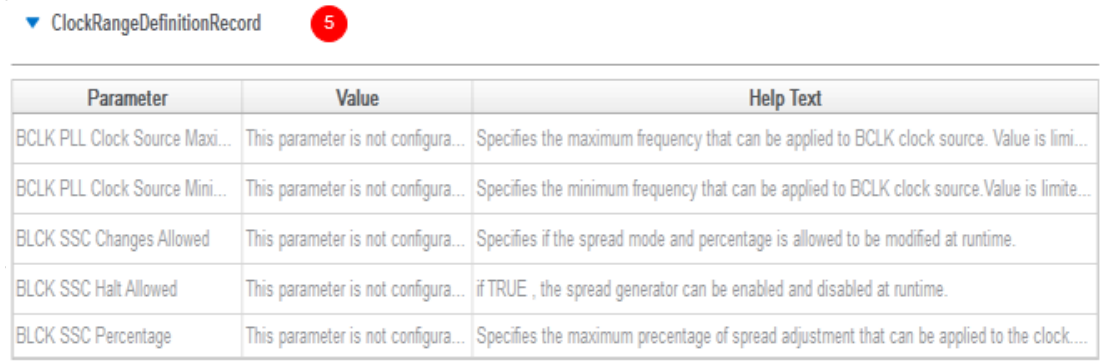

| # | Parameter | Platform | Settings |
|---|---|---|---|
| 2 | **Integrated Clock Controller - Profiles - Profile 0**<br><br>**Note:** Intel® ME image has to be loaded to enable other ICC profile settings.<br><br>**For CNL/CFL-S/H,** Intel® FIT provides 2 pre- defined ICC profiles to choose from.<br>•**Standard**: 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** CNL/CFL-S/H**,** 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"** | CFL-S<br>CFL-H | 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. | CFL-S<br>CFL-H | Profile 0<br>Profile 0 |
| | **Profile Type**<br><br>Available ICC profiles for CNL/CFL-S/H 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. | CFL-S<br>CFL-H | Standard<br>Standard |
| 3 | **+ 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**.** | CFL-S<br>CFL-H | |
| **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 3 of 9)

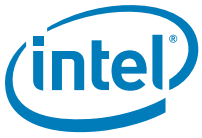



| # | Parameter | Platform | Settings |
|---|---|---|---|
| 4 | **Integrated Clock Controller - Profiles - Profile BclkClockConfiguration** | | |
| | **BCLK Clock Frequency -** This parameter allows user to select the nominal frequency for the selected clock. Range is limited based on the Clock Range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

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




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



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

| | | | |
|---|---|---|---|
| | **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>**Standard Setting Profile Type -** Option is grayed out.<br>**Adaptive Setting Profile Type -** Option is able to be edited. | CFL-S<br>CFL-H | |
| | **BCLK SSC Changes Allowed -** This parameter allows user to specify if the spread mode and percentage is allowed to be modified at runtime or not. if set to **"True':** Runtime modification is allowed.<br>**Standard Setting Profile Type -** Option is grayed out.<br>**Adaptive Setting Profile Type -** Option is able to be edited. | CFL-S<br>CFL-H | |
| | **BCLK SSC Halt Allowed -** This parameter allows user to select if the spread generator can be disabled at runtime or not.if set to **"True"**, the spread generator can be enabled and disabled at runtime.<br>**Standard Setting Profile Type -** Option is grayed out.<br>**Adaptive Setting Profile Type -** Option is able to be edited. | CFL-S<br>CFL-H | |
| | **BCLK SSC Percentage -** This parameter Specifies the maximum percentage of spread adjustment that can be applied to the clock. Value is specified in 1/100th of percent(50=0.5%)<br>**Standard Setting Profile Type -** Option is grayed out.<br>**Adaptive Setting Profile Type -** Option is able to be edited. | CFL-S<br>CFL-H | |
| **Click on Integrated Clock Controller in the left tabs menu> Profiles >Profile> Clock Output Configuration is expanded by default:** | | | |

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

Clock Output Configuration 6

| Parameter | Value | |
|---|---|---|
| ITPXDP | Enabled | Enable/Disable the CLKOUT_ITPXDP diffe |
| SRC0 | Enabled | Enable/Disable the CLKOUT_SRC0 differe |
| SRC1 | Enabled | Enable/Disable the CLKOUT_SRC1 differe |
| SRC2 | Enabled | Enable/Disable the CLKOUT_SRC2 differe |
| SRC3 | Enabled | Enable/Disable the CLKOUT_SRC3 differe |
| SRC4 | Enabled | Enable/Disable the CLKOUT_SRC4 differe |
| SRC5 | Enabled | Enable/Disable the CLKOUT_SRC5 differe |
| SRC6 | Enabled | Enable/Disable the CLKOUT_SRC6 differe |
| SRC7 | Enabled | Enable/Disable the CLKOUT_SRC7 differe |
| SRC8 | Enabled | Enable/Disable the CLKOUT_SRC8 differe |
| SRC9 | Enabled | Enable/Disable the CLKOUT_SRC9 differe |
| SRC10 | Enabled | Enable/Disable the CLKOUT_SRC10 differ |
| SRC11 | Enabled | Enable/Disable the CLKOUT_SRC11 differ |
| SRC12 | Enabled | Enable/Disable the CLKOUT_SRC12 differ |
| SRC13 | Enabled | Enable/Disable the CLKOUT_SRC13 differ |
| SRC14 | Enabled | Enable/Disable the CLKOUT_SRC14 differ |
| SRC15 | Enabled | Enable/Disable the CLKOUT_SRC15 differ |
| LPC0 | Enabled | Enable/Disable the CLKOUT_LPC0 single |
| LPC1 | Enabled | Enable/Disable the CLKOUT_LPC1 single |
| CLKOUT CPUNSSC P/N Clock Path Generation | Direct XTAL IN / Out Path | This setting determines if CLKOUT_CPUN |

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

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

| | | | |
|---|---|---|---|
| | **ITPXDP,SRC[0:5]**<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><br>These settings should match with platform hardware design.<br><br>For CRB, recommend keeping defaults for bring up with Intel® ME FW.<br><br>These parameters are specifically used to Enable/Disable the respective CLKOUT_XXX differential output buffers | CFL-S<br>CFL-H | Enabled<br>Enabled |
| | **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® ME FW.<br><br>These parameters are specifically used to Enable/Disable the respective CLKOUT_XXX differential output buffers | CFL-S<br>CFL-H | Enabled<br>Enabled |
| | **SRC1**<br>**Values: Enabled / Disabled**<br>Enables or Disables the CLKOUT_SRC1 differential output buffer. | CFL-S<br>CFL-H | Enabled<br>Enabled |
| | **SRC2**<br>**Values: Enabled / Disabled**<br>Enables or Disables the CLKOUT_SRC2 differential output buffer. | CFL-S<br>CFL-H | Enabled<br>Enabled |
| | **SRC3**<br>**Values: Enabled / Disabled**<br>Enables or Disables the CLKOUT_SRC3 differential output buffer. | CFL-S<br>CFL-H | Enabled<br>Enabled |
| | **SRC4**<br>**Values: Enabled / Disabled**<br>Enables or Disables the CLKOUT_SRC4 differential output buffer. | CFL-S<br>CFL-H | Enabled<br>Enabled |
| | **SRC5**<br>**Values: Enabled / Disabled**<br>Enables or Disables the CLKOUT_SRC5 differential output buffer. | CFL-S<br>CFL-H | Enabled<br>Enabled |
| | **SRC6**<br>**Values: Enabled / Disabled**<br>Enables or Disables the CLKOUT_SRC5 differential output buffer. | CFL-S<br>CFL-H | Enabled<br>Enabled |
| | **SRC7**<br>**Values: Enabled / Disabled**<br>Enables or Disables the CLKOUT_SRC5 differential output buffer. | CFL-S<br>CFL-H | Enabled<br>Enabled |
| | **SRC8**<br>**Values: Enabled / Disabled**<br>Enables or Disables the CLKOUT_SRC5 differential output buffer. | CFL-S<br>CFL-H | Enabled<br>Enabled |
| | **SRC9**<br>**Values: Enabled / Disabled**<br>Enables or Disables the CLKOUT_SRC5 differential output buffer. | CFL-S<br>CFL-H | Enabled<br>Enabled |
| | **SRC10**<br>**Values: Enabled / Disabled**<br>Enables or Disables the CLKOUT_SRC5 differential output buffer. | CFL-S<br>CFL-H | Enabled<br>Enabled |

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

| | | | |
|---|---|---|---|
| | **SRC11**<br>**Values: Enabled / Disabled**<br>Enables or Disables the CLKOUT_SRC5 differential output buffer. | CFL-S<br>CFL-H | Enabled<br>Enabled |
| | **SRC12**<br>**Values: Enabled / Disabled**<br>Enables or Disables the CLKOUT_SRC5 differential output buffer. | CFL-S<br>CFL-H | Enabled<br>Enabled |
| | **SRC13**<br>**Values: Enabled / Disabled**<br>Enables or Disables the CLKOUT_SRC5 differential output buffer. | CFL-S<br>CFL-H | Enabled<br>Enabled |
| | **SRC14**<br>**Values: Enabled / Disabled**<br>Enables or Disables the CLKOUT_SRC5 differential output buffer. | CFL-S<br>CFL-H | Enabled<br>Enabled |
| | **SRC15**<br>**Values: Enabled / Disabled**<br>Enables or Disables the CLKOUT_SRC5 differential output buffer. | CFL-S<br>CFL-H | Enabled<br>Enabled |
| | **LPC0[1:0]**<br>**Values: Enabled / Disabled**<br>These parameters are used to control Enabling/Disabling of CLKRUN support for CLKOUT_LPC clocks.<br><br>For CRB, recommend keeping defaults for bring up with Intel® ME FW | CFL-S<br>CFL-H | Enabled<br>Enabled |
| | **LPC1**<br>**Values: Enabled / Disabled**<br>Enables or Disables the CLKOUT_LPC1 single ended output buffer. | CFL-S<br>CFL-H | Enabled<br>Enabled |
| | **CLKOUT CPUSSC P / N Clock Path Generation**<br>**Values: HDA PLL Path / Direct XTAL IN / Out Path**<br><br>This setting determines if CLKOUT CPUSSC P/N Clock Path is generated through the HDA_PLL or from Direct XTAL IN/OUT | CFL-S<br><br>CFL-H | Direct XTAL IN / Out Path<br>Direct XTAL IN / Out Path |
| **Click on Integrated Clock Controller in the left tabs menu> Profiles >Profile> Power Management Configuration is expanded by default:** | | | |

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

▼ Power Management Configuration 7

| Parameter | Value | |
|---|---|---|
| SRC0 CLKREQ# Mapping | GPP_B5 | Assign the CLKREQ# signal associated with CLKOUT_SRC0. |
| SRC1 CLKREQ# Mapping | GPP_B6 | Assign the CLKREQ# signal associated with CLKOUT_SRC1. |
| SRC2 CLKREQ# Mapping | GPP_B7 | Assign the CLKREQ# signal associated with CLKOUT_SRC2. |
| SRC3 CLKREQ# Mapping | GPP_B8 | Assign the CLKREQ# signal associated with CLKOUT_SRC3. |
| SRC4 CLKREQ# Mapping | GPP_B9 | Assign the CLKREQ# signal associated with CLKOUT_SRC4. |
| SRC5 CLKREQ# Mapping | GPP_B10 | Assign the CLKREQ# signal associated with CLKOUT_SRC5. |
| SRC6 CLKREQ# Mapping | GPP_H0 | Assign the CLKREQ# signal associated with CLKOUT_SRC6. |
| SRC7 CLKREQ# Mapping | GPP_H1 | Assign the CLKREQ# signal associated with CLKOUT_SRC7. |
| SRC8 CLKREQ# Mapping | GPP_H2 | Assign the CLKREQ# signal associated with CLKOUT_SRC8. |
| SRC9 CLKREQ# Mapping | GPP_H3 | Assign the CLKREQ# signal associated with CLKOUT_SRC9. |
| SRC10 CLKREQ# Mapping | GPP_H4 | Assign the CLKREQ# signal associated with CLKOUT_SRC10. |
| SRC11 CLKREQ# Mapping | GPP_H5 | Assign the CLKREQ# signal associated with CLKOUT_SRC11. |
| SRC12 CLKREQ# Mapping | GPP_H6 | Assign the CLKREQ# signal associated with CLKOUT_SRC12. |
| SRC13 CLKREQ# Mapping | GPP_H7 | Assign the CLKREQ# signal associated with CLKOUT_SRC13. |
| SRC14 CLKREQ# Mapping | GPP_H8 | Assign the CLKREQ# signal associated with CLKOUT_SRC14. |
| SRC15 CLKREQ# Mapping | GPP_H9 | Assign the CLKREQ# signal associated with CLKOUT_SRC15. |
| 24Mhz Crystal Shutdown Wait Interval | 8us | Enable Dynamic power management of Crystal. Upon the even |

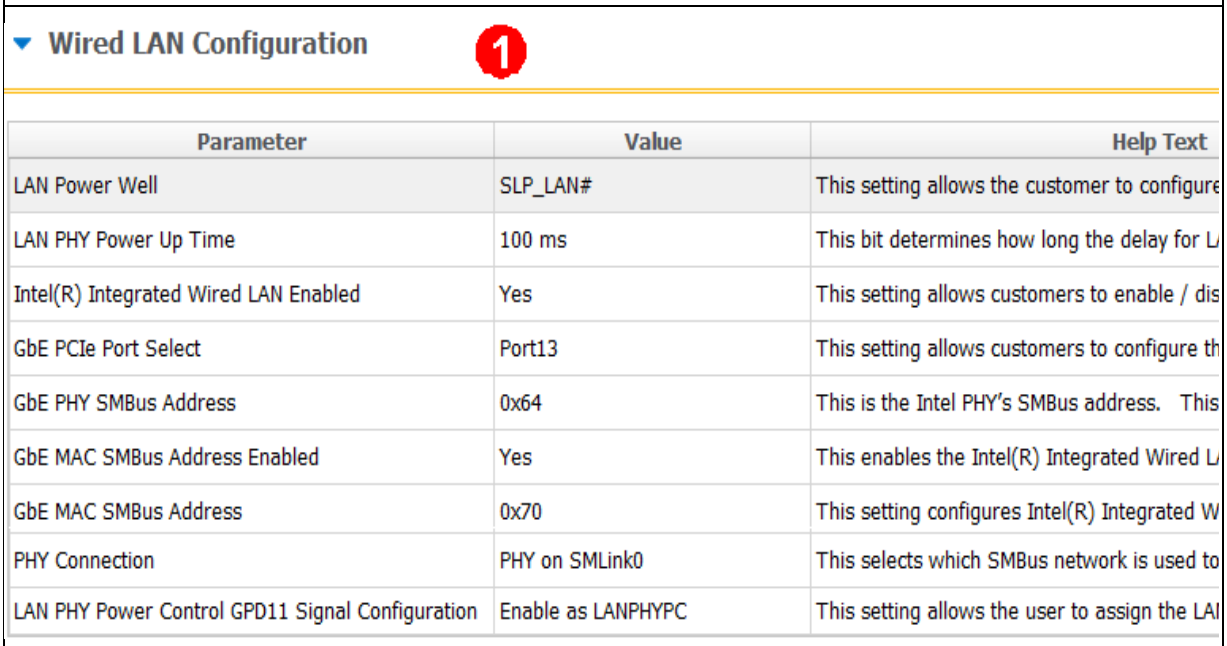
| # | Parameter | Platform | Settings |
|---|---|---|---|
| 7 | **Integrated Clock Controller - Profiles - Profile PwrManagementConfiguration**<br><br>Configuring CLKREQ# and assigning GPIO depends on how CLKOUT_SRCx configuration via FIT is done (Enabled or Disabled) and if CLKREQ is required or not.<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. | | |

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

| | | | |
|---|---|---|---|
| | **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 - CNL/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. | CFL-S<br>CFL-H | GPP_B5<br>GPP_B5 |
| | **SRC1 CLKREQ# Mapping**<br>Assign the CLKREQ# signal associated with CLKOUT_SRC1. | CFL-S<br>CFL-H | GPP_B6<br>GPP_B6 |
| | **SRC2 CLKREQ# Mapping**<br>Assign the CLKREQ# signal associated with CLKOUT_SRC2. | CFL-S<br>CFL-H | GPP_B7<br>GPP_B7 |
| | **SRC3 CLKREQ# Mapping**<br>Assign the CLKREQ# signal associated with CLKOUT_SRC3. | CFL-S<br>CFL-H | GPP_B8<br>GPP_B8 |
| | **SRC4 CLKREQ# Mapping**<br>Assign the CLKREQ# signal associated with CLKOUT_SRC4. | CFL-S<br>CFL-H | GPP_B9<br>GPP_B9 |
| | **SRC5 CLKREQ# Mapping**<br>Assign the CLKREQ# signal associated with CLKOUT_SRC5. | CFL-S<br>CFL-H | GPP_B10<br>GPP_B10 |
| | **SRC6 CLKREQ# Mapping**<br>Assign the CLKREQ# signal associated with CLKOUT_SRC5. | CFL-S<br>CFL-H | GPP_H0<br>GPP_H0 |
| | **SRC7 CLKREQ# Mapping**<br>Assign the CLKREQ# signal associated with CLKOUT_SRC5. | CFL-S<br>CFL-H | GPP_H1<br>GPP_H1 |
| | **SRC8 CLKREQ# Mapping**<br>Assign the CLKREQ# signal associated with CLKOUT_SRC5. | CFL-S<br>CFL-H | GPP_H2<br>GPP_H2 |
| | **SRC9 CLKREQ# Mapping**<br>Assign the CLKREQ# signal associated with CLKOUT_SRC5. | CFL-S<br>CFL-H | GPP_H3<br>GPP_H3 |
| | **SRC10 CLKREQ# Mapping**<br>Assign the CLKREQ# signal associated with CLKOUT_SRC5. | CFL-S<br>CFL-H | GPP_H4<br>GPP_H4 |
| | **SRC11 CLKREQ# Mapping**<br>Assign the CLKREQ# signal associated with CLKOUT_SRC5. | CFL-S<br>CFL-H | GPP_H5<br>GPP_H5 |
| | **SRC12 CLKREQ# Mapping**<br>Assign the CLKREQ# signal associated with CLKOUT_SRC5. | CFL-S<br>CFL-H | GPP_H6<br>GPP_H6 |
| | **SRC13 CLKREQ# Mapping**<br>Assign the CLKREQ# signal associated with CLKOUT_SRC5. | CFL-S<br>CFL-H | GPP_H7<br>GPP_H7 |
| | **SRC14 CLKREQ# Mapping**<br>Assign the CLKREQ# signal associated with CLKOUT_SRC5. | CFL-S<br>CFL-H | GPP_H8<br>GPP_H8 |
| | **SRC15 CLKREQ# Mapping**<br>Assign the CLKREQ# signal associated with CLKOUT_SRC5. | CFL-S<br>CFL-H | GPP_H9<br>GPP_H9 |
| | **24MHz Crystal Shutdown Wait Interval**<br>This parameter allows user to Enable Dynamic power management of Crystal. Upon the event that all conditions (other than this wait timer itself) are satisfied for iSCLK crystal shutdown, a timer is started. Once it expires and there are no wake events, iSCLK will shutdown crystal.<br>**Note:** Recommendation is to leave setting at default value. | CFL-S<br>CFL-H | 8us<br>8us |

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

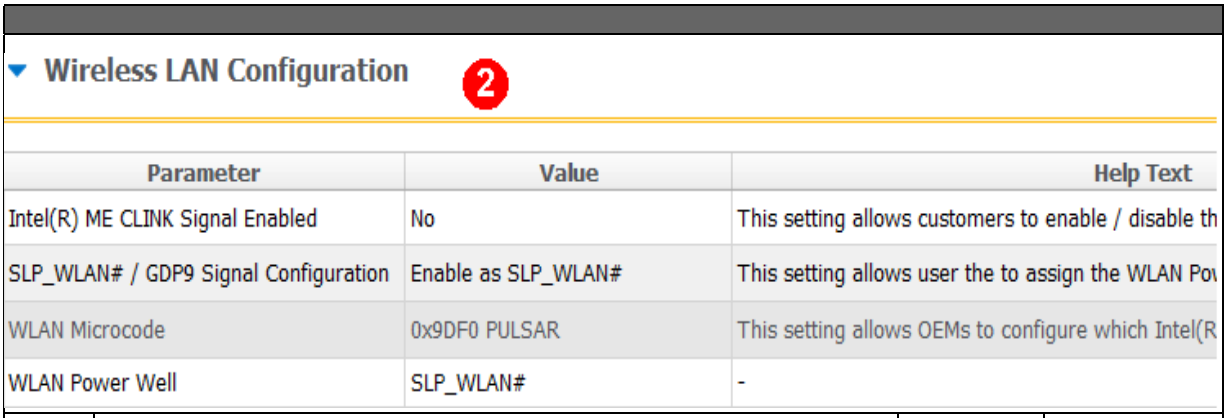
**Click on Networking & Connectivity in the left tabs menu> Wired LAN Configuration is expanded by default:**




| # | Parameter | Platform | Settings |
|---|---|---|---|
| 1 | **Networking & Connectivity - 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#. | CFL-S<br>CFL-H | SLP_LAN#<br>SLP_LAN# |
| | **LAN PHY Power Up Time**<br>**Values: 50ms, 100ms** | CFL-S<br>CFL-H | 100ms<br>100ms |
| | **Intel® Integrated Wired LAN Enable**<br>**Values: Enabled/Disabled -** This setting enables or disables the Intel® Integrated LAN. | CFL-S<br>CFL-H | Yes<br>Yes |
| | **GbE PCIe Port Select**<br>**Values: PORT5, PORT9, PORT12, PORT13** - This setting allows customers to configure the PCIe Port that will Intel® Integrated LAN will operate on. | CFL-S<br>CFL-H | Port13<br>Port5 |
| | **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. | CFL-S<br>CFL-H | 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. | CFL-S<br>CFL-H | Yes<br>Yes |
| | **GbE MAC SMBus Address** | CFL-S<br>CFL-H | 0x70<br>0x70 |
| | **PHY Connection**<br>**Values: No PHY connected, PHY on SMLink0** | CFL-S<br>CFL-H | 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. | CFL-S<br>CFL-H | LANPHYPC<br>LANPHYPC |

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

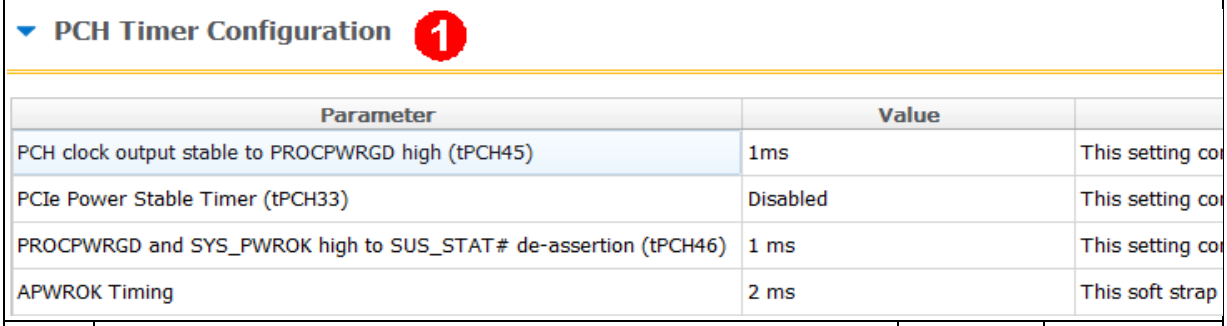
## Table 2-9. - Networking & Connectivity (Sheet 2 of 2)




| # | Parameter | Platform | Settings |
|---|---|---|---|
| 2 | **Networking & Connectivity - Wireless LAN Configuration** | | |
| | **CLINK Enabled**<br>**Values: Yes/No** - This setting allows customers to enable / disable the Wireless LAN CLINK signal through Intel® ME firmware. **Note:** For using Intel® vPro™ Wireless solutions this should be set to "Yes". | CFL-S<br>CFL-H | No<br>No |
| | **SLP_WLAN# / GPD9 Signal Configuration**<br>**Values: SLP_WLAN#, GPD9** - This setting allows the customer to assign the WLAN Power Control signal to WLAN or as GDP9. **Note:** If using Intel® Wireless LAN this setting should be set to "Enable as SLP_WLAN#". | CFL-S<br>CFL-H | Enable as SLP_WLAN#<br>Enabled as SLP_WLAN # |
| | **WLAN Microcode** - This setting allow OEMs to configure which Intel® Wireless LAN card microcode to load into the firmware image. | CFL-S<br>CFL-H | 0x9DF0<br>0x9DF0 |
| | **WLAN Power Well**<br>**Values: Disabled, Sus Well, ME Well, SLP_M#\|\|SPDA, SLP_WLAN#** - This setting allows OEMs to configure the power well that will be used by Intel® Wireless LAN.<br>WLAN Sleep via SLP_WLAN# (default)<br>**Note:** Recommended setting is SLP_WLAN#. | CFL-S<br>CFL-H | SLP_WLAN#<br>SLP_WLAN# |

## 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 | **Internal PCH Buses - 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 Cannon Lake H Platform Controller Hub EDS. | CFL-S<br>CFL-H | 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. **Note:** The recommended setting is "Disabled". | CFL-S<br>CFL-H | 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 Cannon Lake H Platform Controller Hub EDS. | CFL-S<br>CFL-H | 1ms<br>1ms |
| | **APWROK Timing**<br>**Values: 2ms, 4ms, 8ms, 16ms** - This soft strap determines the time between the SLP_A# pin de-asserting and the APWROK timer expiration. For further details see Cannon Lake H Platform Controller Hub EDS. | CFL-S<br>CFL-H | 2ms<br>2ms |

**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

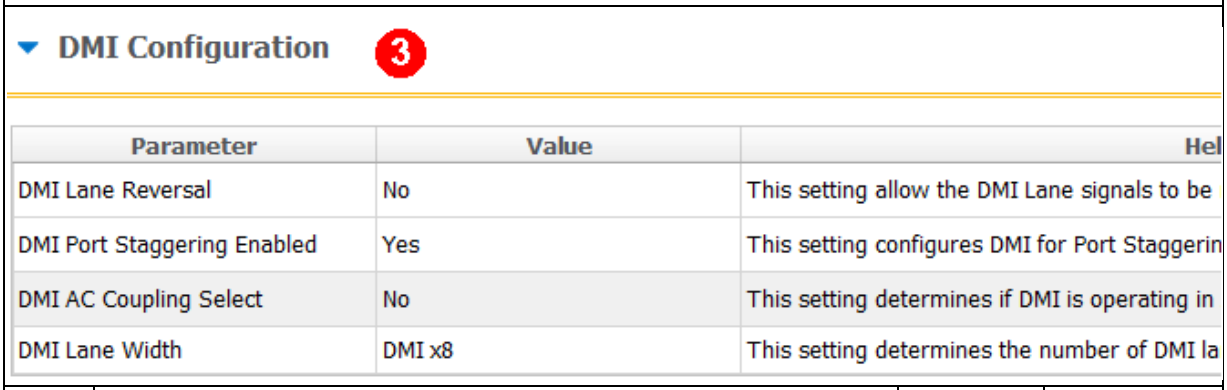
| Parameter | Value | He |
|---|---|---|
| Intel(R) SMBus ASD Address | 0x00 | This setting configures the Intel(R) SMBu |
| Intel(R) SMBus ASD Address Enabled | No | This setting enables / disables the Intel(R |
| Intel(R) SMBus Subsystem Vendor Device ID for ASF | 0x00000000 | This setting configures the Intel(R) SMBus |
| Intel(R) SMBus I2C Address | 0x00 | This setting configures the Intel(R) SMBus |
| Intel(R) SMBus I2C Address Enabled | No | This setting enables / disables the Intel(R |
| Intel(R) SMBus MCTP Address | 0x00 | This setting configures the Intel(R) SMBus |
| Intel(R) SMBus MCTP Address Enabled | No | This setting enables / disables the Intel(R |
| SMBus / SMLink TCO Slave Connection | Intel(R) SMBus | This setting configures the TCO Slave con |
| SMLink0 Enabled | Yes | This setting enables / disables SMLink0 in |
| SMLink0 Frequency | 1 MHz | This setting determines the frequency at v |
| SMLink1 I2C Target Address | 0x00 | This setting configures SMLink1 I2C Targ |
| SMLink1 I2C Target Address Enabled | No | This setting configures SMLink1 I2C Targ |
| SMLink1 GP Target Address | 0x0 | This setting configures SMLink1 GP Targe |
| SMLink1 GP Target Address Enabled | No | This setting enables / disables SMLink1 GI |
| SMLink1 Enabled | No | This setting enables / disables SMLink1 in |
| SMLink1 Frequency | 1 MHz | This setting determines the frequency at v |
| Intel(R) SMBus ASD Mode Configuration | Enable as GPP_C2 | This setting determines the native mode c |

| # | Parameter | Platform | Settings |
|---|---|---|---|
| 2 | **Internal PCH Buses - SMBus / SMLink Configuration** | | |
| | **Intel® SMBus ASD Address** - This setting configures the Intel® SMBus Alert Sending Device Address. For details see Cannon Lake H SPI Programming guide for further details. | CFL-S<br>CFL-H | 0x00000000<br>0x00000000 |
| | **Intel® SMBus ASD Address Enable**<br>**Values: Yes / No** - This setting enables / disables the Intel® SMBus Alert Sending Device. For details see Cannon Lake H SPI Programming guide for further details. | CFL-S<br>CFL-H | 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 Cannon Lake H SPI Programming guide further details. | CFL-S<br>CFL-H | 0x00000000<br>0x00000000 |
| | **Intel® SMBus I2C Address** - This setting configures the Intel® SMBus I2C Address. **Note:** This setting is only used for testing purposes. The recommended setting is "0000000". | CFL-S<br>CFL-H | 0x00000000<br>0x00000000 |
| | **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". | CFL-S<br>CFL-H | No<br>No |

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

| | | | |
|---|---|---|---|
| | **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". | CFL-S<br>CFL-H | 0x00000000<br>0x00000000 |
| | **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". | CFL-S<br>CFL-H | 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 Cannon Lake H Platform Controller Hub EDS. | CFL-S<br>CFL-H | Intel® SMBus<br>Intel® SMBus |
| | **SMLink0 Enabled**<br>**Values: Yes / No** - This setting enables / disables SMLink0 interface. For further details see Cannon Lake H Platform Controller Hub EDS. | CFL-S<br>CFL-H | 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". | CFL-S<br>CFL-H | 1 MHz<br>1 MHz |
| | **SMLink1 I2C Target Address** - This setting configures SMLink1 I2C Target Address. For further details see Cannon Lake H Platform Controller Hub EDS. | CFL-S<br>CFL-H | 0x00000000<br>0x00000000 |
| | **SMLink1 I2C Target Address Enabled**<br>**Values: Yes / No** - This setting configures SMLink1 I2C Target Address. For further details see Cannon Lake H Platform Controller Hub EDS. | CFL-S<br>CFL-H | No<br>No |
| | **SMLink1 GP Target Address** - This setting configures SMLink1 GP Target Address. For further details see Cannon Lake H Platform Controller Hub EDS. | CFL-S<br>CFL-H | 0x00000000<br>0x00000000 |
| | **SMLink1 GP Target Address Enabled**<br>**Values: Yes / No** - This setting enables / disables SMLink1 GP Target Address interface. For further details see Cannon Lake H Platform Controller Hub EDS. **Note:** This setting must be set to "Yes" if using PCH / MCP Thermal reporting. | CFL-S<br>CFL-H | No<br>No |
| | **SMLink1 Enabled**<br>**Values: Yes / No** - This setting enables / disables SMLink1 interface. For further details see Cannon Lake H Platform Controller Hub EDS. **Note:** This setting must be set to "Yes" if using PCH / MCP Thermal reporting. | CFL-S<br>CFL-H | 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". | CFL-S<br>CFL-H | 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. | CFL-S<br>CFL-H | Enable as GPP_C2<br>Enable as GPP_C2 |

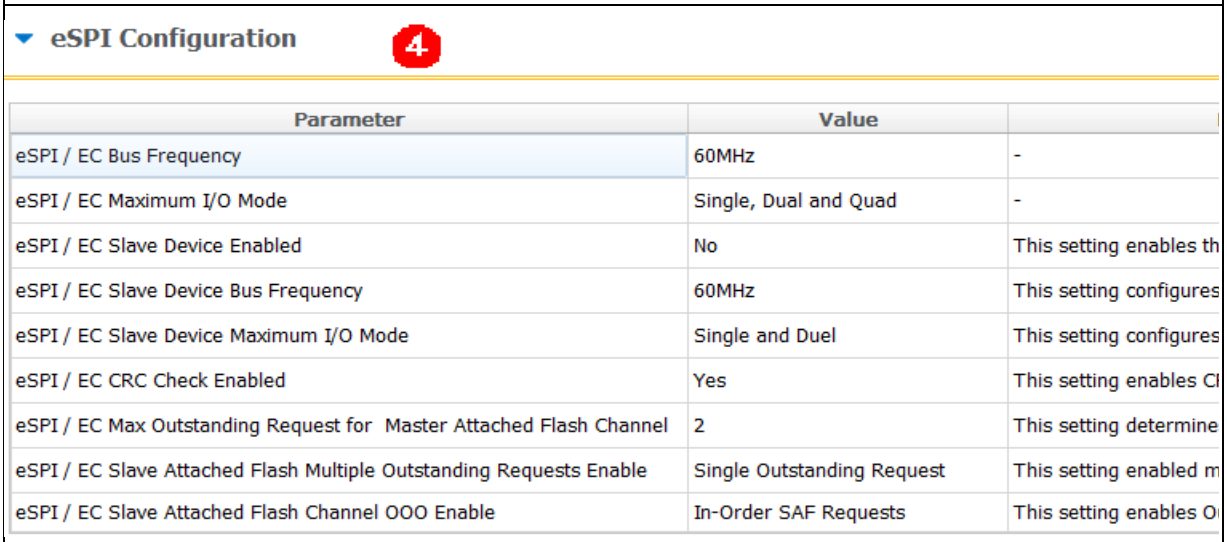
**Click on Internal PCH Buses in the left tabs menu> DMI Configuration is expanded by default:**



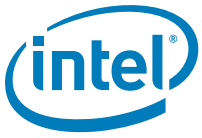

| # | Parameter | Platform | Settings |
|---|---|---|---|
| 3 | **Internal PCH Buses - DMI Configuration** | | |

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

| | | | |
|---|---|---|---|
| | **DMI Lane Reversal**<br>**Values: Yes/No** - This setting allows the DMI Lane signals to be reversed. For further details see Cannon Lake H Platform Controller Hub EDS. | CFL-S<br>CFL-H | Yes<br>No |
| | **DMI Port Staggering**<br>**Values: Yes/No** - This setting configures DMI for Port Staggering. For further details see Cannon Lake H Platform Controller Hub EDS. | CFL-S<br>CFL-H | Yes<br>Yes |
| | **DMI AC Coupling**<br>**Values: Yes/No -** This determines if DMI is operating in AC or DC coupled mode | CFL-S<br>CFL-H | No<br>No |
| | **DMI Lane Width**<br>**Values: Disabled, x1, x2, x4** - This setting determines the number of DMI lanes available | CFL-S<br>CFL-H | DMI x4<br>DMI x4 |
| **Click on Internal PCH Buses in the left tabs menu> eSPI Configuration is expanded by default:** | | | |




| # | Parameter | Platform | Settings |
|---|---|---|---|
| 4 | **Internal PCH Buses - eSPI Configuration** | | |
| | **eSPI / EC Bus Frequency**<br>**20MHz, 24MHz, 30MHz, 40MHz, 60MHz** | CFL-S<br>CFL-H | 60MHz<br>60MHz |
| | **eSPI / EC Maximum I/O Mode**<br>**Values: Single, Single and Dual, Single and Quad, Single Dual and Quad** | CFL-S<br>CFL-H | Single, Dual and Quad<br>Single, Dual and Quad |
| | **eSPI / EC Slave Device Enabled** | CFL-S<br>CFL-H | No<br>No |
| | **eSPI / EC Slave Device Bus Frequency** | CFL-S<br>CFL-H | 60MHz<br>60MHz |
| | **eSPI / EC Slave Device Maximum I/O Mode** | CFL-S<br>CFL-H | Single, Dual and Quad<br>Single, Dual and Quad |
| | **eSPI / EC CRC Check Enabled**<br>**Values: Yes/No** | CFL-S<br>CFL-H | Yes<br>Yes |
| | **eSPI / EC Slave 1 Device CRC Check Enabled**<br>**Values: Yes/No** | CFL-S<br>CFL-H | Yes<br>Yes |
| | **eSPI / EC Max Outstanding Request for Master Attached Flash Channel** | CFL-S<br>CFL-H | 2<br>2 |

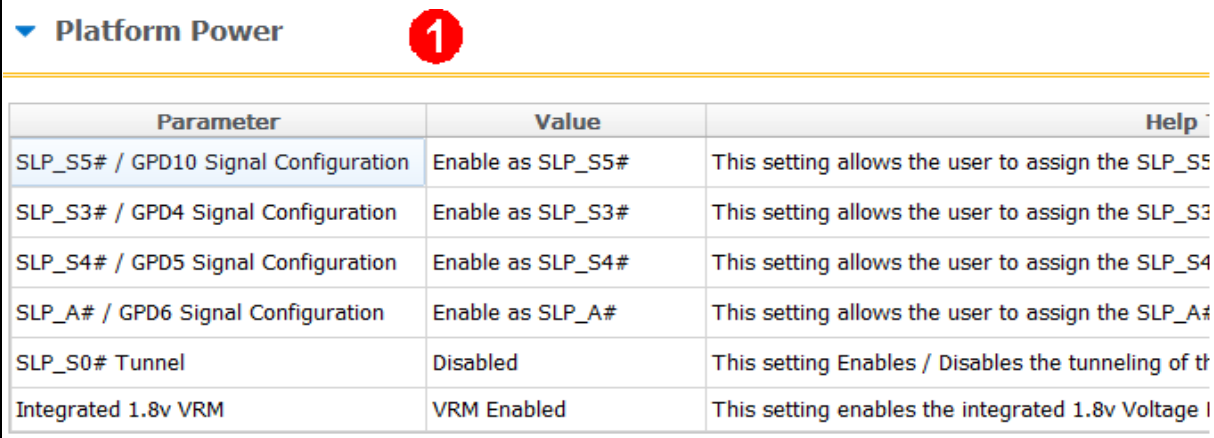


## Table 2-10. - Internal PCH Buses (Sheet 5 of 5)

| | | | |
|---|---|---|---|
| | **eSPI / EC Slave Attached Flash Multiple Outstanding Requests Enable** | CFL-S<br>CFL-H | Single Outstanding Request<br>Single Outstanding Request |
| | **eSPI / EC Slave Attached Flash Channel OOO Enable** | CFL-S<br>CFL-H | In-Order SAF Requests<br>In-Order SAF Requests |

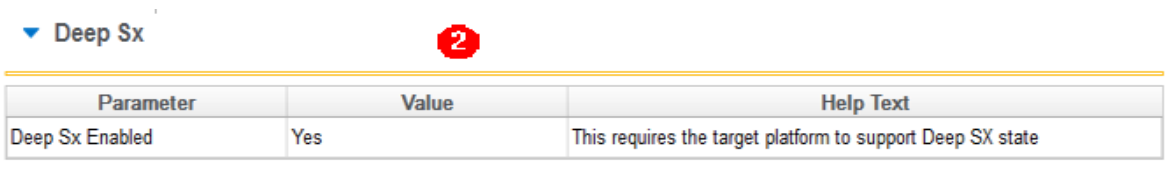
## Table 2-11. - Power (Sheet 1 of 2)

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

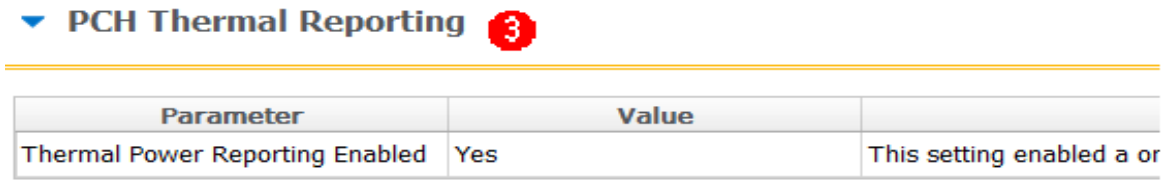



| # | Parameter | Platform | Settings |
|---|---|---|---|
| 1 | **Power - Platform Power** | | |
| | **SLP_S5# / GPD10 Signal Configuration**<br>**Values: SLP_S5#, GPD10** - This setting allows the customer to assign the SLP_S5# Power Control signal as SLP_S5# or as GDP10. For further details see Cannon Lake H Platform Controller Hub EDS. | CFL-S<br>CFL-H | SLP_S5#<br>SLP_S5# |
| | **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 Cannon Lake H Platform Controller Hub EDS. | CFL-S<br>CFL-H | 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 Cannon Lake H Platform Controller Hub EDS. | CFL-S<br>CFL-H | SLP_S4#<br>SLP_S4# |
| | **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 Cannon Lake H Platform Controller Hub EDS. | CFL-S<br>CFL-H | SLP_A#<br>SLP_A# |
| | **SLP_S0# Tunnel**<br>**Values: Enabled, Disabled**<br>This setting Enables / Disables the tunneling of the SLP_S0# pin over eSPI to the EC when in eSPI mode.<br>***Warning:*** This setting needs to be set to disabled when the platform is running in eSPI mode. | CFL-S<br>CFL-H | Disabled<br>Disabled |
| | **Integrated 1.8v VRM**<br>**Values: VRM Enabled, VRM Disabled**<br>This setting enables the integrated 1.8v Voltage Regulator on the PCH for CFL S & H. | CFL-S<br>CFL-H | VRM Enabled<br>VRM Enabled |

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



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

| # | Parameter | Platform | Settings |
|---|---|---|---|
| 2 | **Power - Deep Sx** | | |
| | **Deep Sx Enabled**<br>**Values: Yes/ No -** This setting enables / disables support for Deep Sx operation. For further details see Cannon Lake H Platform Controller Hub EDS. **Note:** Support for Deep Sx is board design dependent. | CFL-S<br>CFL-H | Yes<br>Yes |
| **Click on Power in the left tabs menu> PCH Thermal Reporting is expanded by default:** | | | |
|  | | | |
| # | Parameter | Platform | Settings |
| 3 | **Power - 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. | CFL-S<br>CFL-H | Yes<br>Yes |

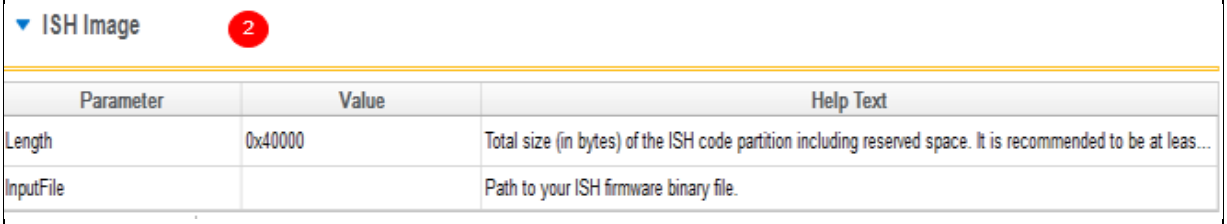
## Table 2-12. - Integrated Sensor Hub (Sheet 1 of 2)

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



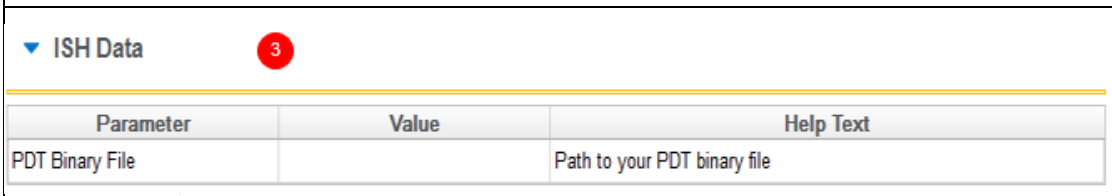

| # | Parameter | Platform | Settings |
|---|---|---|---|
| 1 | **Integrated Sensor Hub** | | |
| | **Integrated Sensor Hub Supported**<br>**Values: Yes / No**<br>This setting allows customers to disable ISH on the platform. | CFL-S<br>CFL-H | No<br>No |
| | **Integrated Sensor Hub Power Up State**<br>**Values: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

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

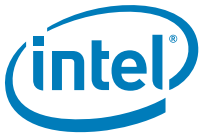



| # | Parameter | Platform | Settings |
|---|---|---|---|
| 2 | **Integrated Sensor Hub - ISH Image** | | |
| | **Length** - Total size (in bytes) of the ISH code partition including reserved space. It is recommended to be at least 256kb. | CFL-S<br>CFL-H | |
| | **Input File** | | |

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




| # | Parameter | Platform | Settings |
|---|---|---|---|
| 3 | **Integrated Sensor Hub - ISH Data** | | |

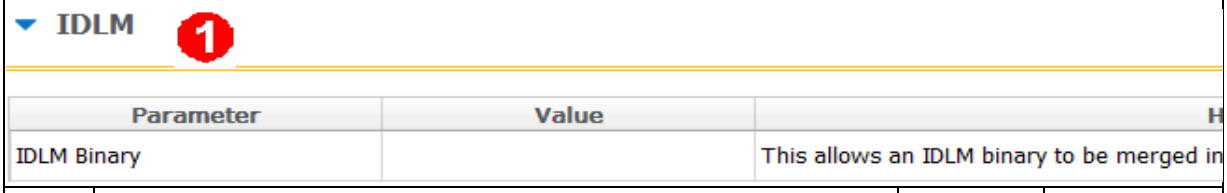


### Table 2-12. - Integrated Sensor Hub (Sheet 2 of 2)

| | | | |
|---|---|---|---|
| | **PDT Binary File** | CFL-S<br>CFL-H | Path for PDT Binary file<br>Path for PDT Binary file |

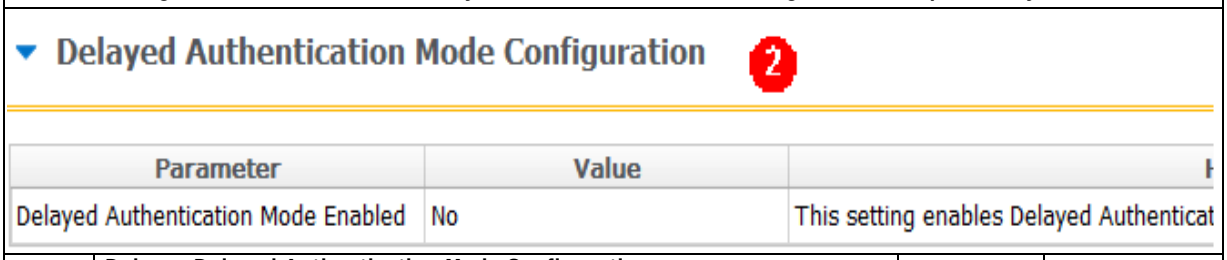
## Table 2-13. - Debug (Sheet 1 of 6)

**Click on Debug in the left tabs menu> IDLM is expanded by default:**



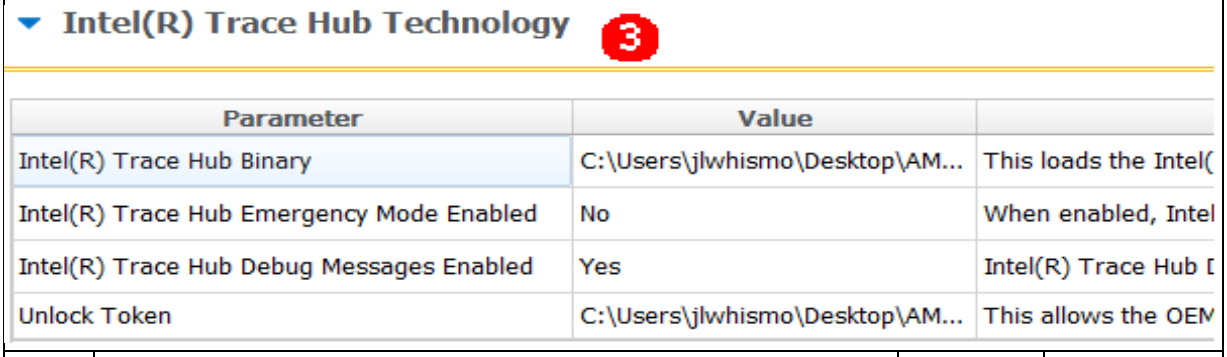

| # | Parameter | Platform | Settings |
|---|---|---|---|
| 1 | **Debug - IDLM** | | |
| | **IDLM Binary**<br>This allows an IDLM binary to be merged into output image built by Intel® FIT. | CFL-S<br>CFL-H | |

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




| | | | |
|---|---|---|---|
| 2 | **Debug - Delayed Authentication Mode Configuration** | | |
| | **Delayed Authentication Mode Enabled**<br>**Values: Yes / No** - This setting enables Delayed Authentication Mode on the platform. | CFL-S<br>CFL-H | No<br>No |

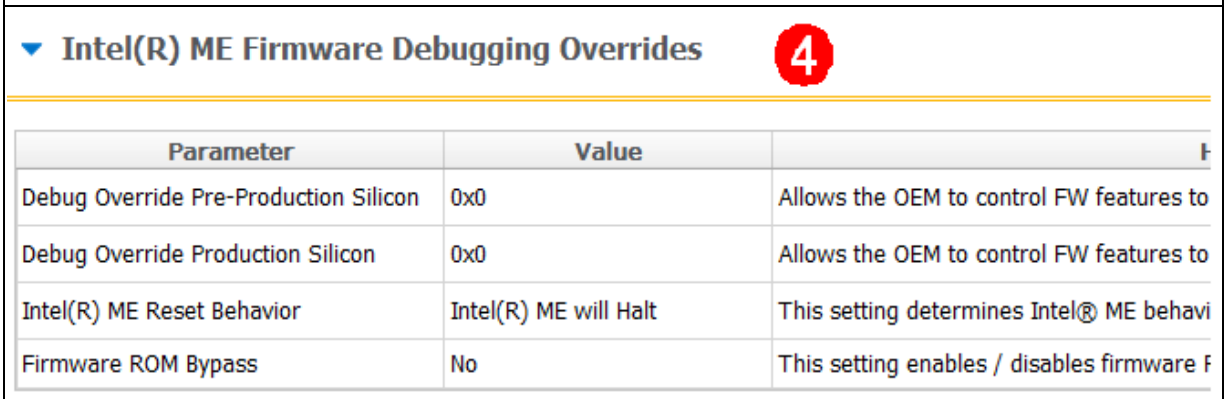
**Click on Debug in the left tabs menu> Intel® Trace Hub Technology is expanded by default:**




| # | Parameter | Platform | Settings |
|---|---|---|---|
| 3 | **Debug - Intel® Trace Hub Technology** | | |
| | **Intel® Trace Hub Binary -** This loads the Intel® Trace Hub binary that will be merged into the output image generated by the Intel® FIT tool. | CFL-S<br>CFL-H | Trace Hub Binary<br>Trace Hub Binary |

## Table 2-13. - Debug (Sheet 2 of 6)

| | | | |
|---|---|---|---|
| | **Intel® Trace Hub Emergency Mode Enabled**<br>**Values: Yes / No** - This setting enable / disables Intel® Trace Hub in the firmware base image. | CFL-S<br>CFL-H | No<br>No |
| | **Intel® Trace Hub Debug Message Enabled**<br>**Values: Yes / No** - This setting enables/disables the Intel® Trace Hub debug messages. **Note:** When enabling this setting you also need to enable Intel® Trace Hub Soft Enable setting for proper operation. | CFL-S<br>CFL-H | Yes<br>Yes |
| | **Unlock Token**<br>This allows the OEM to input an Unlock Token binary file for closed chassis debug. | CFL-S<br>CFL-H | |
| **Click on Debug in the left tabs menu> Intel® ME Debugging Overrides is expanded by default:** | | | |

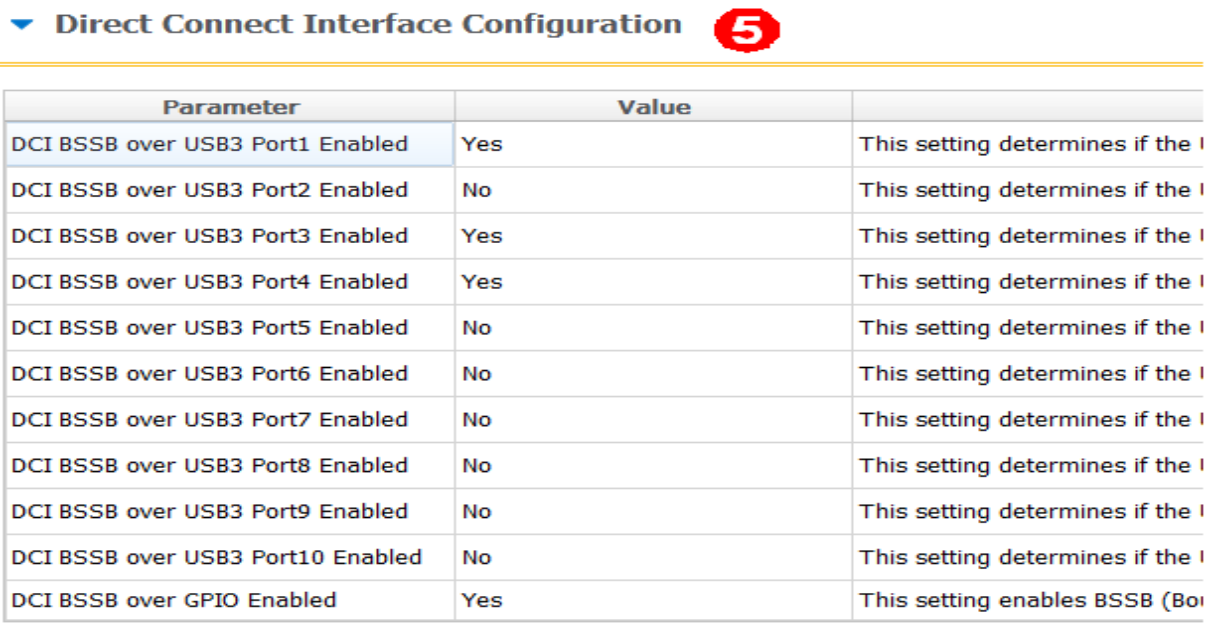



| # | Parameter | Platform | Settings |
|---|---|---|---|
| 4 | **Debug - Intel® ME Firmware Debugging Overrides** | | |
| | **Debug Override Pre-Production Silicon -** Allows the OEM to control FW features to assist with pre-production platform debugging. This control has no effect if used on production silicon.<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. | CFL-S<br>CFL-H | 0x00000000<br>0x00000000 |
| | **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. | CFL-S<br>CFL-H | 0x00000000<br>0x00000000 |
| | **Intel® ME Reset Behavior**<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. | CFL-S<br>CFL-H | Intel® ME will Halt<br>Intel® ME will Halt |

## Table 2-13. - Debug (Sheet 3 of 6)

| | | | |
|---|---|---|---|
| | **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. | CFL-S<br>CFL-H | No<br>No |

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

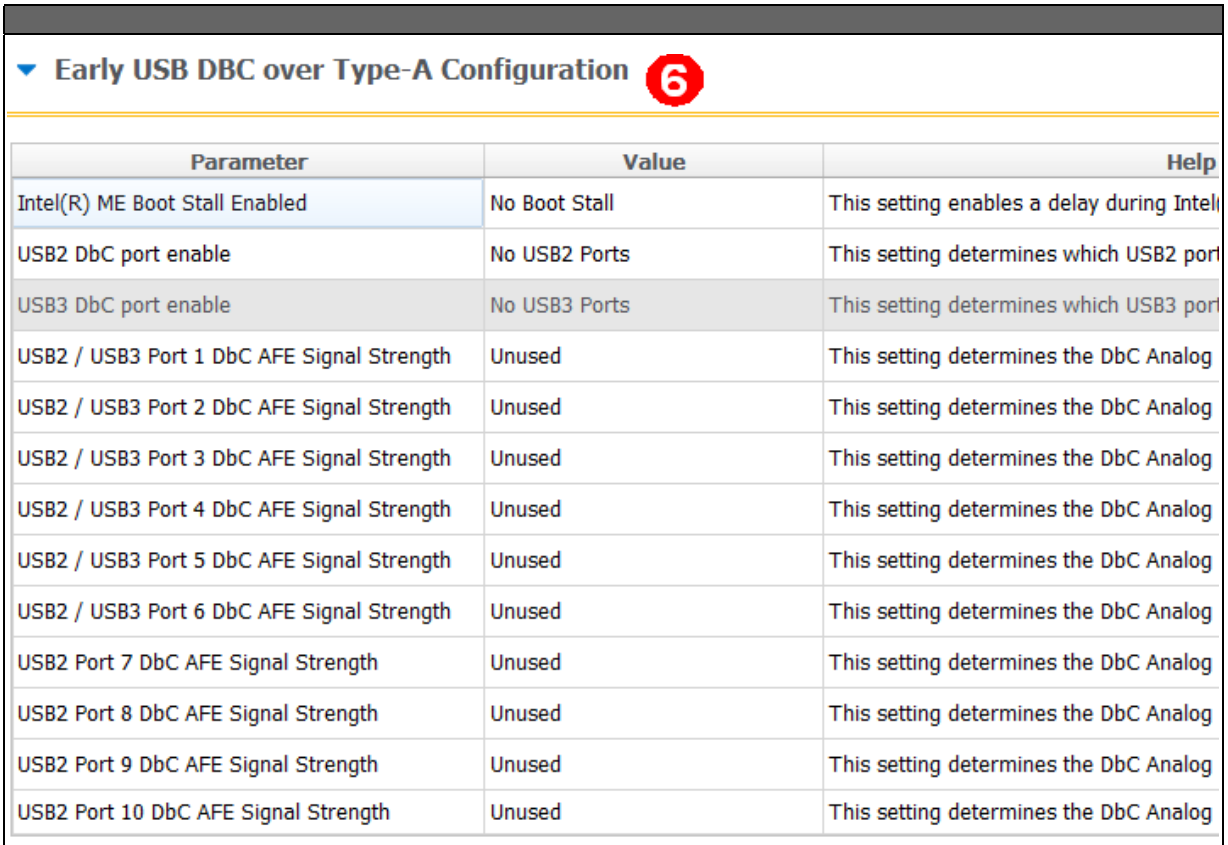



| # | Parameter | Platform | Settings |
|---|---|---|---|
| 5 | **Debug - Direct Connection Interface Configuration**<br>***Note:*** When any of the DCI BSSB USB3 Port interfaces are enabled the associated USB3 port selection control will be grayed out under the USB3 Combo Port Configuration settings section under the Flex I/O tab | | |
| | **DCI BSSB over USB3 Port 1 Enabled**<br>This setting determines if the USB port 1 has BSSB (Boundary Scan Side Band) enabled.<br>***Note:*** For S0ix and reset flows BSSB should be enabled. | CFL-S<br>CFL-H | Yes<br>Yes |
| | **DCI BSSB over USB3 Port 2 Enabled**<br>This setting determines if the USB port 2 has BSSB (Boundary Scan Side Band) enabled.<br>***Note:*** For S0ix and reset flows BSSB should be enabled. | CFL-S<br>CFL-H | Yes<br>Yes |
| | **DCI BSSB over USB3 Port 3 Enabled**<br>This setting determines if the USB port 3 has BSSB (Boundary Scan Side Band) enabled.<br>***Note:*** For S0ix and reset flows BSSB should be enabled. | CFL-S<br>CFL-H | Yes<br>Yes |
| | **DCI BSSB over USB3 Port 4 Enabled**<br>This setting determines if the USB port 4 has BSSB (Boundary Scan Side Band) enabled.<br>***Note:*** For S0ix and reset flows BSSB should be enabled. | CFL-S<br>CFL-H | Yes<br>Yes |

## Table 2-13. - Debug (Sheet 4 of 6)

| | | | |
|---|---|---|---|
| | **DCI BSSB over USB3 Port 5 Enabled**<br>This setting determines if the USB port 5 has BSSB (Boundary Scan Side Band) enabled.<br><br>***Note:*** For S0ix and reset flows BSSB should be enabled. | CFL-S<br>CFL-H | Yes<br>Yes |
| | **DCI BSSB over USB3 Port 6 Enabled**<br>This setting determines if the USB port 5 has BSSB (Boundary Scan Side Band) enabled.<br><br>***Note:*** For S0ix and reset flows BSSB should be enabled. | CFL-S<br>CFL-H | Yes<br>Yes |
| | **DCI BSSB over USB3 Port 7 Enabled**<br>This setting determines if the USB port 7 has BSSB (Boundary Scan Side Band) enabled.<br><br>***Note:*** For S0ix and reset flows BSSB should be enabled.<br>***Note:*** When this setting is enabled the corresponding USB3 Combo Port in the Flex I/O Tab will be Grayed out. | CFL-S<br>CFL-H | Yes<br>Yes |
| | **DCI BSSB over USB3 Port 8 Enabled**<br>This setting determines if the USB port 8 has BSSB (Boundary Scan Side Band) enabled.<br><br>***Note:*** For S0ix and reset flows BSSB should be enabled.<br>***Note:*** When this setting is enabled the corresponding USB3 Combo Port in the Flex I/O Tab will be Grayed out. | CFL-S<br>CFL-H | Yes<br>Yes |
| | **DCI BSSB over USB3 Port 9 Enabled**<br>This setting determines if the USB port 5 has BSSB (Boundary Scan Side Band) enabled.<br><br>***Note:*** For S0ix and reset flows BSSB should be enabled.<br>***Note:*** When this setting is enabled the corresponding USB3 Combo Port in the Flex I/O Tab will be Grayed out. | CFL-S<br>CFL-H | No<br>Yes |
| | **DCI BSSB over USB3 Port 10 Enabled**<br>This setting determines if the USB port 5 has BSSB (Boundary Scan Side Band) enabled.<br><br>***Note:*** For S0ix and reset flows BSSB should be enabled.<br>***Note:*** When this setting is enabled the corresponding USB3 Combo Port in the Flex I/O Tab will be Grayed out. | CFL-S<br>CFL-H | Yes<br>Yes |
| | **DCI BSSB over GPIO Enabled**<br>This setting enables BSSB (Boundary Scan Side Band) over GPIO for DCI operations.<br><br>***Note:*** If this setting is enabled the DCI BSSB over USB3 Port1 Enabled also needs to be set to 'Yes'.<br><br>***Note:*** For S0ix and reset flows BSSB should be enabled. | CFL-S<br>CFL-H | Yes<br>Yes |
| | **Direct Connect Interface (DCI) Enabled**<br>**Values: Yes/No** - This setting enables / disables the DCI interface used for Intel® Trace Hub debugging. | CFL-S<br>CFL-H | No<br>No |
| **Click on Debug in the left tabs menu> Early USB DBC Type-A Configuration is expanded by default:** | | | |

## Table 2-13. - Debug (Sheet 5 of 6)



Early USB DBC over Type-A Configuration 6

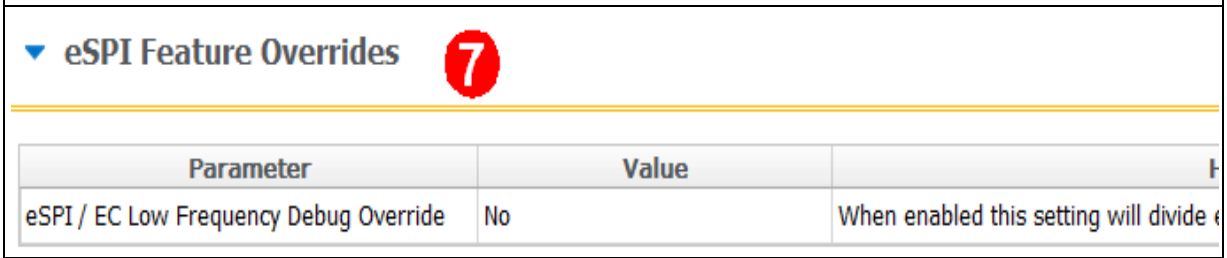
| Parameter | Value | Help |
|---|---|---|
| Intel(R) ME Boot Stall Enabled | No Boot Stall | This setting enables a delay during Intel |
| USB2 DbC port enable | No USB2 Ports | This setting determines which USB2 port |
| USB3 DbC port enable | No USB3 Ports | This setting determines which USB3 port |
| USB2 / USB3 Port 1 DbC AFE Signal Strength | Unused | This setting determines the DbC Analog |
| USB2 / USB3 Port 2 DbC AFE Signal Strength | Unused | This setting determines the DbC Analog |
| USB2 / USB3 Port 3 DbC AFE Signal Strength | Unused | This setting determines the DbC Analog |
| USB2 / USB3 Port 4 DbC AFE Signal Strength | Unused | This setting determines the DbC Analog |
| USB2 / USB3 Port 5 DbC AFE Signal Strength | Unused | This setting determines the DbC Analog |
| USB2 / USB3 Port 6 DbC AFE Signal Strength | Unused | This setting determines the DbC Analog |
| USB2 Port 7 DbC AFE Signal Strength | Unused | This setting determines the DbC Analog |
| USB2 Port 8 DbC AFE Signal Strength | Unused | This setting determines the DbC Analog |
| USB2 Port 9 DbC AFE Signal Strength | Unused | This setting determines the DbC Analog |
| USB2 Port 10 DbC AFE Signal Strength | Unused | This setting determines the DbC Analog |

| # | Parameter | Platform | Settings |
|---|---|---|---|
| 6 | **Debug - Early USB DBC Type-A Configuration** | | |
| | **Intel® ME Boot Stall Enabled**<br>This setting enables a delay during Intel® ME FW bring-up to allow USB DCI to be established and Early DbC arbitration to be granted. | CFL-S<br>CFL-H | No Boot Stall<br>No Boot Stall |
| | **USB2 DbC port enable**<br>This setting determines which USB2 ports are enabled for Early DbC debugging. | CFL-S<br>CFL-H | No USB2 Ports<br>No USB2 Ports |
| | **USB3 DbC port enable**<br>This setting determines which USB3 ports are enabled for Early DbC debugging. | CFL-S<br>CFL-H | No USB3 Ports<br>No USB3 Ports |
| | **USB2 / USB3 Port 1 DbC AFE Signal Strength**<br>This setting determines the DbC Analog Front End signal strength for USB2 / USB3 port 1. | CFL-S<br>CFL-H | Unused<br>Unused |
| | **USB2 / USB3 Port 2 DbC AFE Signal Strength**<br>This setting determines the DbC Analog Front End signal strength for USB2 / USB3 port 2. | CFL-S<br>CFL-H | Unused<br>Unused |
| | **USB2 / USB3 Port 3 DbC AFE Signal Strength**<br>This setting determines the DbC Analog Front End signal strength for USB2 / USB3 port 3. | CFL-S<br>CFL-H | Unused<br>Unused |
| | **USB2 / USB3 Port 4 DbC AFE Signal Strength**<br>This setting determines the DbC Analog Front End signal strength for USB2 / USB3 port 4. | CFL-S<br>CFL-H | Unused<br>Unused |
| | **USB2 / USB3 Port 5 DbC AFE Signal Strength**<br>This setting determines the DbC Analog Front End signal strength for USB2 / USB3 port 5. | CFL-S<br>CFL-H | Unused<br>Unused |

## Table 2-13. - Debug (Sheet 6 of 6)

| | | | |
|---|---|---|---|
| | **USB2 / USB3 Port 6 DbC AFE Signal Strength**<br>This setting determines the DbC Analog Front End signal strength for USB2 / USB3 port 6. | CFL-S<br>CFL-H | Unused<br>Unused |
| | **USB2 / USB3 Port 7 DbC AFE Signal Strength**<br>This setting determines the DbC Analog Front End signal strength for USB2 port 7. | CFL-S<br>CFL-H | Unused<br>Unused |
| | **USB2 / USB3 Port 8 DbC AFE Signal Strength**<br>This setting determines the DbC Analog Front End signal strength for USB2 port 8. | CFL-S<br>CFL-H | Unused<br>Unused |
| | **USB2 / USB3 Port 9 DbC AFE Signal Strength**<br>This setting determines the DbC Analog Front End signal strength for USB2 port 9. | CFL-S<br>CFL-H | Unused<br>Unused |
| | **USB2 / USB3 Port 10 DbC AFE Signal Strength**<br>This setting determines the DbC Analog Front End signal strength for USB2 port 10. | CFL-S<br>CFL-H | Unused<br>Unused |
| | **USB2 Port 11 DbC AFE Signal Strength**<br>This setting determines the DbC Analog Front End signal strength for USB2 port 11. | CFL-S<br>CFL-H | Unused<br>Unused |
| | **USB2 Port 12 DbC AFE Signal Strength**<br>This setting determines the DbC Analog Front End signal strength for USB2 port 12. | CFL-S<br>CFL-H | Unused<br>Unused |
| | **USB2 Port 13 DbC AFE Signal Strength**<br>This setting determines the DbC Analog Front End signal strength for USB2 port 13. | CFL-S<br>CFL-H | Unused<br>Unused |
| | **USB2 Port 14 DbC AFE Signal Strength**<br>This setting determines the DbC Analog Front End signal strength for USB2 port 14. | CFL-S<br>CFL-H | Unused<br>Unused |

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




| # | Parameter | Platform | Settings |
|---|---|---|---|
| 7 | **Debug - 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 setting enable will impact eSPI performance. | CFL-S<br>CFL-H | No<br>No |

### Table 2-14. - CPU Straps (Sheet 1 of 3)

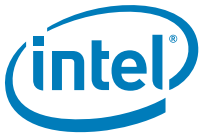
**Click on CPU Straps in the left tabs menu> CPU Straps are expanded by default:**

▼ CPU Straps 1

| Parameter | Value | |
|---|---|---|
| Disable Hyperthreading | No | This setting control enabling / disabling of Hyper threading. Note: This strap is intended for del |
| Number of Active Cores | All Cores Active | This setting controls the number of active processor cores. Note: This strap is intended for de |
| Flex Ratio | 0x00000000 | This setting controls the maximum processor non-turbo ratio. Note: This strap is intended for |
| Processor Boot Max Frequency | Yes | This setting determines if the processor will operate at maximum frequency at power-on and b |
| JTAG Power Disable | No JTAG Power on C10 and Lo... | This setting determines if JTAG power will be maintained on C10 or lower power states. Note |
| SA Power Plane Topology | 0x00000002 | This setting determines the SA power plane topology. See Processor EDS for details. Note: T |
| SA VR Type | SVID | This setting determines the SA core domain VR type. See Processor EDS for details. |
| IA Power Plane Topology | 0x00000000 | This setting determines the IA power plane topology. See Processor EDS for details. Note: Th |
| IA Power Plane VR | SVID | This setting determines the IA core domain VR type. See Processor EDS for details. |
| Ring Power Plane Topology | 0x00000000 | This setting determines the Ring power plane topology. See Processor EDS for details. Note: |
| Ring VR Type | SVID | This setting determines the Ring domain VR type. See Processor EDS for details. |
| GT_US Power Plane Topology | 0x00000001 | This setting determines the GT Unslice power plane topology. See Processor EDS for details. |
| GT_US VR Type | SVID | This setting determines the GT Unslice domain VR type. See Processor EDS for details. |
| GT_S Power Plane Topology | 0x00000001 | This setting determines the GT slice power plane topology. See Processor EDS for details. No |
| SVID Presence | SVID is present | This setting determine if SVID rails are present on the platform. See Processor EDS for details. |
| Platform IMON Disable | 0x00000000 | This strap should be left at the recommended default setting. |
| eOPIO Power Plane Topology | 0x00000000 | This setting determines the eOPIO power plane topology. See Processor EDS for details. Note |
| eOPIO VR Type | Fixed VR | This setting determines the eOPIO domain VR type. See Processor EDS for details. |
| EdramPowerPlaneTopology | 0x00000000 | This setting determines the EDRAM power plane topology. See Processor EDS for details. |
| EDRAM VR Type | Fixed VR | This setting determines the EDRAM domain VR type. See Processor EDS for details. |
| SE Key Mode | 0x00000000 | Note: This strap should be left at the recommended default setting. |
| GT_S VR Type | SVID | This setting determines the GT slice domain VR type. See Processor EDS for details. |
| VCCIN SVID Address | 0x00000000 | This setting determines the VCCIN SVID Address. |
| VCCIN VR Type | Fixed VR | This setting determines the VCCIN VR Type. |
| BIST Initialization | No | This setting determines if BIST will be run at platform reset after BIOS requested actions. N... |

## Table 2-14. - CPU Straps (Sheet 2 of 3)

| # | Parameter | Platform | Settings |
|---|---|---|---|
| 1 | **CPU Straps - CPU Straps** | | |
| | **Disable Hyperthreading**<br>**Values: Yes/No**<br>This setting controls enabling or disabling of Hyper threading. **Note:** This strap is intended for debugging purposes only. See BIOS Spec for more details on enabling / disabling Hyperthreading. | CFL-S<br>CFL-H | No<br>No |
| | **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. **Note:** This strap is intended for debugging purposes only. See BIOS Spec for more details on enabling or disabling processor cores. | CFL-S<br>CFL-H | All<br>All |
| | **Flex Ratio**<br>This setting controls the maximum processor non-turbo ratio. **Note:** This strap is intended for debugging purposes only. See BIOS Spec for more details on maximum processor non-turbo ratio configuration. | CFL-S<br>CFL-H | 0x0<br>0x0 |
| | **Processor Boot Max Frequency**<br>**Values: Yes/No**<br>This setting determines if the processor will operate at maximum frequency at power-on and boot. **Note:** This strap is intended for debugging purposes only. | CFL-S<br>CFL-H | 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. **Note:** This strap is intended for debugging purposes only. | CFL-S<br>CFL-H | No<br>No |
| | **SA Power Plane Topology**<br>This setting determines the SA power plane topology. See Processor EDS for details. **Note:** This strap should be left at the recommended default setting. | CFL-S<br>CFL-H | 0x2<br>0x2 |
| | **SA VR Type**<br>**Value: SVID/Fixed VR**<br>This setting determines the SA core domain VR type. See Processor EDS for details. | CFL-S<br>CFL-H | Fixed VR<br>SVID |
| | **IA Power Plane Topology**<br>This setting determines the IA power plane topology. See Processor EDS for details. **Note:** This strap should be left at the recommended default setting. | CFL-S<br>CFL-H | 0x0<br>0x0 |
| | **IA Power Plane VR**<br>**Value: SVID/Fixed VR**<br>This setting determines the IA core domain VR type. See Processor EDS for details. | CFL-S<br>CFL-H | SVID<br>SVID |
| | **Ring Power Plane Topology**<br>This setting determines the Ring power plane topology. See Processor EDS for details. **Note:** This strap should be left at the recommended default setting. | CFL-S<br>CFL-H | 0x0<br>0x0 |
| | **Ring VR Type**<br>**Value: SVID/Fixed VR**<br>This setting determines the Ring domain VR type. See Processor EDS for details. | CFL-S<br>CFL-H | SVID<br>SVID |
| | **GT_US Power Plane Topology**<br>This setting determines the GT Unslice power plane topology. See Processor EDS for details. **Note:** This strap should be left at the recommended default setting. | CFL-S<br>CFL-H | 0x1<br>0x1 |
| | **GT_US VR Type**<br>**Value: SVID/Fixed VR**<br>This setting determines the GT Unslice domain VR type. See Processor EDS for details. | CFL-S<br>CFL-H | SVID<br>SVID |
| | **GT_S Power Plane Topology**<br>This setting determines the GT slice power plane topology. See Processor EDS for details. **Note:** This strap should be left at the recommended default setting. | CFL-S<br>CFL-H | 0x1<br>0x1 |

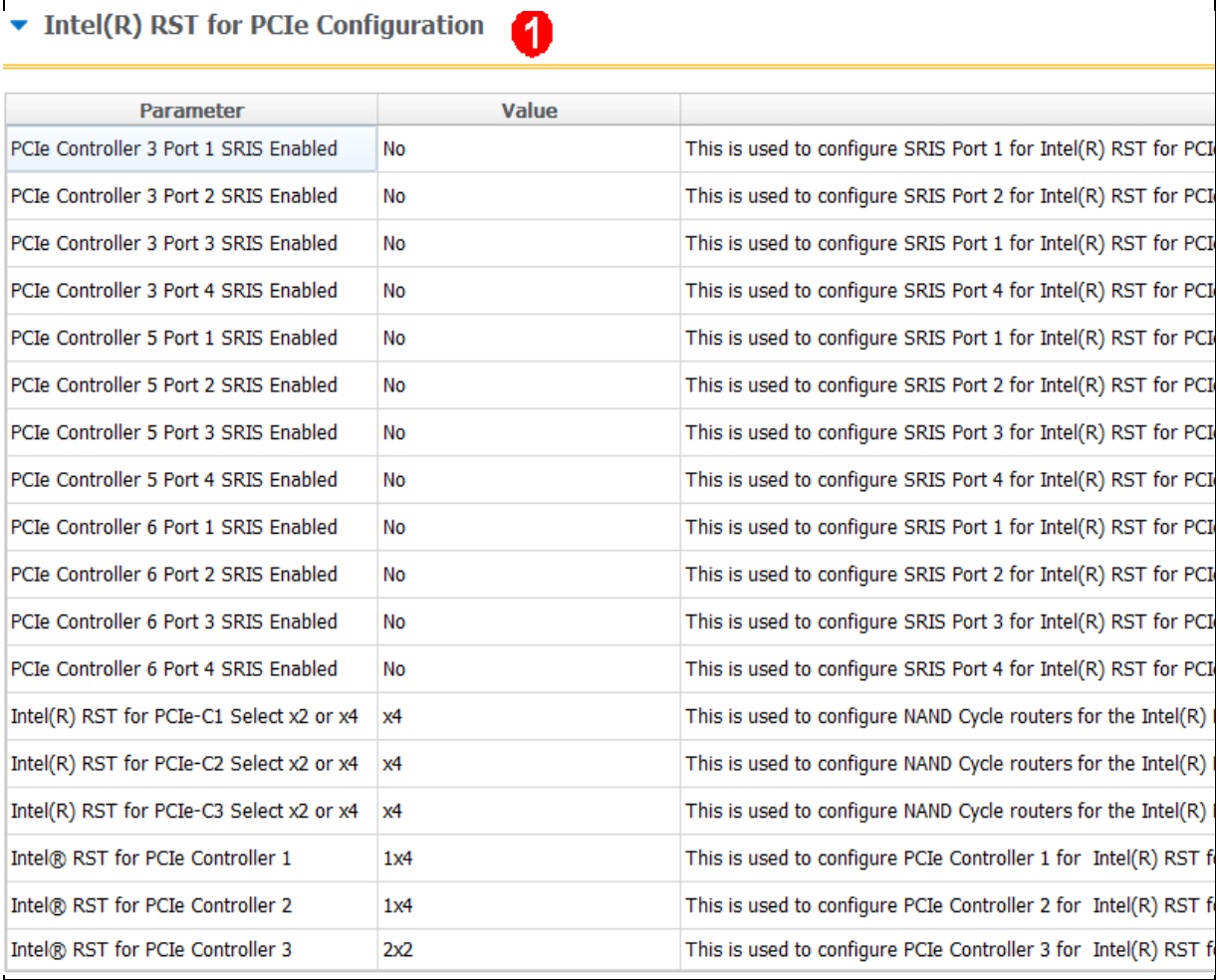


## Table 2-14. - CPU Straps (Sheet 3 of 3)

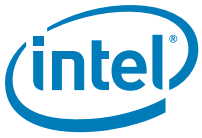
| | | | |
|---|---|---|---|
| | **SVID Presence**<br>**Value: SVID Present/SVID Not Present**<br>This setting determines if SVID rails are present on the platform. See Processor EDS for details. | CFL-S<br>CFL-H | SVID Present<br>SVID Present |
| | **Platform IMON Disable**<br>Also known as Psys.<br>This strap should be left at the recommended default setting. | CFL-S<br>CFL-H | 0x1<br>0x0 |
| | **eOPIO Power Plane Topology**<br>This setting determines the eOPIO power plane topology. See Processor EDS for details. **Note:** This strap should be left at the recommended default setting. | CFL-S<br>CFL-H | 0x0<br>0x0 |
| | **eOPIO VR Type**<br>**Value: SVID/Fixed VR**<br>This setting determines the eOPIO domain VR type. See Processor EDS for details. | CFL-S<br>CFL-H | Fixed VR<br>Fixed VR |
| | **EDRAM Power Plane Topology**<br>This setting determines the EDRAM power plane topology. See Processor EDS for details. **Note:** This strap should be left at the recommended default setting. | CFL-S<br>CFL-H | 0x0<br>0x0 |
| | **EDRAM VR Type**<br>**Value: SVID/Fixed VR**<br>This setting determines the EDRAM domain VR type. See Processor EDS for details. | CFL-S<br>CFL-H | Fixed VR<br>Fixed VR |
| | **SE Key Mode**<br>Note: This strap should be left at the recommended default setting. | CFL-S<br>CFL-H | 0x0<br>0x0 |
| | **GT_S VR Type**<br>**Value: SVID/Fixed VR**<br>This setting determines the GT slice domain VR type. See Processor EDS for details. | CFL-S<br>CFL-H | SVID<br>SVID |
| | **VCCIN SVID Address**<br>This setting determines the VCCIN SVID Address. See Processor EDS for details. **Note:** This strap should be left at the recommended default setting. | CFL-S<br>CFL-H | 0x0<br>0x0 |
| | **VCCIN VR Type**<br>**Value: SVID/Fixed VR**<br>This setting determines the VCCIN VR type. See Processor EDS for details. | CFL-S<br>CFL-H | Fixed VR<br>Fixed VR |
| | **BIST Initialization**<br>**Value: Yes / No**<br>This setting determines if BIST will be run at platform reset after BIOS requested actions.<br><br>***Note:*** This setting is intended for debugging purposes only. | CFL-S<br>CFL-H | No<br>No |

## Table 2-15. - Flex I/O Straps (Sheet 1 of 12)

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




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

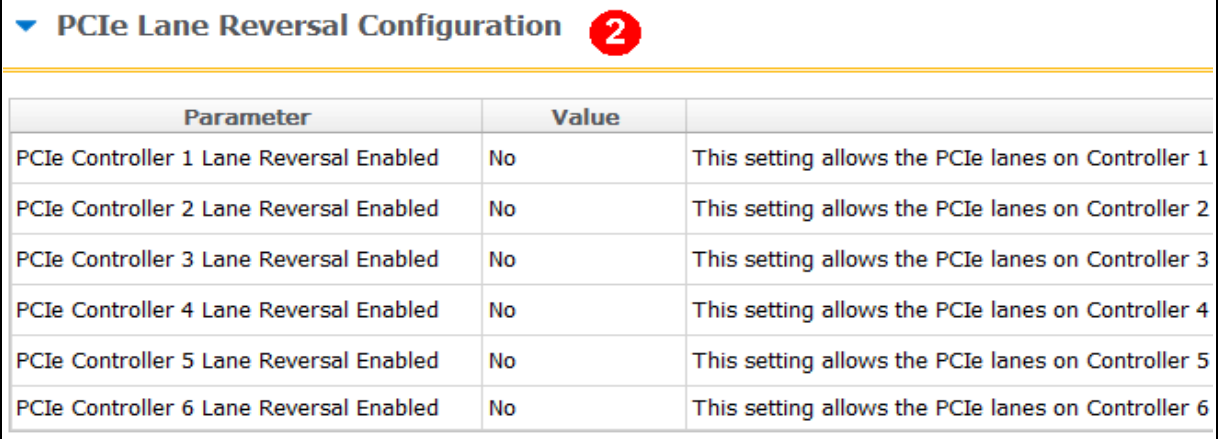


## Table 2-15. - Flex I/O Straps (Sheet 2 of 12)

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

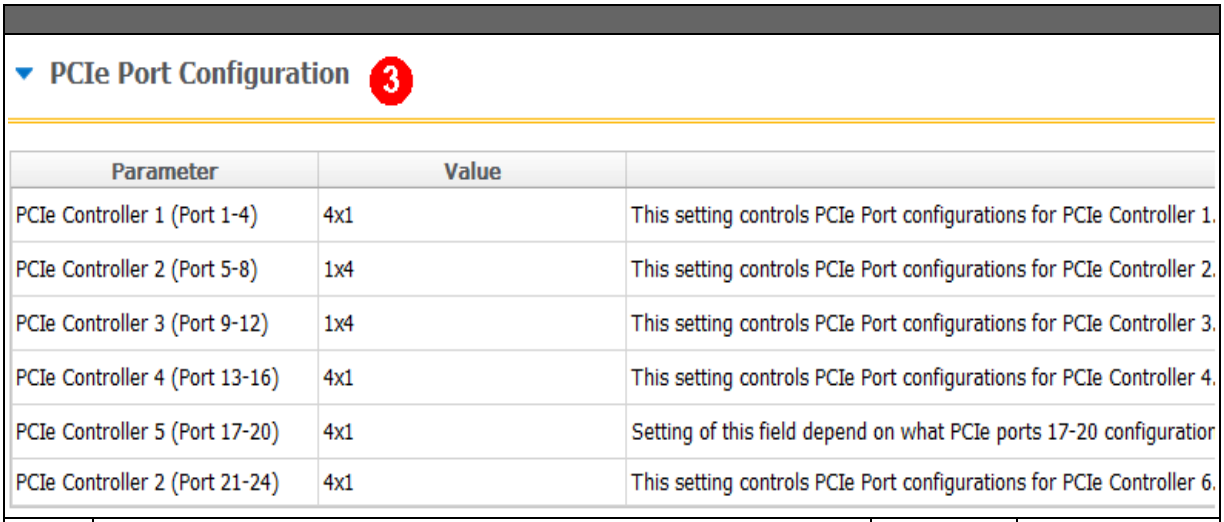
## Table 2-15. - Flex I/O Straps (Sheet 3 of 12)

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




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

## Table 2-15. - Flex I/O Straps (Sheet 4 of 12)



PCIe Port Configuration 3

| Parameter | Value | |
|---|---|---|
| PCIe Controller 1 (Port 1-4) | 4x1 | This setting controls PCIe Port configurations for PCIe Controller 1. |
| PCIe Controller 2 (Port 5-8) | 1x4 | This setting controls PCIe Port configurations for PCIe Controller 2. |
| PCIe Controller 3 (Port 9-12) | 1x4 | This setting controls PCIe Port configurations for PCIe Controller 3. |
| PCIe Controller 4 (Port 13-16) | 4x1 | This setting controls PCIe Port configurations for PCIe Controller 4. |
| PCIe Controller 5 (Port 17-20) | 4x1 | Setting of this field depend on what PCIe ports 17-20 configuratior |
| PCIe Controller 2 (Port 21-24) | 4x1 | This setting controls PCIe Port configurations for PCIe Controller 6. |

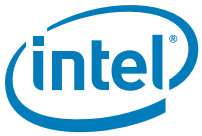
| # | Parameter | Platform | Settings |
|---|---|---|---|
| 3 | **Flex I/O - PCIe Port Configuration** | | |
| | **PCIe Controller 1 (Port 1-4)**<br>**Values: 4x1, (1x2, 2x1), 2x2, 1x4** - This setting controls PCIe Port configurations for PCIe Controller 1. For further details see Cannon Lake H Platform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

## Table 2-15. - Flex I/O Straps (Sheet 5 of 12)

### SATA / PCIe Combo Port Configuration 4

| Parameter | Value | |
|---|---|---|
| SATA / PCIe Combo Port 0 Mode Select | PCIe CLKREQ# | The corresponding CLKREQ# GPIO can only functi |
| SATA / PCIe Combo Port 1 Mode Select | PCIe CLKREQ# | The corresponding CLKREQ# GPIO can only functi |
| SATA / PCIe Combo Port 2 Mode Select | PCIe CLKREQ# | The corresponding CLKREQ# GPIO can only functi |
| SATA / PCIe Combo Port 3 Mode Select | PCIe CLKREQ# | The corresponding CLKREQ# GPIO can only functi |
| SATA / PCIe Combo Port 4 Mode Select | PCIe CLKREQ# | The corresponding CLKREQ# GPIO can only functi |
| SATA / PCIe Combo Port 5 Mode Select | PCIe CLKREQ# | The corresponding CLKREQ# GPIO can only functi |
| SATA / PCIe Combo Port 6 Mode Select | PCIe CLKREQ# | The corresponding CLKREQ# GPIO can only functi |
| SATA / PCIe Combo Port 7 Mode Select | PCIe CLKREQ# | The corresponding CLKREQ# GPIO can only functi |
| SATA / PCIe Combo Port 8 Mode Select | PCIe CLKREQ# | The corresponding CLKREQ# GPIO can only functi |
| SATA / PCIe Combo Port 9 Mode Select | PCIe CLKREQ# | The corresponding CLKREQ# GPIO can only functi |
| SATA / PCIe Combo Port 0 | PCIe | This setting configures the PCIe port to operate as |
| SATA / PCIe Combo Port 1 | GPIO Polarity PCIe | This setting configures the PCIe port to operate as |
| SATA / PCIe Combo Port 2 | PCIe | This setting configures the PCIe port to operate as |
| SATA / PCIe Combo Port 3 | SATA | This setting configures the PCIe port to operate as |
| SATA / PCIe Combo Port 4 | SATA | This setting configures the PCIe port to operate as |
| SATA / PCIe Combo Port 5 | SATA | This setting configures the PCIe port to operate as |
| SATA / PCIe Combo Port 6 | GPIO Polarity PCIe | This setting configures the PCIe port to operate as |
| SATA / PCIe Combo Port 7 | GPIO Polarity PCIe | This setting configures the PCIe port to operate as |
| SATA / PCIe Combo Port 8 | GPIO Polarity PCIe | This setting configures the PCIe port to operate as |
| SATA / PCIe Combo Port 9 | GPIO Polarity PCIe | This setting configures the PCIe port to operate as |

| # | Parameter | Platform | Settings |
|---|---|---|---|
| 4 | **Flex I/O - SATA / PCIe Combo Port Configuration** | | |
| | **SATA / PCIe Combo Port 0 Mode Select**<br>**Values: PCIe CLKREQ#, DEVSLP#**<br>The corresponding CLKREQ# GPIO can only function as DEVSLP# if SATA / PCIe Combo Port 0 is assigned to SATA, and SATA / PCIe Combo Port 0 Mode Select is configured to SATA | CFL-S<br>CFL-H | PCIe CLKREQ#<br>PCIe CLKREQ# |
| | **SATA / PCIe Combo Port 1 Mode Select**<br>**Values: PCIe CLKREQ#, DEVSLP#**<br>The corresponding CLKREQ# GPIO can only function as DEVSLP# if SATA / PCIe Combo Port 0 is assigned to SATA, and SATA / PCIe Combo Port 1 Mode Select is configured to SATA | CFL-S<br>CFL-H | PCIe CLKREQ#<br>PCIe CLKREQ# |

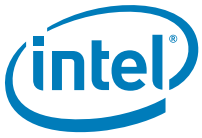


## Table 2-15. - Flex I/O Straps (Sheet 6 of 12)

| | | | |
|---|---|---|---|
| | **SATA / PCIe Combo Port 2 Mode Select**<br>**Values: PCIe CLKREQ#, DEVSLP#**<br>The corresponding CLKREQ# GPIO can only function as DEVSLP# if SATA / PCIe Combo Port 0 is assigned to SATA, and SATA / PCIe Combo Port 2 Mode Select is configured to SATA | CFL-S<br>CFL-H | PCIe CLKREQ#<br>PCIe CLKREQ# |
| | **SATA / PCIe Combo Port 3 Mode Select**<br>**Values: PCIe CLKREQ#, DEVSLP#**<br>The corresponding CLKREQ# GPIO can only function as DEVSLP# if SATA / PCIe Combo Port 0 is assigned to SATA, and SATA / PCIe Combo Port 3 Mode Select is configured to SATA | CFL-S<br>CFL-H | PCIe CLKREQ#<br>PCIe CLKREQ# |
| | **SATA / PCIe Combo Port 4 Mode Select**<br>**Values: PCIe CLKREQ#, DEVSLP#**<br>The corresponding CLKREQ# GPIO can only function as DEVSLP# if SATA / PCIe Combo Port 0 is assigned to SATA, and SATA / PCIe Combo Port 4 Mode Select is configured to SATA | CFL-S<br>CFL-H | PCIe CLKREQ#<br>PCIe CLKREQ# |
| | **SATA / PCIe Combo Port 5 Mode Select**<br>**Values: PCIe CLKREQ#, DEVSLP#**<br>The corresponding CLKREQ# GPIO can only function as DEVSLP# if SATA / PCIe Combo Port 0 is assigned to SATA, and SATA / PCIe Combo Port 5 Mode Select is configured to SATA | CFL-S<br>CFL-H | PCIe CLKREQ#<br>PCIe CLKREQ# |
| | **SATA / PCIe Combo Port 6 Mode Select**<br>**Values: PCIe CLKREQ#, DEVSLP#**<br>The corresponding CLKREQ# GPIO can only function as DEVSLP# if SATA / PCIe Combo Port 0 is assigned to SATA, and SATA / PCIe Combo Port 6 Mode Select is configured to SATA | CFL-S<br>CFL-H | PCIe CLKREQ#<br>PCIe CLKREQ# |
| | **SATA / PCIe Combo Port 7 Mode Select**<br>**Values: PCIe CLKREQ#, DEVSLP#**<br>The corresponding CLKREQ# GPIO can only function as DEVSLP# if SATA / PCIe Combo Port 0 is assigned to SATA, and SATA / PCIe Combo Port 7 Mode Select is configured to SATA | CFL-S<br>CFL-H | PCIe CLKREQ#<br>PCIe CLKREQ# |
| | **SATA / PCIe Combo Port 8 Mode Select**<br>**Values: PCIe CLKREQ#, DEVSLP#**<br>The corresponding CLKREQ# GPIO can only function as DEVSLP# if SATA / PCIe Combo Port 0 is assigned to SATA, and SATA / PCIe Combo Port 8 Mode Select is configured to SATA | CFL-S<br>CFL-H | PCIe CLKREQ#<br>PCIe CLKREQ# |
| | **SATA / PCIe Combo Port 9 Mode Select**<br>**Values: PCIe CLKREQ#, DEVSLP#**<br>The corresponding CLKREQ# GPIO can only function as DEVSLP# if SATA / PCIe Combo Port 0 is assigned to SATA, and SATA / PCIe Combo Port 9 Mode Select is configured to SATA | CFL-S<br>CFL-H | PCIe CLKREQ#<br>PCIe CLKREQ# |
| | **SATA / PCIe Combo Port 0**<br>**Values: SATA, PCIe (or GbE), GPIO** - 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 Cannon Lake H Platform Controller Hub EDS. | CFL-S<br>CFL-H | 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 1a<br>For further details on Flex I/O see Cannon Lake H Platform Controller Hub EDS.<br><br>***Note:*** This port is shared with GbE Port select if PCIe Port 12 has been selected for Intel® Integrated LAN this port setting will be grayed out. | CFL-S<br>CFL-H | PCIe<br>GPIO Polarity PCIe |
| | **SATA / PCIe Combo Port 2**<br>**Values: SATA, PCIe, GPIO Polarity PCIe, GPIO Polarity SATA** - This setting configures the PCIe port to operate as either:<br>PCIe Port 13 or SATA Port 0b<br>For further details on Flex I/O see Cannon Lake H Platform Controller Hub EDS.<br><br>***Note:*** This port is shared with GbE Port select if PCIe Port 13 has been selected for Intel® Integrated LAN this port setting will be grayed out. | CFL-S<br>CFL-H | GbE<br>SATA |

## Table 2-15. - Flex I/O Straps (Sheet 7 of 12)

| | | | |
|---|---|---|---|
| | **SATA / PCIe Combo Port 3**<br>**Values: SATA, PCIe, GPIO Polarity PCIe, GPIO Polarity SATA -** This setting configures the PCIe port to operate as either:<br>PCIe Port 14 or SATA Port 1b<br>For further details on Flex I/O see Cannon Lake H Platform Controller Hub EDS. | CFL-S<br>CFL-H | SATA<br>SATA |
| | **SATA / PCIe Combo Port 4**<br>**Values: SATA, PCIe, GPIO Polarity PCIe, GPIO Polarity SATA -** This setting configures the PCIe port to operate as either:<br>PCIe Port 15 or SATA Port 2<br>For further details on Flex I/O see Cannon Lake H Platform Controller Hub EDS. | CFL-S<br>CFL-H | SATA<br>SATA |
| | **SATA / PCIe Combo Port 5**<br>**Values: SATA, PCIe, GPIO Polarity PCIe, GPIO Polarity SATA -** This setting configures the PCIe port to operate as either:<br>PCIe Port 16 or SATA Port 3<br>For further details on Flex I/O see Cannon Lake H Platform Controller Hub EDS. | CFL-S<br>CFL-H | SATA<br>SATA |
| | **SATA / PCIe Combo Port 6**<br>**Values: SATA, PCIe, GPIO Polarity PCIe, GPIO Polarity SATA -** This setting configures the PCIe port to operate as either:<br>PCIe Port 17 or SATA Port 4<br>For further details on Flex I/O see Cannon Lake H Platform Controller Hub EDS. | CFL-S<br>CFL-H | GPIO Polarity PCIe<br>SATA |
| | **SATA / PCIe Combo Port 7**<br>**Values: SATA, PCIe, GPIO Polarity PCIe, GPIO Polarity SATA -** This setting configures the PCIe port to operate as either:<br>PCIe Port 18 or SATA Port 5<br>For further details on Flex I/O see Cannon Lake H Platform Controller Hub EDS. | CFL-S<br>CFL-H | PCIe<br>SATA |
| | **SATA / PCIe Combo Port 8**<br>**Values: SATA, PCIe, GPIO Polarity PCIe, GPIO Polarity SATA -** This setting configures the PCIe port to operate as either:<br>PCIe Port 19 or SATA Port 6<br>For further details on Flex I/O see Cannon Lake H Platform Controller Hub EDS.<br><br>***Note:*** **Workstation / Server Only** | CFL-S<br>CFL-H | NA<br>NA |
| | **SATA / PCIe Combo Port 9**<br>**Values: SATA, PCIe, GPIO Polarity PCIe, GPIO Polarity SATA -** This setting configures the PCIe port to operate as either:<br>PCIe Port 20 or SATA Port 7<br>For further details on Flex I/O see Cannon Lake H Platform Controller Hub EDS.<br><br>***Note:*** **Workstation / Server Only** | CFL-S<br>CFL-H | NA<br>NA |
| **Click on Flex I/O in the left tabs menu> USB3 Port Configuration is expanded by default:** | | | |



## Table 2-15. - Flex I/O Straps (Sheet 8 of 12)

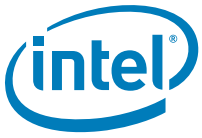
### USB3 Port Configuration

5

| Parameter | Value | |
|---|---|---|
| USB3 / PCIe Combo Port 0 | USB3 | This setting configures the PCIe port to operate as either |
| USB3 / PCIe Combo Port 1 | USB3 | This setting configures the PCIe port to operate as either |
| USB3 / PCIe Combo Port 2 | USB3 | This setting configures the PCIe port to operate as either |
| USB3 / PCIe Combo Port 3 | USB3 | This setting configures the PCIe port to operate as either |
| USB3 Port 1 Connector Type Select | Type C | This setting configures the physical connector type to be |
| USB3 Port 2 Connector Type Select | Type A | This setting configures the physical connector type to be |
| USB3 Port 3 Connector Type Select | Type A | This setting configures the physical connector type to be |
| USB3 Port 4 Connector Type Select | Type A | This setting configures the physical connector type to be |
| USB3 Port 5 Connector Type Select | Type A | This setting configures the physical connector type to be |
| USB3 Port 6 Connector Type Select | Type A | This setting configures the physical connector type to be |
| USB3 Port 7 Connector Type Select | Type A | This setting configures the physical connector type to be |
| USB3 Port 8 Connector Type Select | Type A | This setting configures the physical connector type to be |
| USB3 Port 9 Connector Type Select | Type A | This setting configures the physical connector type to be |
| USB3 Port 10 Connector Type Select | Type A | This setting configures the physical connector type to be |
| USB3 Port 1 Initialization Speed Select | USB3.1 Gen1 LBPM | This setting determines USB3 Port 1 speed during platfor |
| USB3 Port 2 Initialization Speed Select | USB3.1 Gen1 LBPM | This setting determines USB3 Port 2 speed during platfor |
| USB3 Port 3 Initialization Speed Select | USB3.1 Gen1 LBPM | This setting determines USB3 Port 3 speed during platfor |
| USB3 Port 4 Initialization Speed Select | USB3.1 Gen1 LBPM | This setting determines USB3 Port 4 speed during platfor |
| USB3 Port 5 Initialization Speed Select | USB3.1 Gen1 LBPM | This setting determines USB3 Port 5 speed during platfor |
| USB3 Port 6 Initialization Speed Select | USB3.1 Gen1 LBPM | This setting determines USB3 Port 6 speed during platfor |
| USB3 Port 1 Speed Capability | USB 3.1 Gen2 | This setting determines the USB3 Port 1 speed capabilitie |
| USB3 Port 2 Speed Capability | USB 3.1 Gen2 | This setting determines the USB3 Port 2 speed capabilitie |
| USB3 Port 3 Speed Capability | USB 3.1 Gen2 | This setting determines the USB3 Port 3 speed capabilitie |
| USB3 Port 4 Speed Capability | USB 3.1 Gen2 | This setting determines the USB3 Port 4 speed capabilitie |
| USB3 Port 5 Speed Capability | USB 3.1 Gen2 | This setting determines the USB3 Port 5 speed capabilitie |
| USB3 Port 6 Speed Capability | USB 3.1 Gen2 | This setting determines the USB3 Port 6 speed capabilitie |
| USB Type AB Mode Select | USB Type AB HW Select | This setting determines how the USB Type AB connector |

## Table 2-15. - Flex I/O Straps (Sheet 9 of 12)

| # | Parameter | Platform | Settings |
|---|---|---|---|
| 5 | **Flex I/O - USB3 Port Configuration**<br><br>***Note:*** USB Type-C Mux Control: On Cannon / Coffee Lake PCH, device mode is supported on all USB3.1 Type-C ports. EC/PD/PC needs to send a OOB command to the PCH to properly map the USB 2.0 and USB 3.1 signals to the Host controller or Device mode controller when a connection is detected on the Type-C port. Without these OOB message, the USB2.0/ 3.1 signals may not be correctly mapped and the USB functionality may be impacted. For more detail, see Cannon Lake and Coffee Lake Platform USB Type-C Mux Control Over eSPI doc # 570737. | | |
| | **USB3 / PCIe Combo Port 0**<br>**Values: USB3, PCIe**<br>This setting configures the PCIe port to operate as either:<br>PCIe Port 1 or USB3 Port 1<br><br>For further details on Flex I/O see Cannon Lake H Platform Controller Hub EDS.<br><br>***Note:*** If DCI BSSB for this USB3 Combo port it will be Grayed out. | CFL-S<br>CFL-H | USB3<br>USB3 |
| | **USB3 / PCIe Combo Port 1**<br>**Values: USB3, PCIe**<br>This setting configures the PCIe port to operate as either:<br>PCIe Port 2 or USB3 Port 2<br><br>For further details on Flex I/O see Cannon Lake H Platform Controller Hub EDS.<br><br>***Note:*** If DCI BSSB for this USB3 Combo port it will be Grayed out. | CFL-S<br>CFL-H | USB3<br>USB3 |
| | **USB3 / PCIe Combo Port 2**<br>**Values: USB3, PCIe**<br>This setting configures the PCIe port to operate as either:<br>PCIe Port 3 or USB3 Port 3<br><br>For further details on Flex I/O see Cannon Lake H Platform Controller Hub EDS.<br><br>***Note:*** If DCI BSSB for this USB3 Combo port it will be Grayed out. | CFL-S<br>CFL-H | PCIe<br>USB3 |
| | **USB3 / PCIe Combo Port 3**<br>**Values: USB3, PCIe**<br>This setting configures the PCIe port to operate as either:<br>PCIe 4 or USB3 Port 4<br><br>For further details on Flex I/O see Cannon Lake H Platform Controller Hub EDS.<br><br>***Note:*** If DCI BSSB for this USB3 Combo port it will be Grayed out. | CFL-S<br>CFL-H | USB3<br>USB3 |
| | **USB3 Port 1 Connector Type Select**<br>**Values: Type C, Micro AB, Type A, Type B, Express Card / M.2 S2**<br>This setting configures the physical connector type to be used for USB 3.1 Port 1. | CFL-S<br>CFL-H | Type A<br>Type A |
| | **USB3 Port 2 Connector Type Select**<br>**Values: Type C, Micro AB, Type A, Type B, Express Card / M.2 S2**<br>This setting configures the physical connector type to be used for USB 3.1 Port 2. | CFL-S<br>CFL-H | Type A<br>Type A |
| | **USB3 Port 3 Connector Type Select**<br>**Values: Type C, Micro AB, Type A, Type B, Express Card / M.2 S2**<br>This setting configures the physical connector type to be used for USB 3.1 Port 3. | CFL-S<br>CFL-H | Type A<br>Type A |



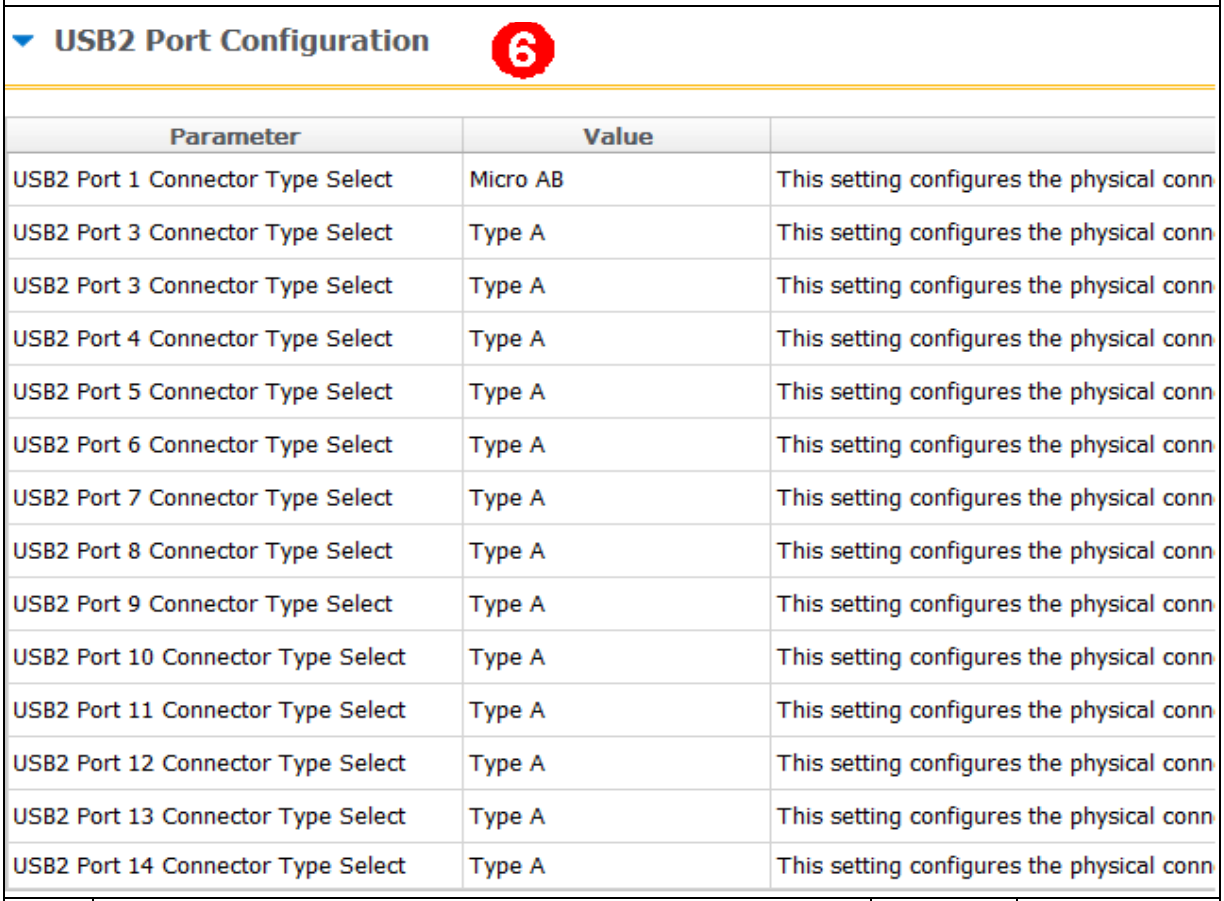
## Table 2-15. - Flex I/O Straps (Sheet 10 of 12)

| | | | |
|---|---|---|---|
| | **USB3 Port 4 Connector Type Select**<br>**Values: Type C, Micro AB, Type A, Type B, Express Card / M.2 S2**<br>This setting configures the physical connector type to be used for USB 3.1 Port 4. | CFL-S<br>CFL-H | Type A<br>Type A |
| | **USB3 Port 5 Connector Type Select**<br>**Values: Type C, Micro AB, Type A, Type B, Express Card / M.2 S2**<br>This setting configures the physical connector type to be used for USB 3.1 Port 5. | CFL-S<br>CFL-H | Type A<br>Type A |
| | **USB3 Port 6 Connector Type Select**<br>**Values: Type C, Micro AB, Type A, Type B, Express Card / M.2 S2**<br>This setting configures the physical connector type to be used for USB 3.1 Port 6. | CFL-S<br>CFL-H | Type A<br>Type A |
| | **USB3 Port 7 Connector Type Select**<br>**Values: Type C, Micro AB, Type A, Type B, Express Card / M.2 S2**<br>This setting configures the physical connector type to be used for USB 3.1 Port 7. | CFL-S<br>CFL-H | Type A<br>Type A |
| | **USB3 Port 8 Connector Type Select**<br>**Values: Type C, Micro AB, Type A, Type B, Express Card / M.2 S2**<br>This setting configures the physical connector type to be used for USB 3.1 Port 8. | CFL-S<br>CFL-H | Type A<br>Type A |
| | **USB3 Port 9 Connector Type Select**<br>**Values: Type C, Micro AB, Type A, Type B, Express Card / M.2 S2**<br>This setting configures the physical connector type to be used for USB 3.1 Port 9. | CFL-S<br>CFL-H | Express Card / M.2<br>Type A |
| | **USB3 Port 10 Connector Type Select**<br>**Values: Type C, Micro AB, Type A, Type B, Express Card / M.2 S2**<br>This setting configures the physical connector type to be used for USB 3.1 Port 10. | CFL-S<br>CFL-H | Type A<br>Type A |
| | **USB3 Port 1 Initialization Speed Select**<br>**Values: USB3.1 Gen1 LBPM, USB3.1 Gen2 Skip LBPM**<br>This setting determines USB3 Port 1 speed during platform power-up. | CFL-S<br>CFL-H | USB3.1 Gen1 LBPM<br>USB3.1 Gen1 LBPM |
| | **USB3 Port 2 Initialization Speed Select**<br>**Values: USB3.1 Gen1 LBPM, USB3.1 Gen2 Skip LBPM**<br>This setting determines USB3 Port 2 speed during platform power-up. | CFL-S<br>CFL-H | USB3.1 Gen1 LBPM<br>USB3.1 Gen1 LBPM |
| | **USB3 Port 3 Initialization Speed Select**<br>**Values: USB3.1 Gen1 LBPM, USB3.1 Gen2 Skip LBPM**<br>This setting determines USB3 Port 3 speed during platform power-up. | CFL-S<br>CFL-H | USB3.1 Gen1 LBPM<br>USB3.1 Gen1 LBPM |
| | **USB3 Port 4 Initialization Speed Select**<br>**Values: USB3.1 Gen1 LBPM, USB3.1 Gen2 Skip LBPM**<br>This setting determines USB3 Port 4 speed during platform power-up. | CFL-S<br>CFL-H | USB3.1 Gen1 LBPM<br>USB3.1 Gen1 LBPM |
| | **USB3 Port 5 Initialization Speed Select**<br>**Values: USB3.1 Gen1 LBPM, USB3.1 Gen2 Skip LBPM**<br>This setting determines USB3 Port 5 speed during platform power-up. | CFL-S<br>CFL-H | USB3.1 Gen1 LBPM<br>USB3.1 Gen1 LBPM |
| | **USB3 Port 6 Initialization Speed Select**<br>**Values: USB3.1 Gen1 LBPM, USB3.1 Gen2 Skip LBPM**<br>This setting determines USB3 Port 6 speed during platform power-up. | CFL-S<br>CFL-H | USB3.1 Gen1 LBPM<br>USB3.1 Gen1 LBPM |
| | **USB3 Port 1 Speed Capability**<br>**Values: USB3.1 Gen1, USB3.1 Gen2**<br>This setting determines the USB3 Port 1 speed capabilities. | CFL-S<br>CFL-H | USB 3.1 Gen2<br>USB 3.1 Gen2 |
| | **USB3 Port 2 Speed Capability**<br>**Values: USB3.1 Gen1, USB3.1 Gen2**<br>This setting determines the USB3 Port 2 speed capabilities. | CFL-S<br>CFL-H | USB 3.1 Gen2<br>USB 3.1 Gen2 |
| | **USB3 Port 3 Speed Capability**<br>**Values: USB3.1 Gen1, USB3.1 Gen2**<br>This setting determines the USB3 Port 3 speed capabilities. | CFL-S<br>CFL-H | USB 3.1 Gen2<br>USB 3.1 Gen2 |

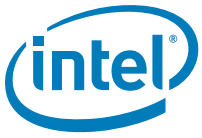
## Table 2-15. - Flex I/O Straps (Sheet 11 of 12)

| | | | |
|---|---|---|---|
| | **USB3 Port 4 Speed Capability**<br>**Values: USB3.1 Gen1, USB3.1 Gen2**<br>This setting determines the USB3 Port 4 speed capabilities. | CFL-S<br>CFL-H | USB 3.1 Gen2<br>USB 3.1 Gen2 |
| | **USB3 Port 5 Speed Capability**<br>**Values: USB3.1 Gen1, USB3.1 Gen2**<br>This setting determines the USB3 Port 5 speed capabilities. | CFL-S<br>CFL-H | USB 3.1 Gen2<br>USB 3.1 Gen2 |
| | **USB3 Port 6 Speed Capability**<br>**Values: USB3.1 Gen1, USB3.1 Gen2**<br>This setting determines the USB3 Port 6 speed capabilities. | CFL-S<br>CFL-H | USB 3.1 Gen2<br>USB 3.1 Gen2 |
| | **USB Type AB Mode Select**<br>**Values: USB Type AB SW Select, USB Type AB HW Select**<br>This setting determines how the USB Type AB connector switching is handled. | CFL-S<br>CFL-H | 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 |
|---|---|---|---|
| 6 | **Flex I/O - USB2 Port Configuration** | | |
| | **USB2 Port 1 Connector Type**<br>This setting configures the physical connector type to be used for USB2 Port 1. | CFL-S<br>CFL-H | Type A<br>Type A |
| | **USB2 Port 2 Connector Type**<br>This setting configures the physical connector type to be used for USB2 Port 2. | CFL-S<br>CFL-H | Type A<br>Type A |

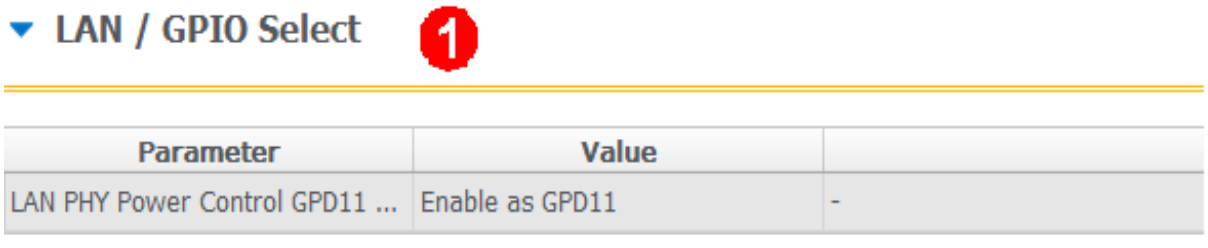


## Table 2-15. - Flex I/O Straps (Sheet 12 of 12)

| | | | |
|---|---|---|---|
| | **USB2 Port 3 Connector Type**<br>This setting configures the physical connector type to be used for USB2 Port 3. | CFL-S<br>CFL-H | Type A<br>Type A |
| | **USB2 Port 4 Connector Type**<br>This setting configures the physical connector type to be used for USB2 Port 4. | CFL-S<br>CFL-H | Type A<br>Type A |
| | **USB2 Port 5 Connector Type**<br>This setting configures the physical connector type to be used for USB2 Port 5. | CFL-S<br>CFL-H | Type A<br>Type A |
| | **USB2 Port 6 Connector Type**<br>This setting configures the physical connector type to be used for USB2 Port 6. | CFL-S<br>CFL-H | Type A<br>Type A |
| | **USB2 Port 7 Connector Type**<br>This setting configures the physical connector type to be used for USB2 Port 7. | CFL-S<br>CFL-H | Type A<br>Type A |
| | **USB2 Port 8 Connector Type**<br>This setting configures the physical connector type to be used for USB2 Port 8. | CFL-S<br>CFL-H | Type A<br>Type A |
| | **USB2 Port 9 Connector Type**<br>This setting configures the physical connector type to be used for USB2 Port 9. | CFL-S<br>CFL-H | Express Card / M.2<br>Type A |
| | **USB2 Port 10 Connector Type**<br>This setting configures the physical connector type to be used for USB2 Port 10. | CFL-S<br>CFL-H | Type A<br>Type A |
| | **USB2 Port 11 Connector Type**<br>This setting configures the physical connector type to be used for USB2 Port 11. | CFL-S<br>CFL-H | Type A<br>Type A |
| | **USB2 Port 12 Connector Type**<br>This setting configures the physical connector type to be used for USB2 Port 12. | CFL-S<br>CFL-H | Type A<br>Type A |
| | **USB2 Port 13 Connector Type**<br>This setting configures the physical connector type to be used for USB2 Port 13. | CFL-S<br>CFL-H | Type A<br>Type A |
| | **USB2 Port 14 Connector Type**<br>This setting configures the physical connector type to be used for USB2 Port 14. | CFL-S<br>CFL-H | Type A<br>Express Card / M.2 |

## Table 2-16. - GPIO (Sheet 1 of 4)

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



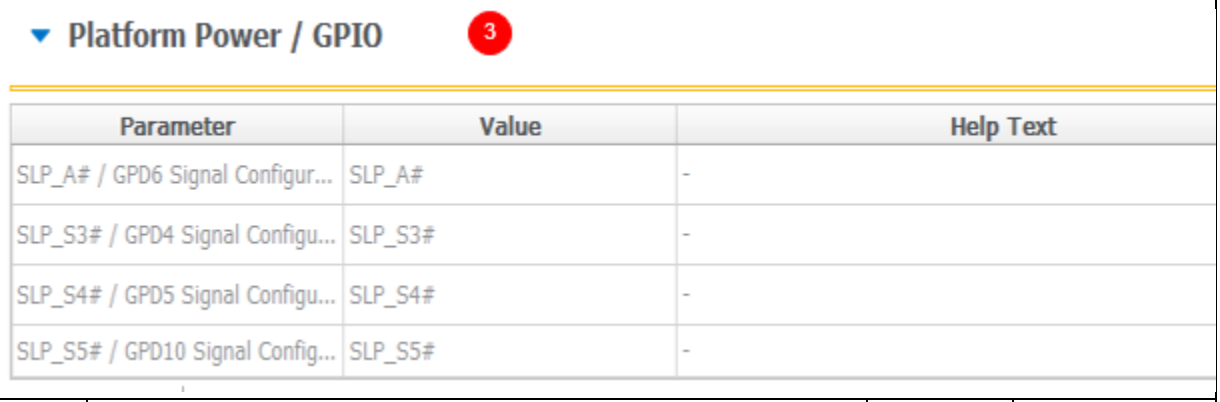

| # | Parameter | Platform | Settings |
|---|---|---|---|
| 1 | **GPIO - LAN / GPIO Select** | | |
| | **LAN PHY Power Control GPD11 Signal Configuration** | CFL-S<br>CFL-H | LANPHYPC<br>LANPHYPC |

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




| # | Parameter | Platform | Settings |
|---|---|---|---|
| 2 | **GPIO - WLAN / GPIO Select** | | |
| | **SLP_WLAN# / GPD9 Signal Configuration** | CFL-S<br>CFL-H | SLP_WLAN#<br>SLP_WLAN# |

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

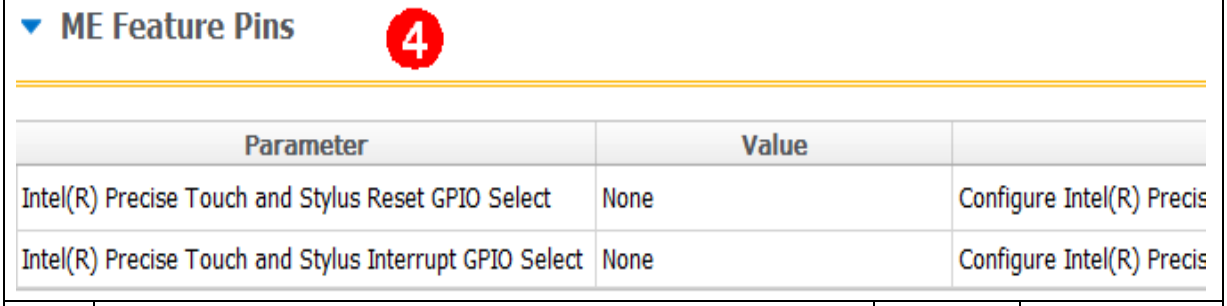



| # | Parameter | Platform | Settings |
|---|---|---|---|

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

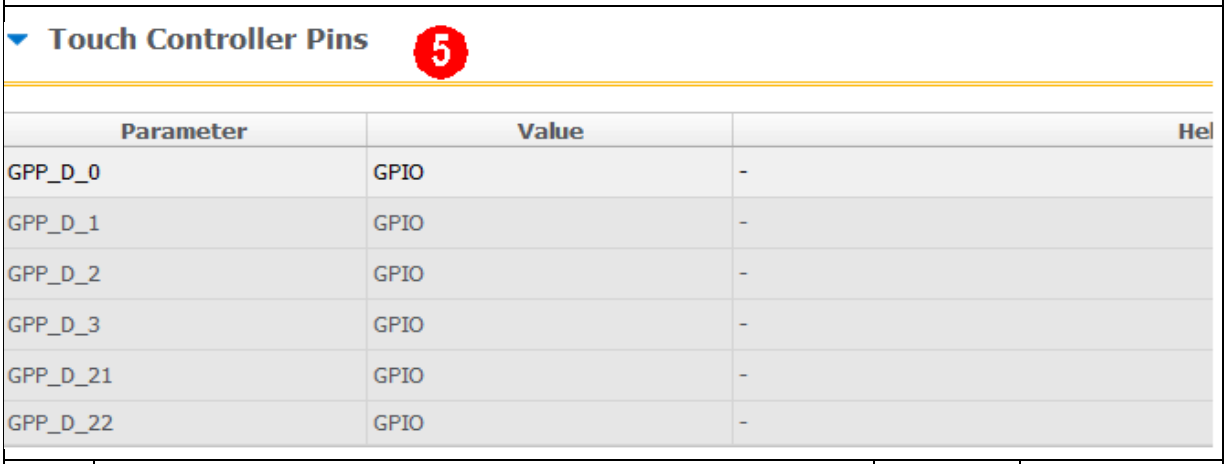
| | | | |
|---|---|---|---|
| 3 | **GPIO - Platform Power / GPIO** | | |
| | **SLP_A# / GPD6 Signal Configuration** | CFL-S<br>CFL-H | SLP_A#<br>SLP_A# |
| | **SLP_S3# / GPD4 Signal Configuration** | CFL-S<br>CFL-H | SLP_S3#<br>SLP_S3# |
| | **SLP_S4# / GPD5 Signal Configuration** | CFL-S<br>CFL-H | SLP_S4#<br>SLP_S4# |
| | **SLP_S5# / GPD10 Signal Configuration** | CFL-S<br>CFL-H | SLP_S5#<br>SLP_S5# |

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




| # | Parameter | Platform | Settings |
|---|---|---|---|
| 4 | **GPIO - ME Feature Pins** | | |
| | **Intel® Precise Touch and Stylus Reset GPIO Select**<br>Configure Intel® Precise Touch and Stylus Reset GPIO. | CFL-S<br>CFL-H | None<br>None |
| | **Intel® Precise Touch and Stylus Interrupt GPIO Select**<br>Configure Intel® Precise Touch and Stylus Interrupt GPIO. | CFL-S<br>CFL-H | None<br>None |

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

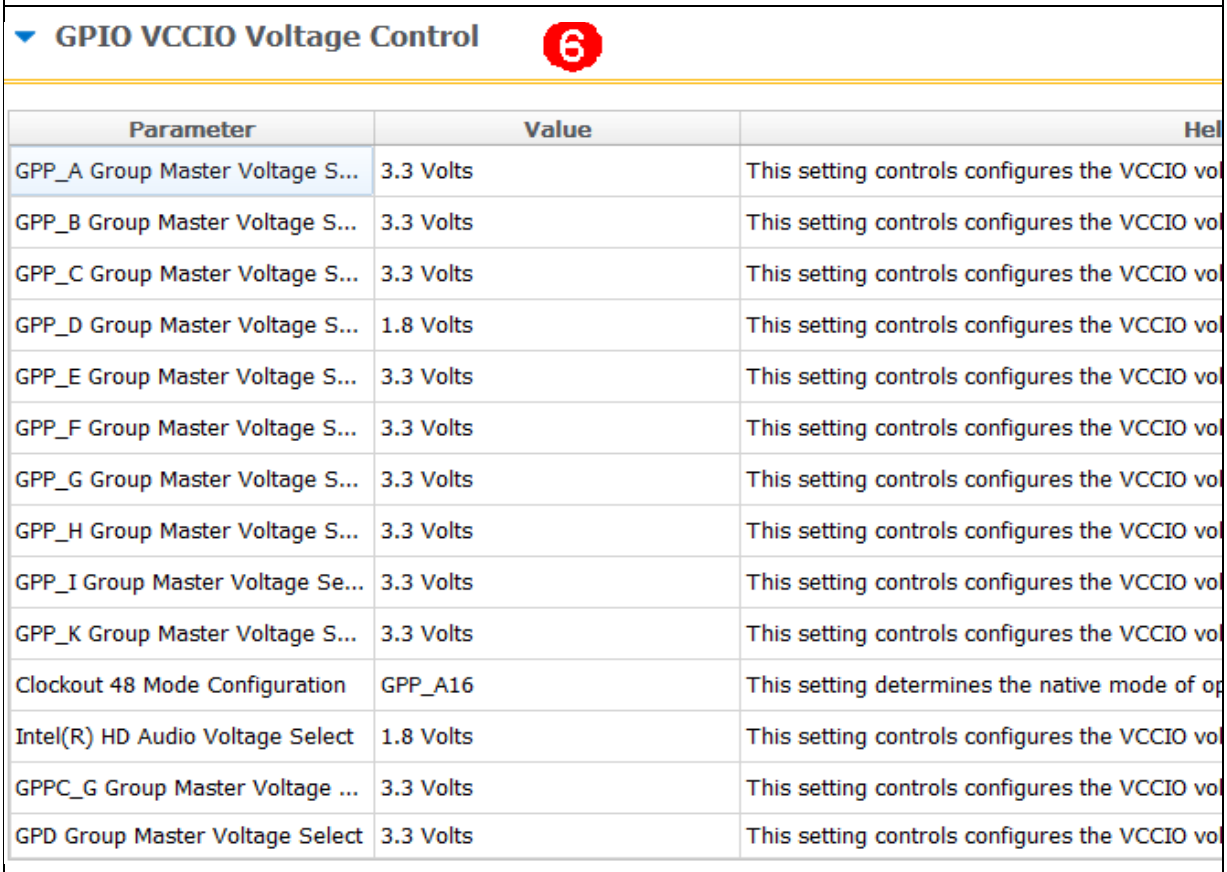



| # | Parameter | Platform | Settings |
|---|---|---|---|

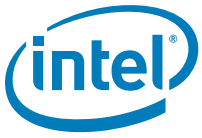
## Table 2-16. - GPIO (Sheet 3 of 4)

| | | | |
|---|---|---|---|
| 5 | **GPIO - Touch Controller Pins** | | |
| | **GPP_D_0** | CFL-S<br>CFL-H | GPIO<br>GPIO |
| | **GPP_D_1** | CFL-S<br>CFL-H | GPIO<br>GPIO |
| | **GPP_D_2** | CFL-S<br>CFL-H | GPIO<br>GPIO |
| | **GPP_D_3** | CFL-S<br>CFL-H | GPIO<br>GPIO |
| | **GPP_D_21** | CFL-S<br>CFL-H | GPIO<br>GPIO |
| | **GPP_D_22** | CFL-S<br>CFL-H | GPIO<br>GPIO |

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




| # | Parameter | Platform | Settings |
|---|---|---|---|
| 6 | **GPIO - GPIO VCCIO Voltage Control**<br><br>***Warning:*** Incorrectly configuring GPIO voltages may result in MCP damage. | | |



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

| | | | |
|---|---|---|---|
| | **GPP_A Group Master Voltage Select**<br>**Values: 3.3 Volts, 1.8 Volts**<br>This setting configures the VCCIO voltage of all the GPP_A GPIO pins. | CFL-S<br>CFL-H | 3.3 Volts<br>3.3 Volts |
| | **GPP_B Group Master Voltage Select**<br>**Values: 3.3 Volts, 1.8 Volts**<br>This setting configures the VCCIO voltage of all the GPP_B GPIO pins. | CFL-S<br>CFL-H | 3.3 Volts<br>3.3 Volts |
| | **GPP_C Group Master Voltage Select**<br>**Values: 3.3 Volts, 1.8 Volts**<br>This setting configures the VCCIO voltage of all the GPP_C GPIO pins. | CFL-S<br>CFL-H | 3.3 Volts<br>3.3 Volts |
| | **GPP_D Group Master Voltage Select**<br>**Values: 3.3 Volts, 1.8 Volts**<br>This setting configures the VCCIO voltage of all the GPP_D GPIO pins. | CFL-S<br>CFL-H | 1.8 Volts<br>1.8 Volts |
| | **GPP_E Group Master Voltage Select**<br>**Values: 3.3 Volts, 1.8 Volts**<br>This setting configures the VCCIO voltage of all the GPP_E GPIO pins. | CFL-S<br>CFL-H | 3.3 Volts<br>3.3 Volts |
| | **GPP_F Group Master Voltage Select**<br>**Values: 3.3 Volts, 1.8 Volts**<br>This setting configures the VCCIO voltage of all the GPP_F GPIO pins. | CFL-S<br>CFL-H | 3.3 Volts<br>3.3 Volts |
| | **GPP_G Group Master Voltage Select**<br>**Values: 3.3 Volts, 1.8 Volts**<br>This setting configures the VCCIO voltage of all the GPP_G GPIO pins. | CFL-S<br>CFL-H | 3.3 Volts<br>3.3 Volts |
| | **GPP_H Group Master Voltage Select**<br>**Values: 3.3 Volts, 1.8 Volts**<br>This setting configures the VCCIO voltage of all the GPP_H GPIO pins. | CFL-S<br>CFL-H | 3.3 Volts<br>3.3 Volts |
| | **GPP_I Group Master Voltage Select**<br>**Values: 3.3 Volts, 1.8 Volts**<br>This setting configures the VCCIO voltage of all the GPP_I GPIO pins. | CFL-S<br>CFL-H | 3.3 Volts<br>3.3 Volts |
| | **GPP_K Group Master Voltage Select**<br>**Values: 3.3 Volts, 1.8 Volts**<br>This setting configures the VCCIO voltage of all the GPP_K GPIO pins. | CFL-S<br>CFL-H | 3.3 Volts<br>3.3 Volts |
| | **Clockout 48 Mode Configuration**<br>**Values: 3.3 Volts, 1.8 Volts**<br>This setting determines the mode of operation for the CLKOUT_48 signal. | CFL-S<br>CFL-H | CLKOUT_48<br>GPP_A16 |
| | **Intel® HD Audio Voltage Configuration**<br>**Values: 3.3 Volts, 1.8 Volts**<br>This setting configures the VCCIO voltage for the Intel® HD Audio GPIO pins. | CFL-S<br>CFL-H | 1.8 Volts<br>1.8 Volts |
| | **GPPC_G Group Master Voltage Select**<br>**Values: 3.3 Volts, 1.8 Volts**<br>This setting configures the VCCIO voltage of all the GPP_G GPIO pins. | CFL-S<br>CFL-H | 3.3 Volts<br>3.3 Volts |
| | **GDP Group Master Voltage Select**<br>**Values: 3.3 Volts, 1.8 Volts.**<br>This setting configures the VCCIO voltage of all the GDP GPIO pins | CFL-S<br>CFL-H | 3.3 Volts<br>3.3 Volts |

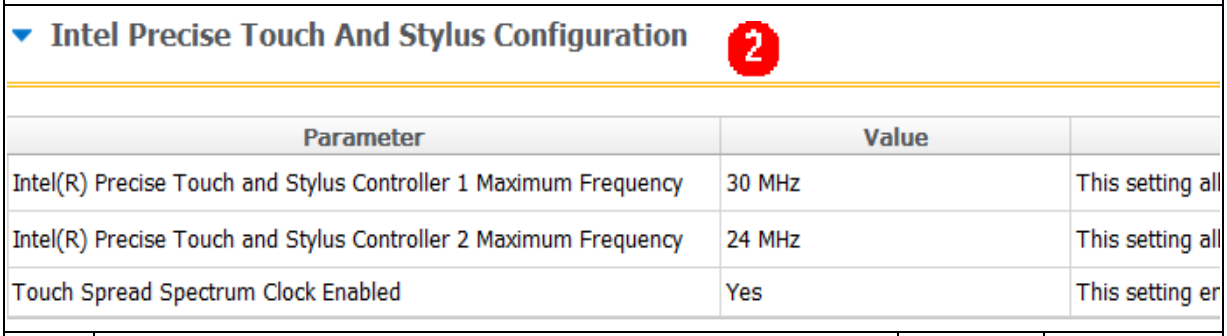
## Table 2-17. - Intel® Precise Touch and Stylus

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



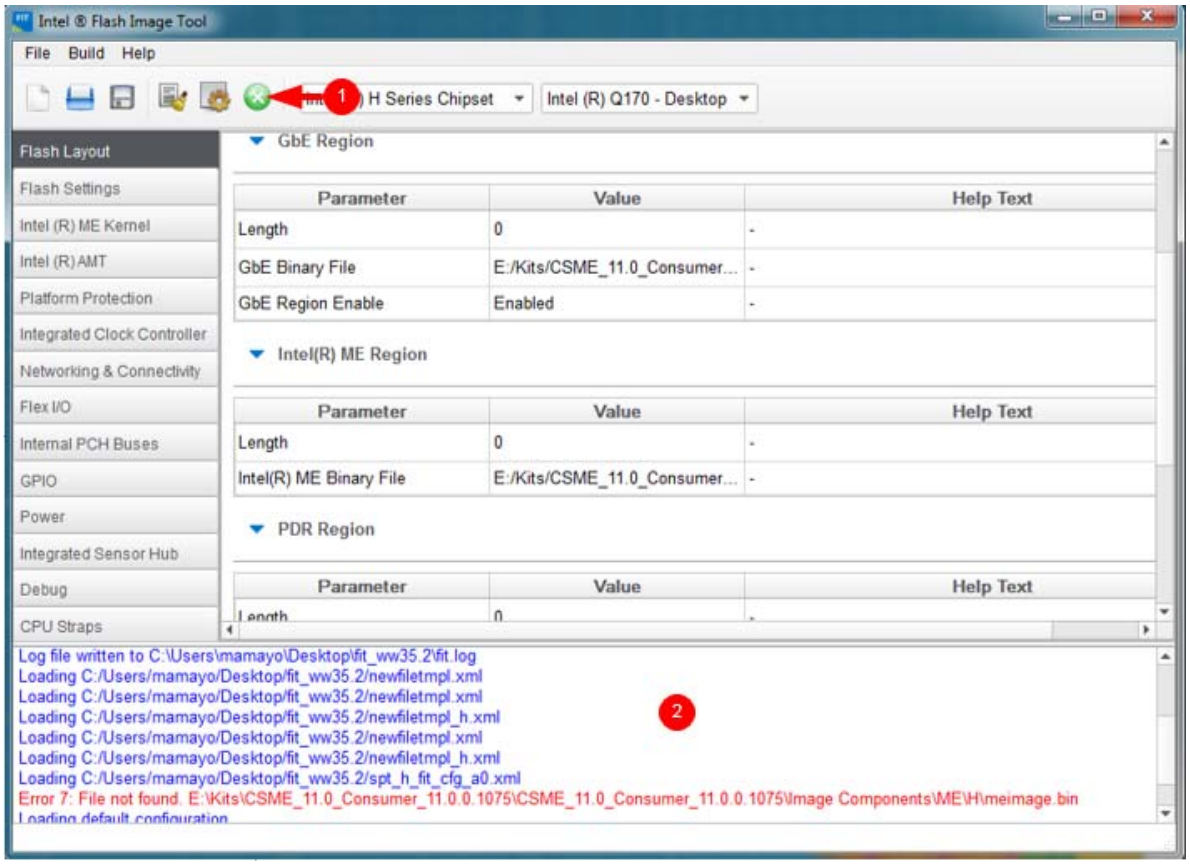

| # | Parameter | Platform | Settings |
|---|---|---|---|
| 1 | **Intel® Precise Touch and Stylus - IntegratedTouchConfiguration** | | |
| | **Intel® Precise Touch and Stylus Enabled** | CFL-S<br>CFL-H | No<br>No |

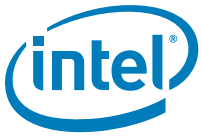
**Click on Intel® Precise Touch and Stylus in the left tabs menu> IntegratedTouchAndStylusConfiguration is expanded by default:**




| | | | |
|---|---|---|---|
| 2 | **Intel® Precise Touch and Stylus - Intel PerciseTouch and Stylus Configuration** | | |
| | **Intel® Precise Touch and Stylus Controller 1 Maximum Frequency** | CFL-S<br>CFL-H | 30MHz<br>30MHz |
| | **Intel® Precise Touch and Stylus Controller 2 Maximum Frequency**<br>**Values: 17 MHz, 24 MHZ, 30 MHz, 48 MHz**<br>This setting configures the maximum frequency for Intel® Precise Touch and Stylus Controller 2. | CFL-S<br>CFL-H | 24MHz<br>24MHz |
| | **Touch Spread Spectrum Clock Enabled**<br>**Values: Yes / No**<br>This setting enabled the use of the spread spectrum clock when generating the SPI_CLK for touch. | CFL-S<br>CFL-H | Yes<br>Yes |

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

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



# 3 Programming SPI Flash Devices and Checking Firmware Status

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

## 3.1 Flash Burner/Programmer

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

1. Navigate to your **Output Directory** (as specified in Table 2.2) where your generated SPI Flash image(s) are saved. It is assumed that this image file is named **outimage.bin**.

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

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

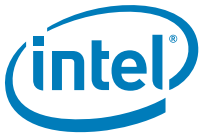
Mobile CRBs have the SPI Flash devices soldered down. As a result, to program the SPI Flash for mobile CRBs, follow these steps:

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

## 3.2 Flash Programming Tool (Intel® FPT)

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

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



### Intel® FPT DOS Version

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

1. Copy all the files in the "(root)\Tools\System Tools\Flash Programming Tool\DOS" directory to the root directory of a bootable USB key.
2. Navigate to your **Output Directory** (as specified in Table 2.2) where your generated SPI Flash image(s) are saved. It is assumed that this image file is named **outimage.bin**. Copy this image file to the root directory of the USB key.
3. Boot the target system to DOS and change to the root directory of the bootable USB key. At the DOS prompt type:

```
fpt.exe -i
```

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

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

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

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

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

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

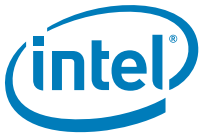
```
FPT Operation Passed
```

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

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

## 3.2.1 Intel® FPT Windows* Version

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



Use the following steps to program the SPI Flash devices,

1. Navigate to your **Output Directory** (as specified in Table 2.2) where your generated SPI Flash image(s) are saved. It is assumed that this image file is named **outimage.bin**. Copy this image file to Intel® FPT directory located at "(root)\Tools\System Tools\Flash Programming Tool\Windows".
2. Boot the target system to Windows* and open a Command Prompt window. In this window, change to the Intel® FPT directory and at the prompt type:

```
fptw.exe -i
```

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

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

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

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

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

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

```
FPT Operation Passed
```

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

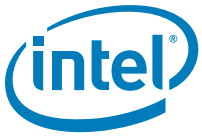
4. Use fptw.exe -greset to perform a G3 power cycle. Next go to Section 3.3 to check the Intel® ME Firmware status.

## 3.3 Checking Intel® ME Firmware Status

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

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

```
MEInfo.exe -fwsts
```



The system should respond with a message similar to below.

```
Intel® MEInfo Version: 12.0.0.xxxx

Copyright(C) 2005 - 2014, Intel Corporation. All rights reserved.

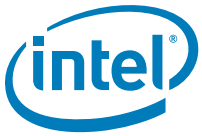
FW Status Register1: 0x1E000255
FW Status Register2: 0x60002306
FW Status Register3: 0x00000300
FW Status Register4: 0x00004001
FW Status Register5: 0x00000101
FW Status Register6: 0x03C00FC9

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

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

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

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



## 3.4 Common Bring Up Issues and Troubleshooting Table

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

| Problem / Issue | Solution / Workaround |
|---|---|
| System does not boot to DOS | By default, the system will boot to EFI Shell. To boot to DOS,<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®*Cannon Lake PCH-H / LP Clocks* and *Intel® Management Engine — Platform Compliancy Guide for ME Hardware*.

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

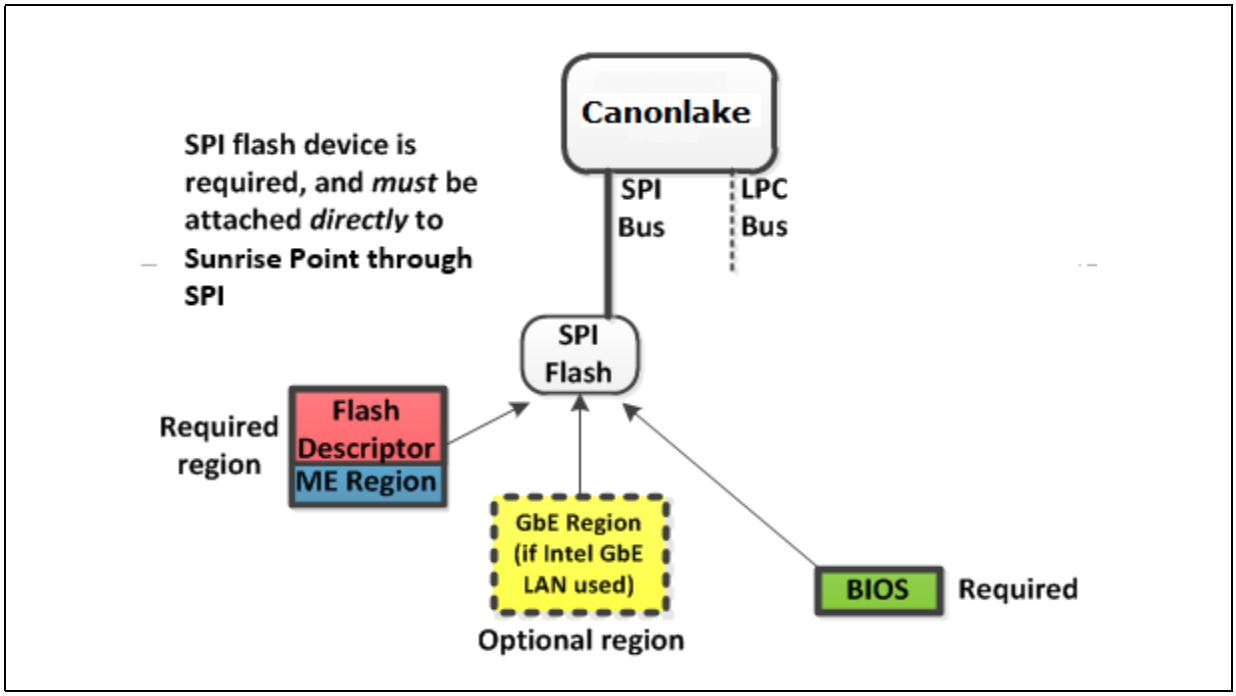


Figure A-2. Configuration "B" — Mobile Only

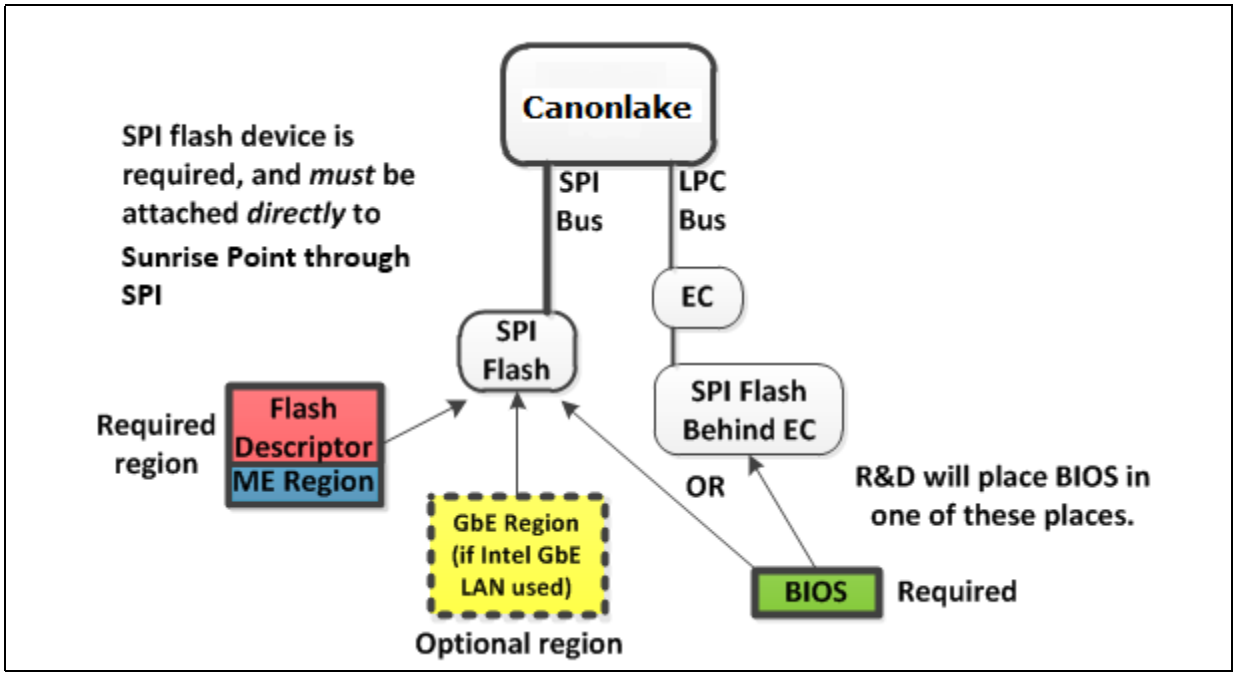



Figure A-3. Configuration "C" — Desktop / Server / Workstation Only

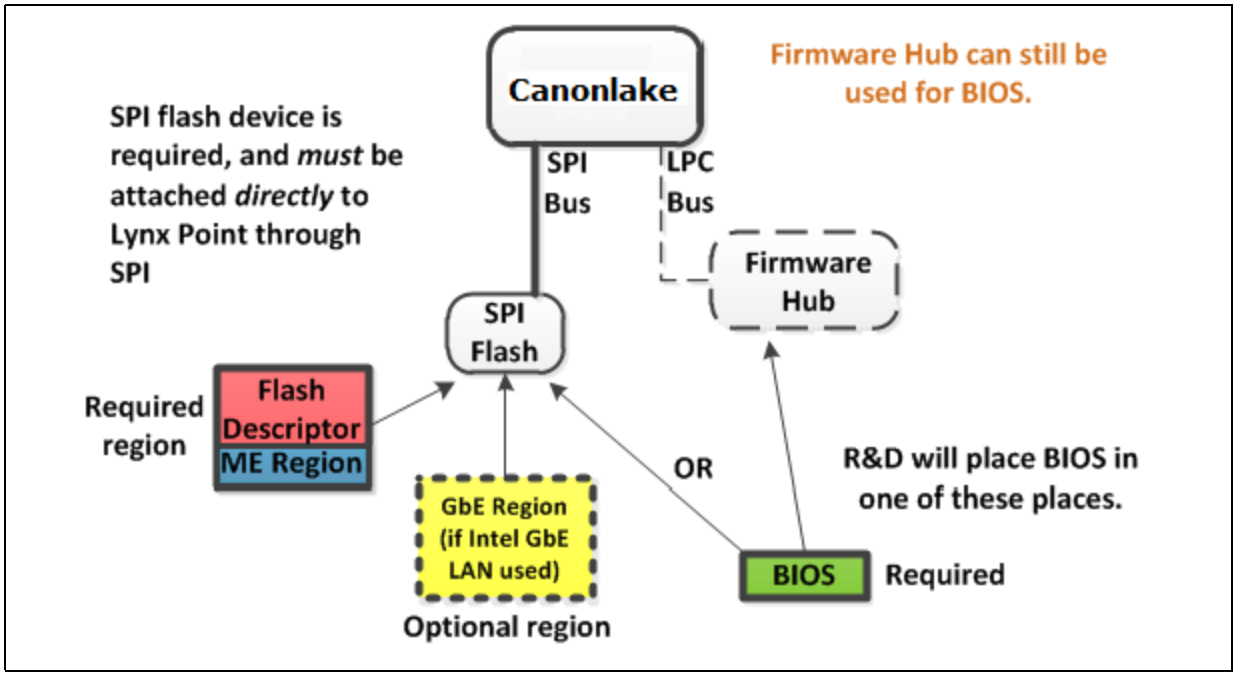
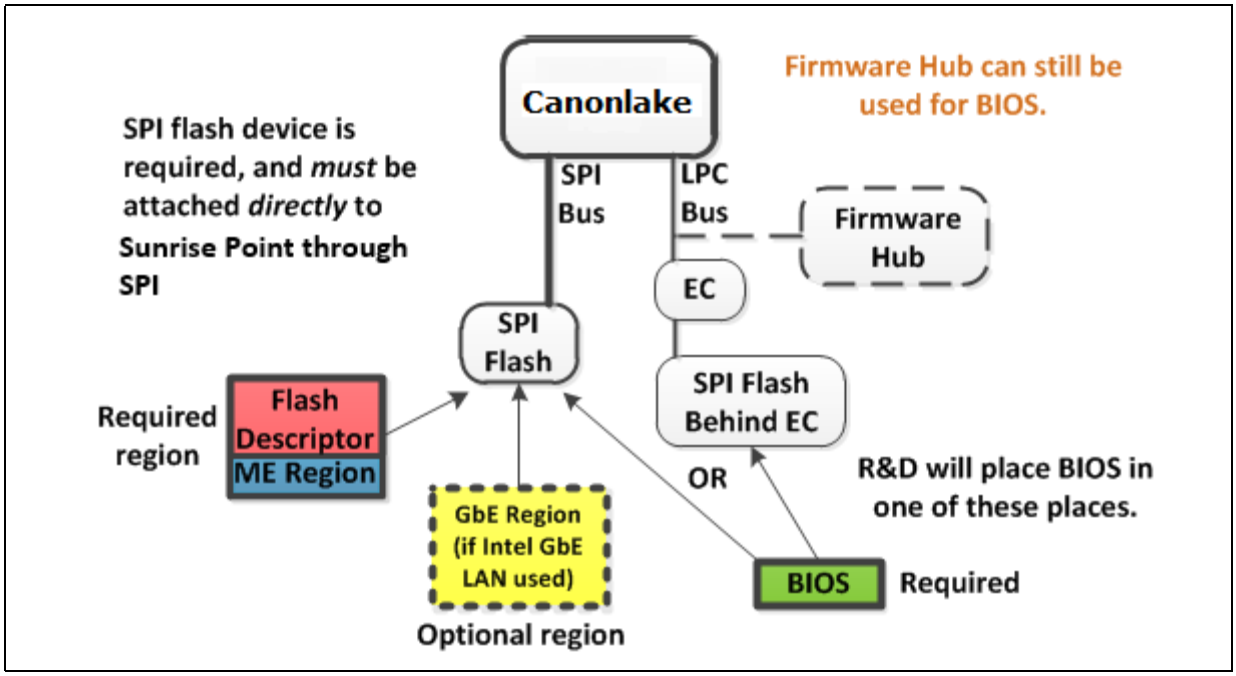


**Figure A-4. Configuration "D" — Mobile Only**




§ §

# 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 Cannon Lake-H SKUs.

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

In below tables,

Min = Clock Div Max (minimum allowed frequency)

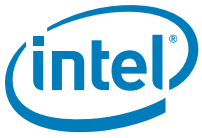
Max = Clock Div Min (maximum allowed frequency)

## B.1 Intel® ICCS SKU Matrix - CNP-H

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

**Table B-1. Intel® ICCS SKU Matrix - CNP-H**

| PCH SKU | Basic | Enhanced |
|---|---|---|
| **Canonpoint H** | | **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% |

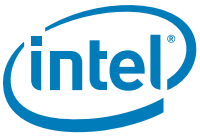


## B.2 How to configure CLKREQ# parameters

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

Configuring CLKREQ# and assigning GPIO depends on how CLKOUT_SRCx configuration via FIT is done (Enabled or Disabled) and if CLKREQ is required or not.

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



# C Appendix — Boot Guard Configuration

## C.1 Boot Guard Profiles

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

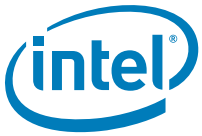
### Table C-1. Profile Description

| Index | Profile Name | F | V | M | ENF | PBE | Description |
|---|---|---|---|---|---|---|---|
| 0 | **Boot Guard Profile - No_FVME** | 0 | 0 | 0 | 00 | 0 | This configuration will invoke Boot Guard during boot with neither Verification nor Measurement. For platforms with all the required Boot Guard components but do not wish to enable Boot Guard boot block verification protection. |
| 1 | **Boot Guard VE** | 0 | 1 | 0 | 01 | 1 | When Verification is desired but if verification fails the platform will continue to boot with the unverified IBB for a short period, to allow remediation. |
| 2 | **Boot Guard VME** | 0 | 1 | 1 | 01 | 1 | When Verification and Measured are desired and the asset protection is provided by both TPM protection and a timed remediation period. |
| 3 | **Boot Guard VM** | 0 | 1 | 1 | 00 | 1 | When Verification and Measured are desired and the asset protection is provided by TPM protection. |
| 4 | **Boot Guard FVE** | 1 | 1 | 0 | 11 | 1 | Strict Verification enforcement. |
| 5 | **Boot Guard FVME** | 1 | 1 | 1 | 11 | 1 | Strict Verification and Measured enforcement. Prevents unverified IBB from running. |

## C.2 Enforcement Policies

### Table C-2. Enforcement Policy Description

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



## C.3 OEM Profile Parameters

### Table C-3. Profile Parameters Description

| Parameter | Description | Settings |
|---|---|---|
| **Force Boot Guard ACM Enabled (F)** | Force Boot Guard Boot determines if the platform starts the Force Boot Guard Boot timer. If it successfully starts it indicates success. When the Force Boot Guard timer stops, it starts the Protect Bios Environment timer, if indicated by the boot policy restrictions. Anchor ACM then jumps to the Initial Boot Block(IBB) with the Force Boot Guard Boot time stopped and the Protect BIOS enable timer running. | **false** - Allow the CPU to jump to the legacy reset vector if the Boot Guard Module cannot be successfully loaded. (default)<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

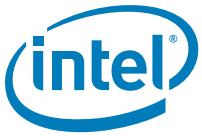
## D.1 Intel® Platform Trust Technology

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

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

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

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



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

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

