Comet Lake-LP Intel® Converged Security and Management Engine Firmware 14.0

Consumer Firmware Bring Up Guide

November 2019

Revision 1.1

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 Comet Lake Platform and Comet 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 © 2014-2019, Intel Corporation. All rights reserved.

Contents

1 Introduction 6
- 1.1 Related Documentation 6
- 1.2 Intel® CSME FW Features 6
- 1.3 Prerequisites 6
- 1.4 Acronyms and Definitions 7
  - 1.4.1 General 7
  - 1.4.2 Intel® Converged Security and Management Engine 8
  - 1.4.3 System States and Power Management 9
- 1.5 Reference Documents 9
- 1.6 Format and Notation 10
- 1.7 Kit Contents 11
- 1.8 External Hardware Requirements for Bring Up 17

2 Image Creation: Intel® Flash Image Tool 18
- 2.1 Start Intel®FIT 18
- 2.2 Step-by-Step Guide to Build SPI Flash Image with Intel® FIT Interface 18

3 Programming SPI Flash Devices and Checking Firmware Status 122
- 3.1 Flash Burner/Programmer 122
  - 3.1.1 In-Circuit SPI Flash Programming for CRB 122
- 3.2 Flash Programming Tool (Intel® FPT) 122
  - 3.2.1 Intel® FPT Windows* Version 123
- 3.3 Checking Intel® ME Firmware Status 124
- 3.4 Common Bring Up Issues and Troubleshooting Table 126

A Appendix — Flash Configurations 127

B Appendix — Intel® ICCS SKU Support Matrix 129

C Appendix — Boot Guard Configuration 131

D Appendix — Intel® Platform Trust Technology 133

E Appendix — Integrated Sensor Hub (ISH) Public Key Settings 134

Figures

Tables

1-1 Number Format Notation 10
1-2 Data Format Notation 10
1-3 Kit Contents 11
2-1 - Initial Screen Layout 19
2-2 - Build Settings 28
2-3 - Flash Layout 30
2-4 - Flash Settings 35
2-5 - Intel® ME Kernel 46
2-6 - Intel® AMT 50
2-7 - Platform Protection 57
2-8 - Integrated Clock Controller 65
2-9 - Networking & Connectivity 71
2-10- Internal PCH Buses 74
2-11- Power 79
2-12- Integrated Sensor Hub 81
2-13- Camera 83
2-14- Debug 85
2-15- CPU Straps 90
2-16- Flex I/O Straps 93
2-17- GPIO 102
2-18- Intel® Precise Touch and Stylus 117
2-19- FW Update Image Build 118
2-20- Intel® FIT - Build Image 121
3-1 Common Bring Up Issues and Troubleshooting Table 126

Revision History

Document Number	Revision Number	Description	Revision Date
	0.8	Pre-Alpha Release	January 2019
	0.81	Corrected missing PCH Configuration options	April 2019
	1.0	Revision updated	September 2019
	1.1	Updated Anti-Rollback default setting to Enabled	November 2019

§ §

1 Introduction

This document covers the Intel® Converged Security and Management Engine Firmware (Intel® CSME) 14.0 - Consumer Firmware bring up procedure. Intel® CSME is tied to essential platform functionality — this dependency cannot be avoided for engineering reasons.

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

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

For more details on SPI Flash layout, see the document **Comet Lake-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® CSME Consumer FW is operating as expected.

1.1 Related Documentation

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

CDI # xxxxxx Intel® Ethernet Connection i219 [Jacksonville]

1.2 Intel® CSME FW Features

This firmware release includes the following applications:

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

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

This document makes only the following limited assumptions regarding hardware:

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

1.4 Acronyms and Definitions

1.4.1 General

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

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

1.4.3 System States and Power Management

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

1.5 Reference Documents

Document	Doc Number/ Location*
Comet Lake Intel® Converged Security and Management Engine (Intel® ME) and Embedded Controller Interaction Product Specification Revision 0.5	TBD / CDI
Intel® Converged Security and Management Engine BIOS Writers Guide	TBD / *
Intel® Converged Security and Management Engine (Intel® ME) 14 SKU Firmware Consumer *Compliance Guide for Comet Lake PCH-H/LP Chipset Family - Comet 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 6)

File or [Directory]	Content Description
[root]	Root directory
[CNP-H]	
CML-H Consumer Bring Up Guide.pdf	Firmware Bring-up Guides for Comet Lake.
CML-LP Consumer Bring Up Guide.pdf	
CML-H Client SPI Programming Guide.pdf	How to program SPI device parameters and descriptor region details. Also contains a complete SPI Flash soft strap reference.
CML-LP Client SPI Programming Guide.pdf	
[Image Components]	
3rd Party Licenses in Security FW	Third party software licenses being used in firmware.
Apache Harmony Apache Version 2.0, January 2004 w header.txt	
Apache-Xerces-Java-XML-Parser.txt	
ConvertUTF unicode license.txt	
CxImage license complete.txt	
HTTP Client C MIT license.txt	
llvm.org University of Illinois_NCSA.txt	
Microsoft TPM 2.0 BSD Two Clause License.txt	
Minix 3.pdf	
MIT Kerberos for Windows.pdf	
newlib_licenses.txt	
Synopsys UFS Host Controller OS.pdf	
wpa supplicant license.txt	
zlib license.txt	
[CSME]	
[H]	
ME_FW_Corporate_CMP-H_PCH.bin	Intel® CSME firmware image (**Non Production FW**) - supports **un-fused** Comet Lake PCH-H PCH stepping: • Un-fused (Super SKU) **Note: For PAVP Testing**, you must match Production FW with Production Part and Non Production FW with Non Production Parts.
[LP]	
ME_FW_Corporate_CMP-LP_PCH.bin	Intel® CSME firmware image (**Non Production FW**) - supports **un-fused** Comet Lake PCH-LP Platform I/O MCP stepping: • Un-fused (Super SKU) **Note: For PAVP Testing**, you must match Production FW with Production Part and Non Production FW with Non Production Parts.
[CSME]	
ME_FW_Consumer_CNP-LP_B0_PCH.bin	Intel® ME firmware image (**Non Production**

Table 1-3. Kit Contents (Sheet 2 of 6)

File or [Directory]	Content Description
pchc_14.x.x.xxxx	PCH Configuration Sub-Partition Binary
CMPH_xx_PMC_FW_PATCH_Vxx.bin	
[Prestitched]	
Base_Prestitched.bin	Pre-Stitched Intel® CSME firmware image binaries
Full_Prestitched.bin	
[Installers]	
Intel®_ME SW Installation Guide.pdf	Intel® CSME Software installation Guide.
[3rd Party Licenses in Security SW]	Third party software licenses being used in software.
ACE-TAO-CIAO.pdf	
Apache-Xerces-C++-XML-Parser.txt	
libxml2.txt	
Microsoft Windows Classic Samples.txt	
Microsoft winfile MIT.txt	
openwsman.pdf	
Windows driver samples.txt	
WixLicenseNote.txt	
[ME_SW_MSI]	
IntelMEFWVer.dll	
MUP.xml	XML file
SetupME.exe	
[MEI-Only Installer MSI]	
IntelMEFWVer.dll	
MEISetup.exe	
MUP.xml	
WixLicenseNote.txt	
[[illegible]ackages]	XML file
[ICLS]	
conf	
Document	
x64	
x86	
[vs2015]	
x64	
x86	
iclsClient.cat	
iclsClient.inf	
[JHI]	
[win10]	
[MEI]	

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

File or [Directory]	Content Description
win10	
[x64]	
TeeDriverW8x64.sys	
[x86]	
TeeDriverW8.sys	
heci.cat	
heci.inf	
[OemExtension]	
OemExtension.cat	
OemExtension.inf	
[SOL]	
mesrl.cat	
mesrl.inf	
[Tools]	
[3rd party Licenses in Security Tools]	Third party software licenses being used in firmware tools.
Android Autogenerated Files Apache 2.0.pdf	
C Make License.pdf	
EFI tool kit intel BSD 2 clause license.txt	
Expat XMLparser MIT license.txt	
Jquery MIT license.txt	
JsonCpp MIT license.txt	
MSDN Example code.pdf	
pugixml license.txt	
[ICC_Tools]	
Intel® ME Firmware ICC Tools User Guide.pdf	ICC Tools User Guide
[CCT]	
[Efi64]	
cct.efi	CCT for EFI
[Windows32]	
CCT.exe	CCT for Windows
[ICC SDK]	
[Windows32]	
[Windows64]	
[WDT Driver]	
[ICCWDT_11.7.0.1000_RS4_Cert]	
[Win7]	
[Win10]	
[System Tools]	
[Documentation]	
Signing and Manifesting Guide.pdf	

Table 1-3. Kit Contents (Sheet 4 of 6)

File or [Directory]	Content Description
SLA_TOOLS.PDF	
System Tools User Guide.pdf	
VSCCommn_bin Content.pdf	
[FIT]	Intel® Flash Image Tool
[WINDOWS32]	
fit.exe	
vsccommn.bin	Binary containing the supported SPI parts
[FPT]	Flash Programming Tool
[Efi64]	
fparts.txt	List of supported SPI Flash devices with specific Flash parameters
fpt.efi	Intel® FPT for EFI
[Windows32]	
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]	Firmware Update Tool
[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)
[FWUpdate_RS]	Firmware Update Tool uEFI reduced size source code.
[Efi64]	

Table 1-3. Kit Contents (Sheet 5 of 6)

File or [Directory]	Content Description
errorlist.c	Reduced size Firmware Update source code samples
errorlist.h	
fwudef.h	
FwUpdateEfiLib.lib	
FWUpdateLib.h	
FWUpdateLibDeprecated.h	
FWUpdLclApp.c	
FWUpdLclAppDeprecated.c	
FwUpdLcl.efi	FW Update Tool (EFI Version reduced size)
[Manifest Extension Utility]	
[MEInfo]	
[Efi64]	
MEInfo.efi	Intel® ME Information Tool (EFI version)
[Windows32]	
MEInfoWin.exe	Intel® ME Information Tool (Windows* version 32bit)
Idrvdll.dll	
Pmxdll.dll	
ISHLib.dll	
[Windows64]	
MEInfoWin64.exe	Intel® ME Information Tool (Windows* version 64bit)
Idrvdll32e.dll	
ISHLib.dll	
Pmxdll32e.dll	
[MEManuf]	
[Efi64]	
MEManuf.efi	Intel® ME Manufacturing Tool (EFI version)
[Windows32]	
Idrvdll.dll	
MEManufWin.exe	Intel® ME Manufacturing Tool (Windows* version 32bit)
Pmxdll.dll	
[Windows64]	
Idrvdll32.dll	
MEManufWin64.exe	Intel® ME Manufacturing Tool (Windows* version 64bit)
Pmxdll32.dll	

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

File or [Directory]	Content Description
[MEU]	
[Windows32]	
meu.exe	Intel® Manifest Extension Utility (MEU) executable file that allows input of FW binary and outputs and independent updatable partition that is compressed and signed.

1.8 External Hardware Requirements for Bring Up

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

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

§ §

2 Image Creation: Intel® Flash Image Tool

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

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

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

2.1 Start Intel®FIT

1. Invoke 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, if the value is the same one value will be listed. If there is a different default value when the program loads with either platform, both values will be listed to show the difference.

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

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

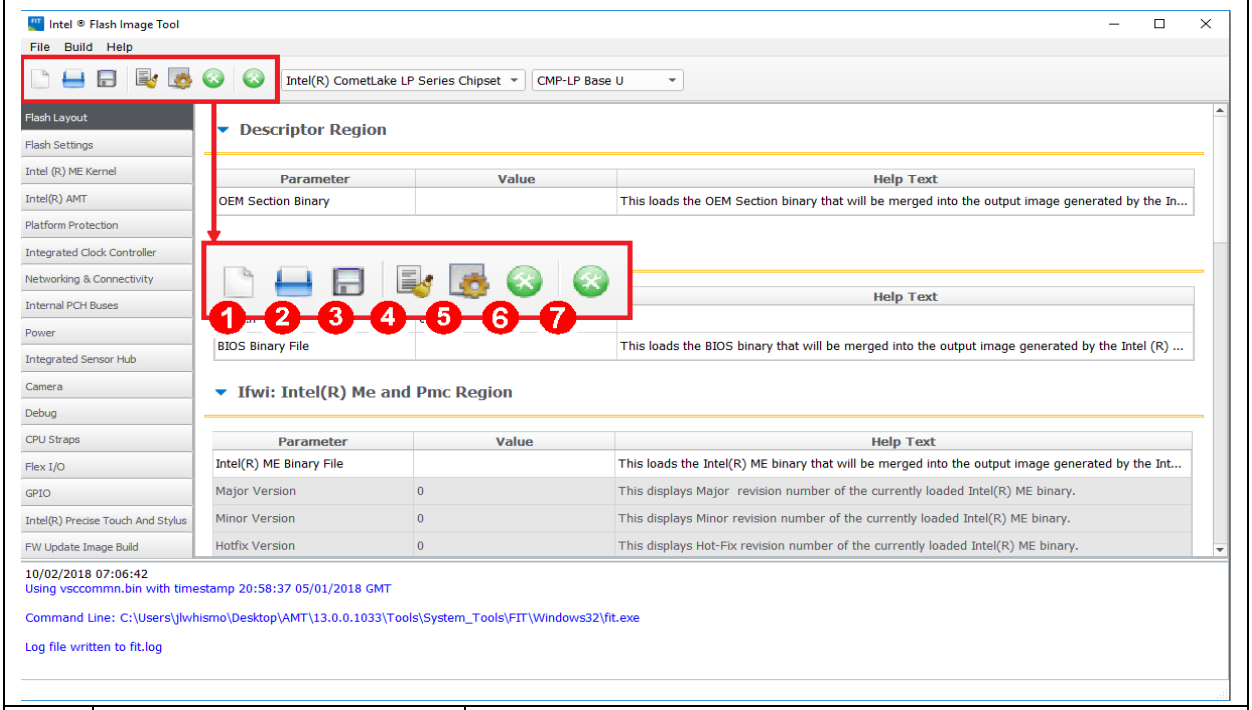
#	Label	Contents
		
1	**New**	This button labeled 'New' on rollover allows opening of a new session with default values
2	**Open**	This button labeled 'Open' on rollover allows opening of an xml or bin file
3	**Save**	This button labeled 'Save' on rollover allows saving of xml file
4	**Clear Console**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

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

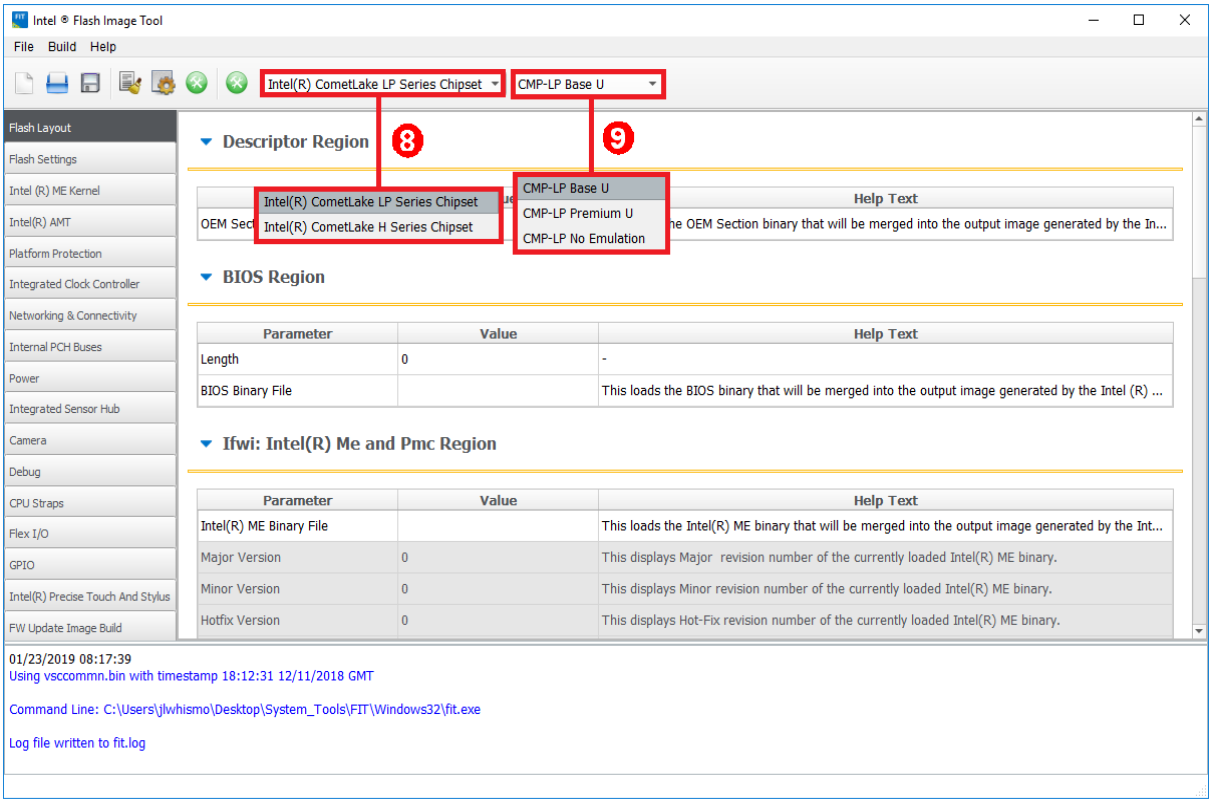
#	Label	Contents
		
8	**Drop Down Selector**	This drop down allows selection of platform
9	**Drop Down Selector**	This drop down allows selection of SKU within platform selected

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

#	Label	Contents

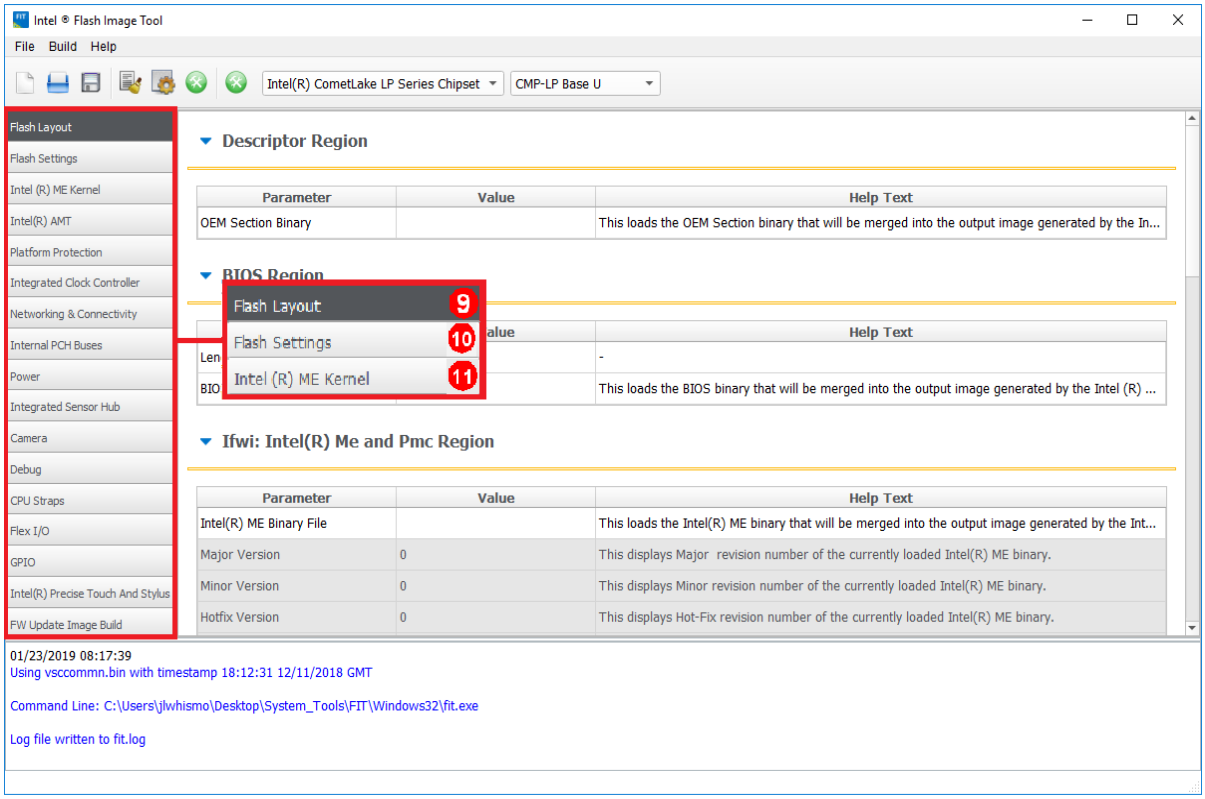


Table 2-1. - Initial Screen Layout (Sheet 4 of 9)

#	Label	Contents
9	**Flash Layout Tab**	Flash Layout which contains (see Table 2-3): • Descriptor Region • BIOS Region • IFWI: Intel® ME and PMC Region • EC Region • GBE Region • SubPartitions • PDR Region
10	**Flash Settings Tab**	Flash Settings which contains (see Table 2-4): • Flash Components • Host CPU/ BIOS Master Access • Intel® ME Master Access • GBE Master Access • EC Master Access • Flash Configuration • VSCC Table - VSCC Entry • BIOS Configuration • OEM and Platform IDs • FPF Configuration
11	**Intel® ME Kernel Tab**	Intel® ME Kernel which contains (see Table 2-5): • Processor • Intel® ME Firmware Update • Intel® Services Configuration • Image Identification • Firmware Diagnostics • Post Manufacturing Lock • MCTP Configuration • Intel® ME Boot Configuration • Reserved

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

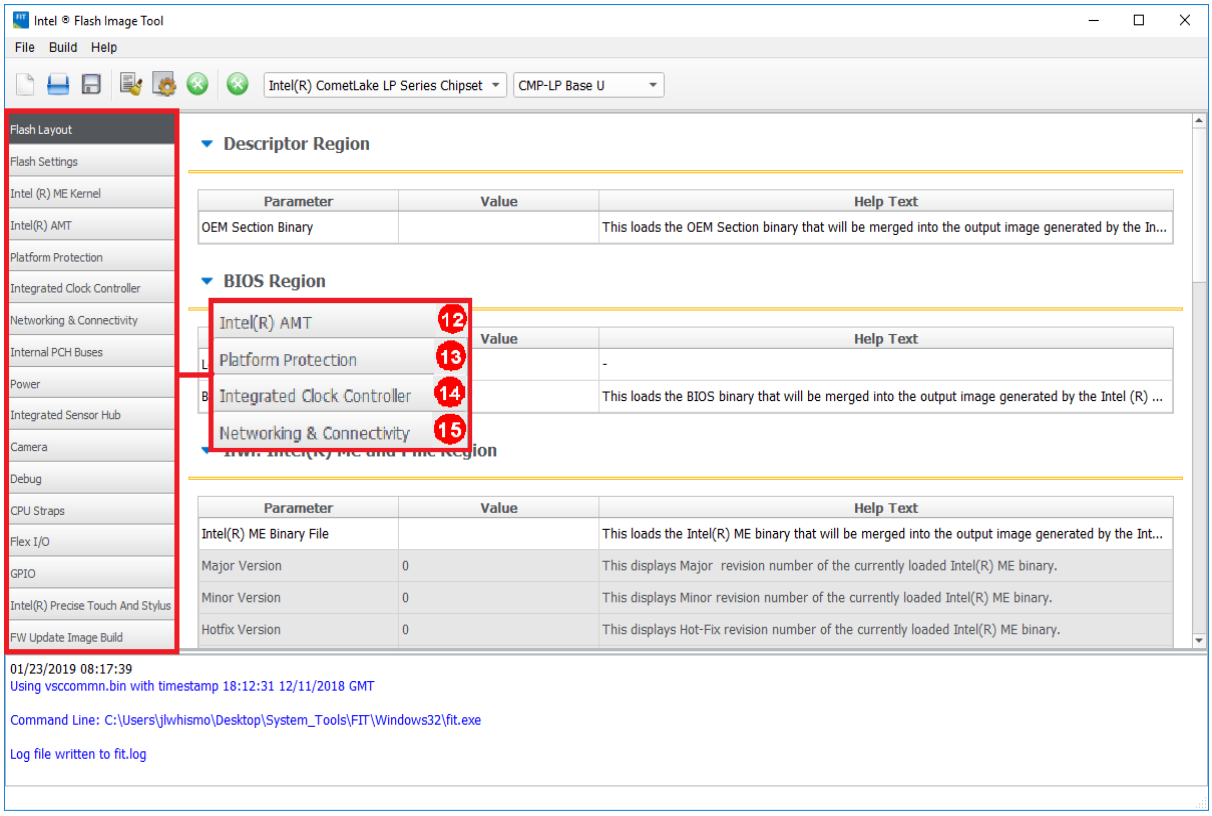
#	Label	Contents
		
12	**Intel® AMT Tab**	Intel® AMT which contains (see Table 2-6): • Intel® AMT Configuration • KVM Configuration • Provisioning Configuration • OEM Customizable Certificates (1, 2, 3) • OEM Default Certificates (1, 2, 3, 4, 5) • Redirection Configuration • TLS Configuration
13	**Platform Protection Tab**	Platform Protection which contains (see Table 2-7): • Content Protection • Graphics uController • Hash Key Configuration for Bootguard / ISH • Exclusion Ranges • Descriptor Configuration • Boot Guard Configuration • Intel® PTT Configuration • TPM Over SPI Bus Configuration • BIOS Guard Configuration • TXT Configuration • Crypto Hardware Support • Platform Trusted Device Support • Intel FPF Anti-Rollback Configuration

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

#	Label	Contents
14	**Integrated Clock Controller Tab**	Integrated Clock Controller which contains (see Table 2-8): • Integrated Clock Controller Policies • Profiles
15	**Networking & Connectivity Tab**	Networking & Connectivity which contains (see Table 2-9): • Platform vPro NIC • Docking Station • Wired LAN Configuration • Wireless LAN Configuration

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

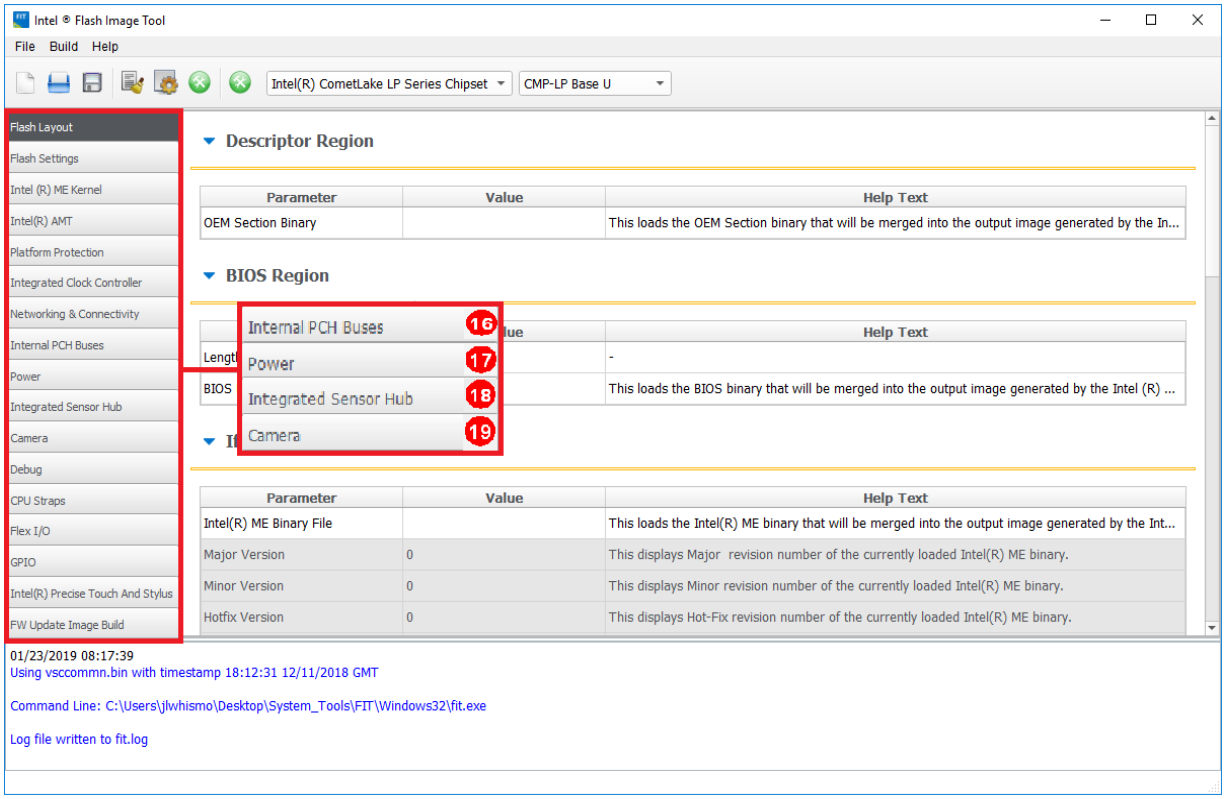
#	Label	Contents
		
16	**Internal PCH Buses Tab**	Internal PCH Buses which contains (see Table 2-10): • PCH Timer Configuration • SMBus / SMLink Configuration • DMI Configuration • OPI Configuration • eSPI Configuration
17	**Power Tab**	Power which contains (see Table 2-11): • Platform Power • Deep Sx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

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

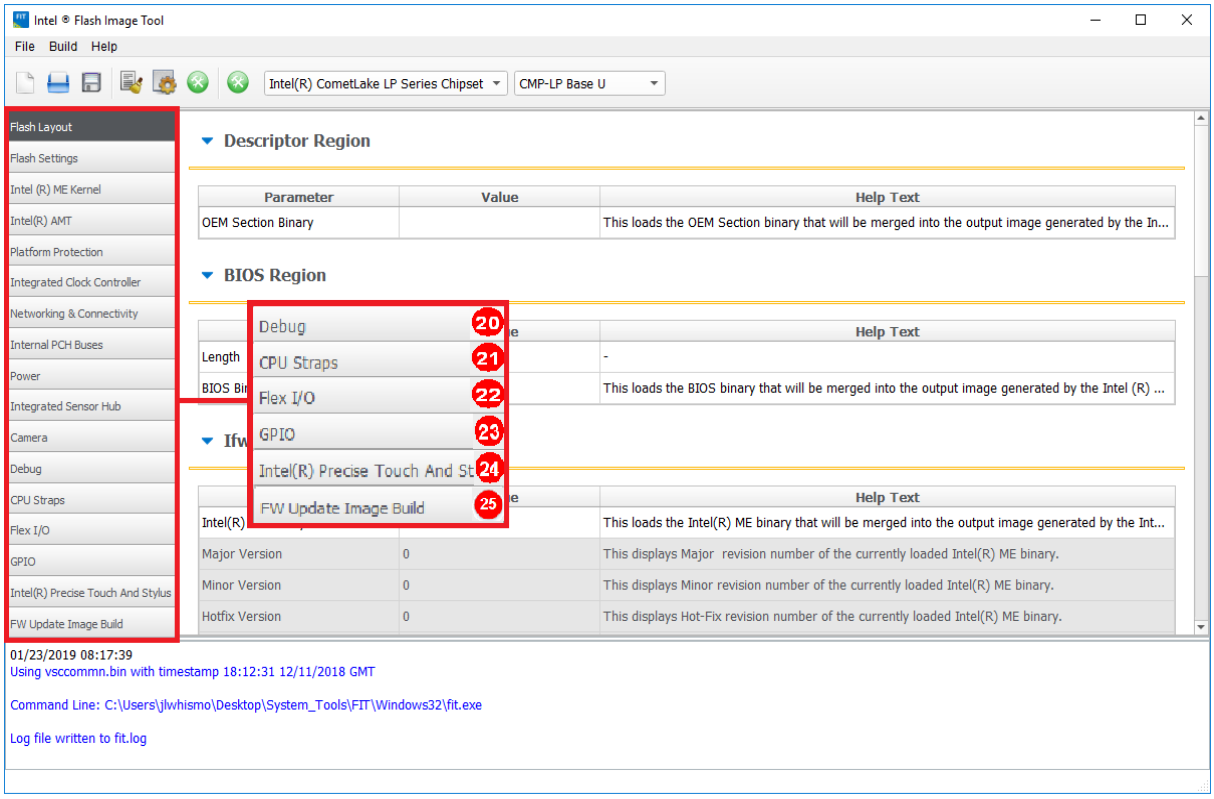
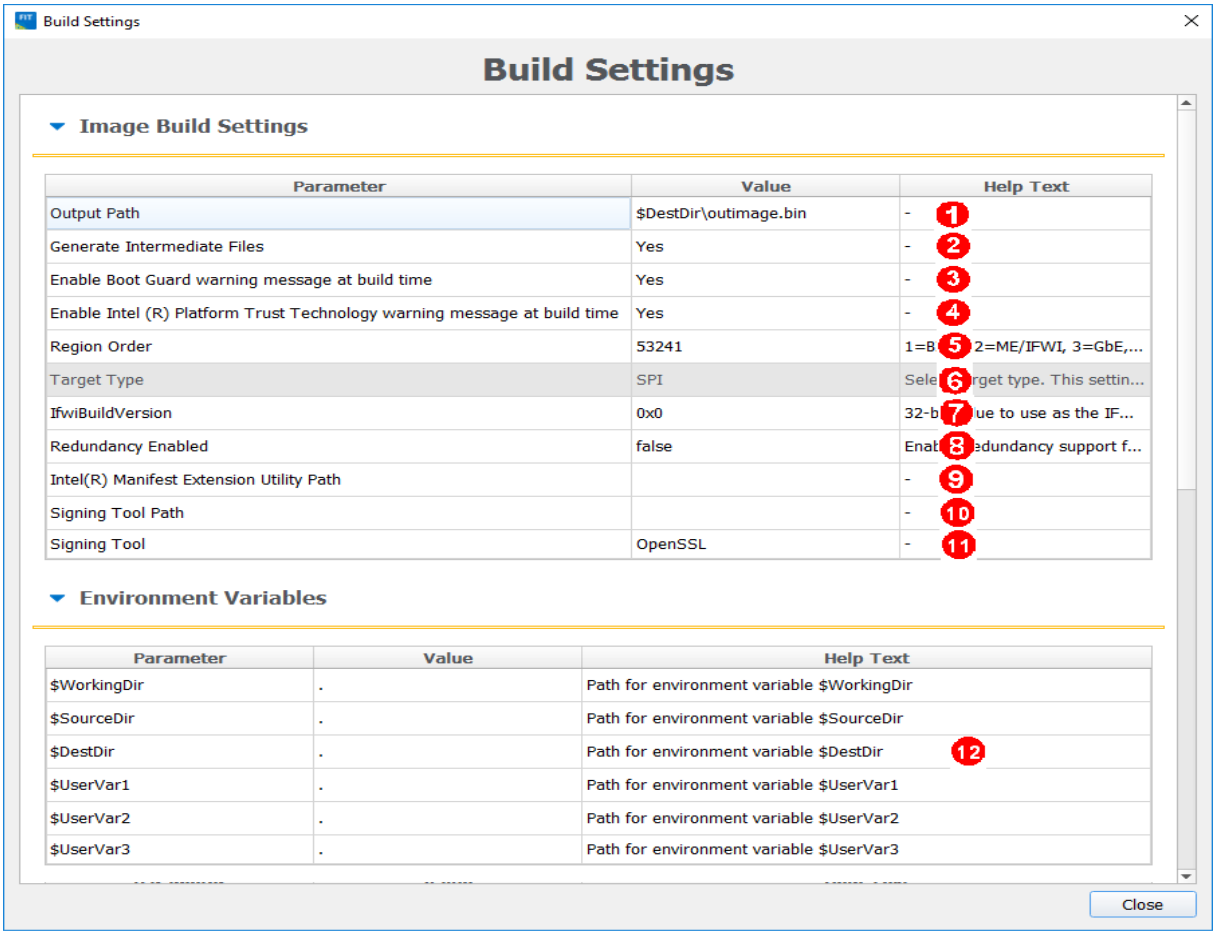
#	Label	Contents
		
20	**Debug Tab**	Debug which contains (see Table 2-14): • IDLM • Delayed Authentication Mode Configuration • Intel® Trace Hub Technology • Intel® ME Firmware Debugging Overrides • Direct Connection Interface Configuration • eSPI Feature Overrides • Early USB DBC over Type-A Configuration
21	**CPU Straps Tab**	CPU Straps which contain a detailed list of parameters (see Table 2-15) • CPU Straps
22	**Flex I/O Tab**	Flex I/O which contains (see Table 2-16): • Intel® RST for PCIe Configuration • PCIe Lane Reversal Configuration • PCIe Port Configuration • SATA / PCIe Combo Port Configuration • SATA / PCIe Combo Port Select Polarity • USB3 Port Configuration • USB2 Port Configuration

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

#	Label	Contents
23	**GPIO Tab**	GPIO which contains (see Table 2-17): • LAN / GPIO Select • WLAN / GPIO Select • Platform Power / GPIO • ME Feature Pins • Touch Controller Pins • SMLink1 Pins • GPIO VCCIO Voltage Control
24	**Intel® Precise Touch and Stylus**	Intel® Precise Touch and Stylus which contains (see Table 2-18): • Integrated Touch Configuration • Intel® Integrated Touch and Stylus Configuration
25	**FW Update Image Build**	FW Update Image Build which contains (see Table 2-19): • ME Image • PMC Image • OEM KM Image • ISH Image • INUIT Image • PCHC Image
	Console Window Area	Displays opening messages, log file entries, and build activity messages

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

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



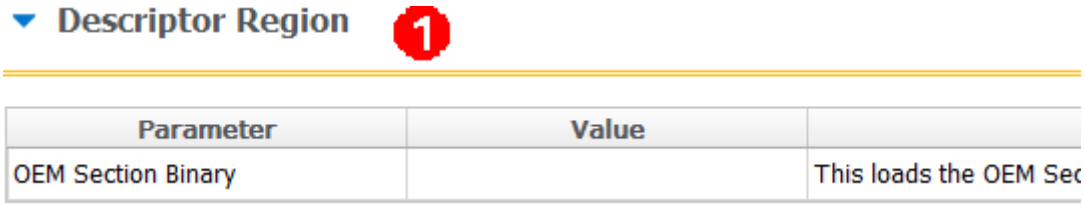
#	Parameter	CRB	Values
1	**Output Path**		Double click to the right of outimage.bin and click to get browse button to specify path and name of file to create for the build - default is outimage.bin in the same folder as Intel® FIT tool
2	**Generate Intermediate Files**	Yes	Yes/No - Yes is default
3	**Enable 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
5	**Region Order**	Yes	53241 - 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:			
6	**Target Type**	Yes	Target boot media type. This setting is configured from the Intel® FIT toolbar drop downs.
7	**IFWI Build Version**	Yes	32-bit value to use as the IFWI build version number.
8	**Redundancy Enabled**	Yes	This setting enabled Redundancy support for critical layout components.
9	**Intel® Manifest Extension Utility Path**	Yes	
10	**Signing Tool Path**	Yes	
11	**Signing Tool**	Yes	
12			$WorkingDir and $DestDir can be left at the default '.' Click on $SourceDir Value field and type in path where the Image Components are located for the Manageability Engine kit

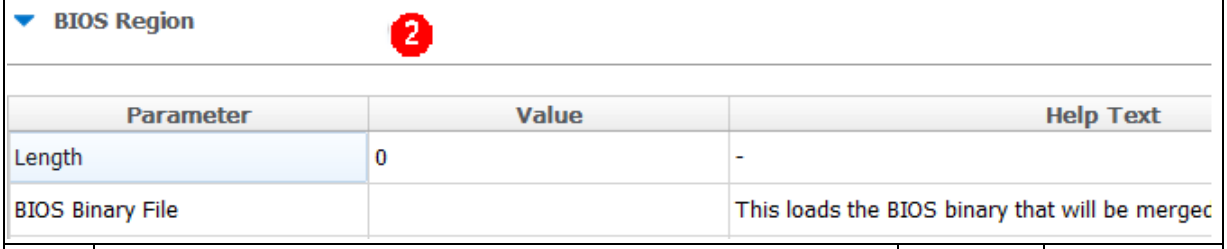
Table 2-3. - Flash Layout (Sheet 1 of 5)

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



#	Parameter	Platform	Settings
1	**Descriptor Region**		
	OEM Section Binary This loads the OEM Section binary that will be merged into the output image generated by the Intel® FIT tool.	CML-Y CML-U	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 **Note:** This value will be automatically populated by Intel® FIT during image build.		
	BIOS Binary File Navigate to path to load bios.rom file. This loads the BIOS binary that will be merged into the output image generated by the Intel® FIT tool.	CML-Y CML-U	biosimage.bin biosimage.bin

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

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

Ifwi: Intel(R) Me and Pmc Region

3

Parameter	Value	Help Text
Intel(R) ME Binary File		This loads the Intel(R) ME binary that will be merged int
Major Version	0	This displays Major revision number of the currently loa
Minor Version	0	This displays Minor revision number of the currently loa
Hotfix Version	0	This displays Hot-Fix revision number of the currently lo
Build Version	0	This displays Build version number of the currently loade
Chipset Initialization Version		This displays the current Chipset Initialization version co
Chipset Initialization Binary		This loads the Chipset Initialization binary that will be m
ChipsetInit Override Version		This displays the version of the Chipset Initializtion Binar
PMC Binary File		This loads the PMC binary that will be merged into the o
PMC Length	0x14000	-
Version		-

3	**IFWI: Intel® ME and PMC Region**		
	Intel® ME Binary File Navigate to your **Source Directory** (as specified in Table 2-2) and switch to the Intel® CSME subdirectory. Choose the appropriate Intel® CSME Firmware binary image. This loads the Intel® CSME binary that will be merged into the into the output image generated by the Intel® FIT tool. **Note:** You may choose to build the Intel® CSME Region only. To do so, the **Number of Flash Components** in **Flash Settings> Flash Components** must be set to 0. **Note:** If loading meimage.bin file, check that the ME region is enabled in tool before building image.	CML-Y CML-U	meimage.bin 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. ***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.	CML-Y CML-U	Chipset.bin (Optional) Chipset.bin (Optional)
	ChipsetInit Override Version - This displays the version of the Chipset Initialization Binary override if specified.		
	PMC Binary File - This loads the PMC binary that will be merged into the output image generated by the Intel® FIT tool.	CML-Y CML-U	PMC.bin 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 **Note:** This value will be automatically populated by Intel® FIT during image build.		
	EC Binary File Navigate to path to load EC bin file. This loads the Embedded Controller binary used for eSPI that will be merged into the output image generated by the Intel® FIT tool.	CML-Y CML-U	EC Binary EC Binary
	EC Region Enable **Values: Enabled / Disabled** This option allows the user to enable or disable the Embedded Controller data region.	CML-Y CML-U	Enabled Enabled
	EC Region Pointer File This loads a binary file containing the 16 byte Embedded Controller pointer value at the start of the flash descriptor	CML-Y CML-U	Pointer Binary 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 **Note:** This value will be automatically populated by Intel® FIT during image build.		
	GbE Binary File Navigate to your **Source Directory** (as specified in Table 2-2) and switch to the GbE subdirectory. Choose the appropriate Intel **GbE** LAN Firmware binary image. **If not using Intel LAN then load the GbE image before disabling the region along with changing additional settings below.** This loads the Intel® integrated LAN binary that will be merged into the output image generated by the Intel® FIT tool. **Note:** If loading gbeimage.bin file, check that the GbE region is enabled in tool before building image.	CML-Y CML-U	gbeimage.bin gbeimage.bin
	GbE Region Enable **Values: Enabled / Disabled -** This option allows the user to enable or disable the Gigabit Ethernet Region. **NOTE:** If choosing a configuration that **does not include the GbE LAN the following settings need to be adjusted**: **LAN Power Well: Core Well** **Intel® Integrated Wired LAN Enabled: No** **GbE MAC SMBus Address: No** **Intel® PHY over PCIe Enabled: No** **LAN PHY Power Control GDP11 Signal Configuration: Enable as GDP11**	CML-Y CML-U	Enabled Enabled
	Image ID		
	Major Version		
	Minor Version		

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

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

6	**SubPartitions**		
	IUnit Binary File This loads the IUnit Sub Partition binary that will be merged into the output image generated by the Intel® FIT tool.	CML-Y CML-U	Iunit.bin (Optional) Iunit.bin (Optional)
	Length **Note:** This value will be automatically populated by Intel® FIT during image build.		

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

PCH Configuration Sub-Partition 7

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

7	**PCH Configuration Sub-Partition** This loads the PCH Configuration binary that will be merged in the output image generated by the Intel® FIT tool.		
	PCH Configuration File Navigate to path to load PCHC.bin file. This loads the PCH Configuration binary.	ICL-Y ICL-U	PCHC.bin PCHC.bin
	Length - This displays the length of the PCH Configuration Sub-Partition. ***Note:*** This value will be automatically populated by Intel® FIT during image build.		

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

PDR Region 8

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

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

Table 2-4. - Flash Settings (Sheet 1 of 11)

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

Flash Components 1

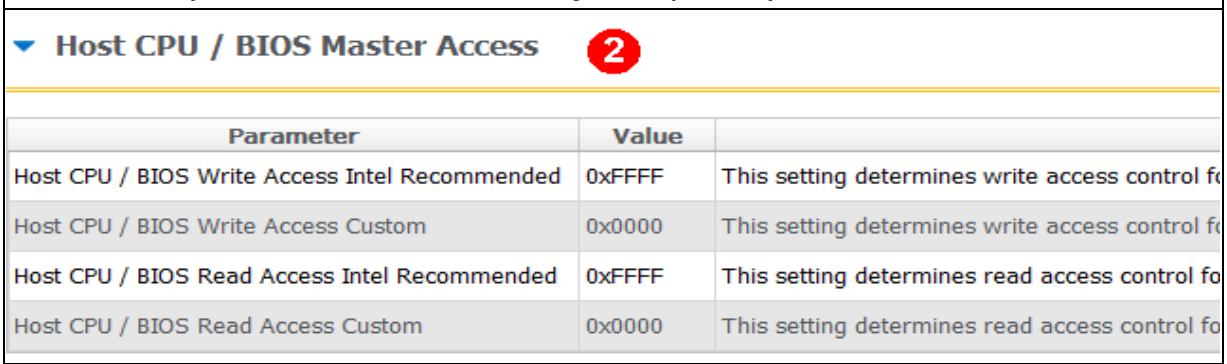
Parameter	Value	Help Tex
Number of Flash Components	1	Specifies the number of Flash components
Flash component 1 Size	16MB	This field identifies the size of the 1st Flas
Flash component 2 Size	8MB	This field identifies the size of the 2nd Flas
SPI Voltage Select	3.3Volts	This strap sets the internal control signal c
SPI Global Protected Range	0x0	Sets the default value of the Global Protec
SPI Idle to Deep Power Down Timeout	0x5	SPI Idle to Deep Power Down Timeout Def
SPI Out of Order operation Enabled	Yes	When this setting is enabled priority opera
SPI Resume Hold-off Delay	4us	Specifies the time after the completion of
SPI Max write / erase Resume to Suspend intervals	No Ceiling	This setting specifies the maximum value t
SPI Suspend / Resume Enabled	Yes	When this setting is enabled writes and er
SPI Software Binding Enabled	No	When enabled this settings will allow for S

#	Parameter	Platform	Settings
1	**Flash Components**		

Table 2-4. - Flash Settings (Sheet 2 of 11)

	Number of Components **Values: 0, 1, 2 -** This setting configures the total number of flash components for the platform. **Note:** Choosing a selection of '0' part will cause the Intel® FIT tool to build an output image containing only the Intel® ME region.	CML-Y CML-U	1 1
	Flash component 1 Size **Values: 512KB, 1MB, 2MB, 4MB, 8MB, 16MB, 32MB, 64MB** - This setting determines the size of Flash component 1 for the platform image.	CML-Y CML-U	16MB 16MB
	Flash component 2 Size **Values: 512KB, 1MB, 2MB, 4MB, 8MB, 16MB, 32MB, 64MB** - This setting determines the size of Flash component 2 for the platform image. **Note:** This setting is only applicable when the Number of Flash Components option is set to '2'.	CML-Y CML-U	Greyed Out Greyed Out
	SPI Voltage Select **Values: 1.8 Volts, 3.3 Volts** - This strap sets the internal control signal on the pad for either 1.8 or 3.3 volts. See Comet Lake LP SPI Programming Guide for further details.	CML-Y CML-U	3.3 Volts 3.3 Volts
	SPI Global Protected Range - This sets the default value of the Global Protected Range register in the SPI Flash Controller.	CML-Y CML-U	0x0 0x0
	SPI Idle to Deep Power Down Timeout - This sets SPI Idle to Deep Power Down Timeout Default Specifies the time in microseconds that the Flash Controller waits after all activity is idle before commanding the flash devices to Deep Power down, time = 2^N microseconds.	CML-Y CML-U	0x5 0x5
	SPI Out of Order operation Enabled - When this setting is enabled priority operations may be issued while waiting for write / erase operations to complete on the flash device. When this setting is disabled all write / erase type operations in order.	CML-Y CML-U	Yes Yes
	SPI Resume Hold-off Delay - This specifies the time after the completion of a pri_op before the flash controller sends the resume instruction. If a new pri_op is eligible to be issued prior to the end of this delay time then the pri_op is issued and the timer is reinitialized to tRHD. 3-bit field encodes count with range 0-7. tRHD = count * 2us.	CML-Y CML-U	4us 4us
	SPI Max write / erase Resume to Suspend intervals - This setting specifies the maximum value for the write and erase Resume to Suspend intervals.	CML-Y CML-U	No Ceiling No Ceiling
	SPI Suspend / Resume Enabled - When this setting is enabled writes and erases may be suspended to allow a read to be issued on the flash device. When this setting is disabled no transaction will be allowed to the busy flash device.	CML-Y CML-U	Yes Yes
	SPI Software Binding Enabled - When enabled this settings will allow for SPI re-binding to a new PCH during re-manufacturing flows.	CML-Y CML-U	No No

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

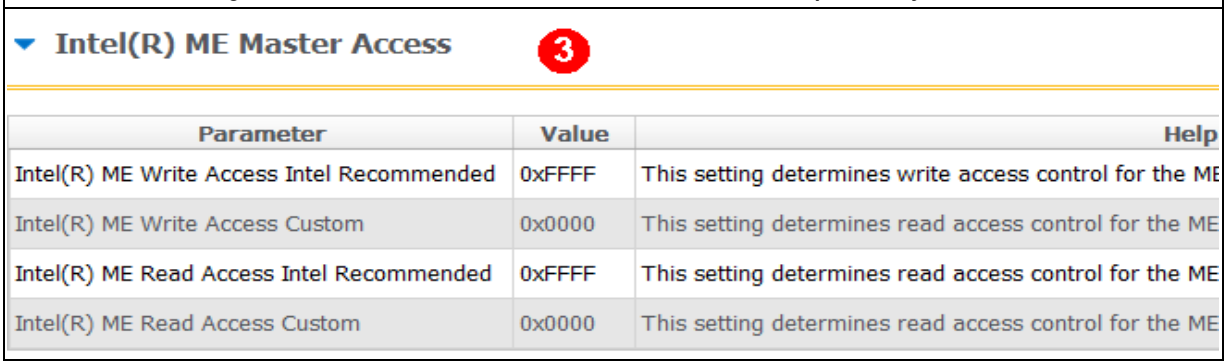


#	Parameter	Platform	Settings
2	**Host CPU / BIOS Master Access**		

Table 2-4. - Flash Settings (Sheet 3 of 11)

	Host CPU / BIOS Write Access Intel Recommended **Values: 0xFFFF, 0x000A, 0x001A, 0x010A, 0x011A** - This setting determines write access control for the BIOS region. **0xFFFF** = Debug/Manufacturing **0x000A** = Production **0x001A** = Production with access to PDR (should ONLY be used if PDR region is implemented). **0x010A** = Production with access to EC **0x011A** = Production with access to EC and PDR **Custom** = User custom Host / BIOS Write Access values For further details on Region Access Control see Comet Lake LP SPI Programming guide further details.	CML-Y CML-U	0xFFFF 0xFFFF
	Host CPU / BIOS Write Access Custom - This setting allows free form user customized Host CPU / BIOS Write Access regions permissions ***Note:*** This setting is grayed out unless Custom is selected under the Host CPU / BIOS Write Access Intel Recommended drop down menu. ***Warning:*** **Setting region access permission values outside of Intel recommendation could result in compromised platform security**	CML-Y CML-U	Hex Input
	Host CPU / BIOS Read Access **Values: 0xFFFF, 0x000F, 0x001F, 0x010F, 0x011F** - This setting determines read access control for the BIOS region. **0xFFFF** = Debug/Manufacturing **0x000F =** Production **0x001F =** Production with access to PDR (should ONLY be used if PDR region is implemented). **0x010F** = Production with access to EC **0x011F** = Production with access to EC and PDR **Custom** = User custom Host / BIOS Read Access values For further details on Region Access Control see Comet Lake LP SPI Programming guide.	CML-Y CML-U	0xFFFF 0xFFFF
	Host CPU / BIOS Read Access Custom - This setting allows free form user customized Host CPU / BIOS Read Access regions permissions ***Note:*** This setting is grayed out unless Custom is selected under the Host CPU / BIOS Read Access Intel Recommended drop down menu. ***Warning:*** **Setting region access permission values outside of Intel recommendation could result in compromised platform security**	CML-Y CML-U	Hex Input

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



Intel(R) ME Master Access 3

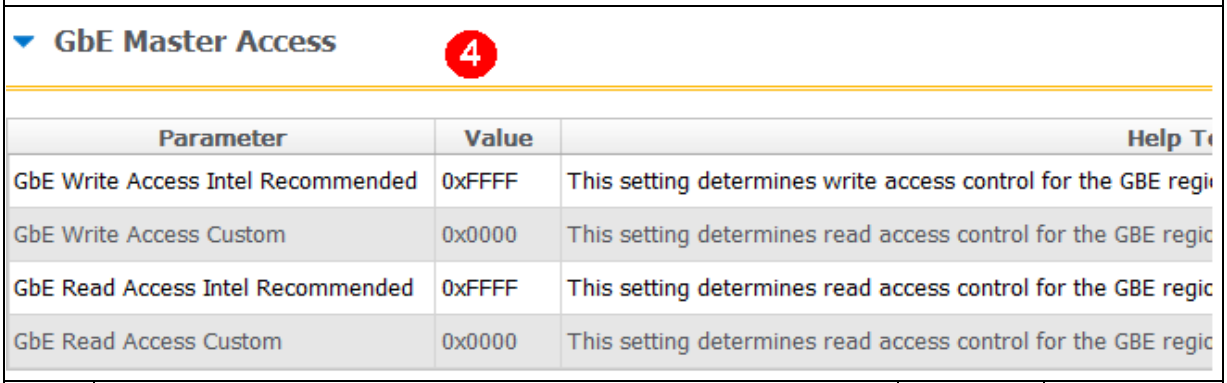
Parameter	Value	Help
Intel(R) ME Write Access Intel Recommended	0xFFFF	This setting determines write access control for the ME
Intel(R) ME Write Access Custom	0x0000	This setting determines read access control for the ME
Intel(R) ME Read Access Intel Recommended	0xFFFF	This setting determines read access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

#	Parameter	Platform	Settings

Table 2-4. - Flash Settings (Sheet 4 of 11)

3	**Intel® ME Master Access**		
	Intel® ME Write Access Intel Recommended **Values: 0xFFFF, 0x0004** - This setting determines write access control for the Intel® CSME region. **0xFFFF** = Debug/Manufacturing **0x0004** = Production **0x000C** = Production **Custom** = User custom Intel® ME Write Access values For further details on Region Access Control see Comet Lake LP SPI Programming guide further details.	CML-Y CML-U	0xFFFF 0xFFFF
	Intel® ME Write Access Custom - This setting allows free form user customized Intel® ME Write Access regions permissions ***Note:*** This setting is grayed out unless Custom is selected under the Intel® ME Write Access Intel Recommended drop down menu. ***Warning:*** **Setting region access permission values outside of Intel recommendation could result in compromised platform security**	CML-Y CML-U	Hex Input
	Intel® ME Read Access Intel Recommended **Values: 0xFFFF, 0x000D** - This setting determines read access control for the Intel® CSME region. **0xFFFF** = Debug/Manufacturing **0x000D** = Production **Custom** = User custom Intel® ME Read Access values For further details on Region Access Control see Comet Lake LP SPI Programming guide further details.	CML-Y CML-U	0xFFFF 0xFFFF
	Intel® ME Read Access Custom - This setting allows free form user customized Intel® ME Read Access regions permissions ***Note:*** This setting is grayed out unless Custom is selected under the Intel® ME Read Access Intel Recommended drop down menu. ***Warning:*** **Setting region access permission values outside of Intel recommendation could result in compromised platform security**	CML-Y CML-U	Hex Input

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



#	Parameter	Platform	Settings

Table 2-4. - Flash Settings (Sheet 5 of 11)

4	**GbE Master Access**		
	GbE Write Access Intel Recommended **Values: 0xFFFF, 0x0008** - This setting determines write access control for the Gigabit Ethernet Region. **0xFFFF** = Debug/Manufacturing **0x0008** = Production **Custom** = User custom GbE Write Access values For further details on Region Access Control see Comet Lake LP SPI Programming guide further details.	CML-Y CML-U	0xFFFF 0xFFFF
	GbE Write Access Custom - This setting allows free form user customized GbE Write Access regions permissions ***Note:*** This setting is grayed out unless Custom is selected under the GbE Write Access Intel Recommended drop down menu. ***Warning:*** **Setting region access permission values outside of Intel recommendation could result in compromised platform security**	CML-Y CML-U	Hex Input
	GbE Read Access Intel Recommended **Values: 0xFFFF, 0x0009** - This setting determines read access control for the Gigabit Ethernet Region. **0xFFFF** = Debug/Manufacturing **0x0009** = Production **Custom** = User custom GbE Read Access values For further details on Region Access Control see Comet Lake LP SPI Programming guide further details.	CML-Y CML-U	0xFFFF 0xFFFF
	GbE Read Access Custom - This setting allows free form user customized GbE Read Access regions permissions ***Note:*** This setting is grayed out unless Custom is selected under the GbE Read Access Intel Recommended drop down menu. ***Warning:*** **Setting region access permission values outside of Intel recommendation could result in compromised platform security**	CML-Y CML-U	Hex Input

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

EC Master Access 5

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

#	Parameter	Platform	Settings

Table 2-4. - Flash Settings (Sheet 6 of 11)

5	**EC Master Access**		
	EC Write Access Intel Recommended **Values: 0xFFFF, 0x0100** - This setting determines write access control for the Embedded Controller Region. **0xFFFF** = Debug/Manufacturing **0x0100** = Production **Custom** = User custom EC Write Access values For further details on Region Access Control see Comet Lake LP SPI Programming guide further details.	CML-Y CML-U	0xFFFF 0xFFFF
	EC Write Access Custom - This setting allows free form user customized EC Write Access regions permissions ***Note:*** This setting is grayed out unless Custom is selected under the EC Write Access Intel Recommended drop down menu. ***Warning:*** **Setting region access permission values outside of Intel recommendation could result in compromised platform security**	CML-Y CML-U	Hex Input
	EC Read Access Intel Recommended **Values: 0xFFFF, 0x0101, 0x0103** - This setting determines read access control for the Embedded Controller Region. **0xFFFF** = Debug/Manufacturing **0x0101 =** Production **0x0103** = Production with EC BIOS Read Access **Custom** = User custom EC Read Access values For further details on Region Access Control see Comet Lake LP SPI Programming guide further details.	CML-Y CML-U	0xFFFF 0xFFFF
	EC Read Access Custom - This setting allows free form user customized EC Read Access regions permissions ***Note:*** This setting is grayed out unless Custom is selected under the EC Read Access Intel Recommended drop down menu. ***Warning:*** **Setting region access permission values outside of Intel recommendation could result in compromised platform security**	CML-Y CML-U	Hex Input
Click on Flash Layout in the left tabs menu> IUnit Sub-Partion is expanded by default:			

Table 2-4. - Flash Settings (Sheet 7 of 11)

Flash Configuration 6

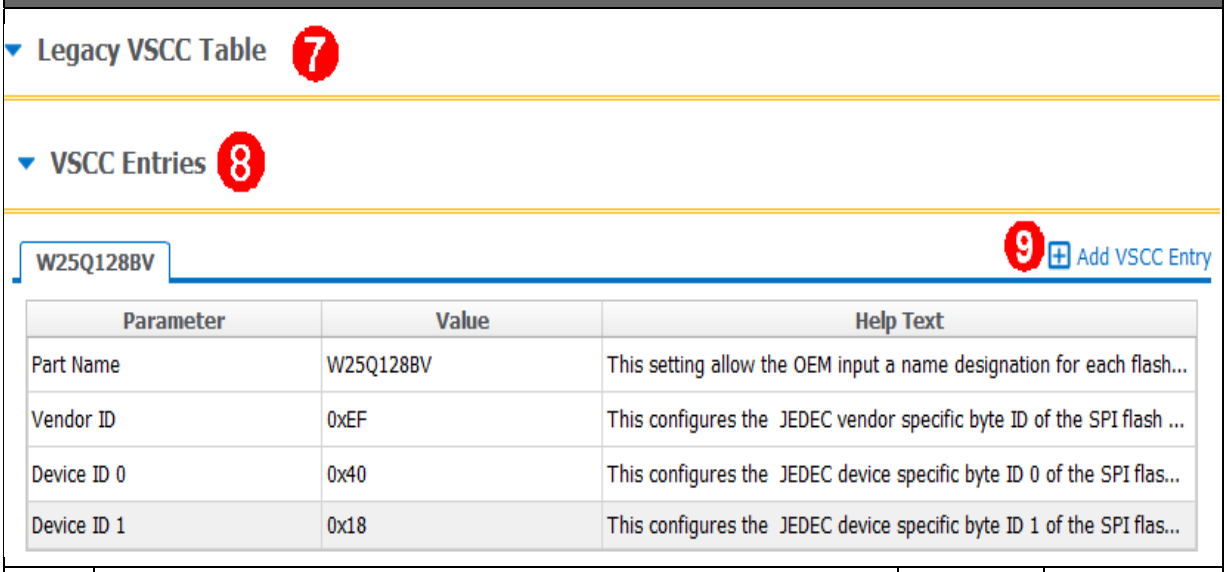
Parameter	Value	Help Text
Dual I/O Read Enable	No	This soft-strap only has effect if Dual I/O Read is discovered as suppo
Dual Output Read Enable	No	This soft-strap only has effect if Dual Output Read is discovered as su
Fast Read Clock Frequency	48MHz	This setting allows customers to configure the flash component clock
Fast Read Supported	Yes	This setting allows customers to enable support for Fast Read capabil
Invalid Instruction 0	0x21	This setting allows customers to configure invalid instruction to protec
Invalid Instruction 1	0x42	This setting allows customers to configure invalid instruction to protec
Invalid Instruction 2	0x60	This setting allows customers to configure invalid instruction to protec
Invalid Instruction 3	0xAD	This setting allows customers to configure invalid instruction to protec
Invalid Instruction 4	0xB7	This setting allows customers to configure invalid instruction to protec
Invalid Instruction 5	0xB9	This setting allows customers to configure invalid instruction to protec
Invalid Instruction 6	0xC4	This setting allows customers to configure invalid instruction to protec
Invalid Instruction 7	0xC7	This setting allows customers to configure invalid instruction to protec
Quad I/O Read Enable	No	This soft-strap only has effect if Quad I/O Read is discovered as supp
Quad Output Read Enable	No	This soft-strap only has effect if Quad Output Read is discovered as s
Read ID and Read Status Clock Frequency	48MHz	This setting allows customers to configure the flash component clock
Write and Erase Clock Frequency	48MHz	This setting allows customers to configure the flash component clock

#	Parameter	Platform	Settings
6	**Flash Configuration**		
	Dual I/O Read Enabled **Values: Yes/No** - This setting allows the customer to enable support for Dual I/O Read capabilities for flash components. See Comet Lake LP SPI Programming guide for further details.	CML-Y CML-U	Yes Yes
	Dual Output Read Enabled **Values: Yes/No** - This setting allows the customer to enable support for Dual Output Read capabilities for flash components. See Comet Lake LP SPI Programming guide for further details.	CML-Y CML-U	Yes Yes
	Fast Read Clock Frequency **Values: 17MHz, 30MHz, 48MHz** - This setting allows the customer to configure the flash component clock frequency setting for Fast Read. See Comet Lake LP SPI Programming guide for further details.	CML-Y CML-U	48MHz 48MHz 48MHz
	Fast Read Supported **Values: Yes/No** - This setting allows the customer to enable support for Fast Read capabilities for flash components. See Comet Lake LP SPI Programming guide for further details. **Note:** If fast read supported is set to **"No"** any changes made to Dual I/O, Quad I/O, Dual Output, or Quad Output will not be affected if set to yes. Fast read supported should also be set to enable frequencies greater than 20MHz.	CML-Y CML-U	Yes Yes

Table 2-4. - Flash Settings (Sheet 8 of 11)

	Invalid Instruction 0 - This setting allows the customer to configure invalid instruction to protect against Chip Erase. See Comet Lake LP SPI Programming guide for further details. **Note:** This setting should be set to '0' if there are not Invalid instructions.	CML-Y CML-U	0x00000021 0x00000021
	Invalid Instruction 1 - This setting allows the customer to configure invalid instruction to protect against Chip Erase. See Comet Lake LP SPI Programming guide for further details. **Note:** This setting should be set to '0' if there are not Invalid instructions.	CML-Y CML-U	0x00000042 0x00000042
	Invalid Instruction 2 - This setting allows the customer to configure invalid instruction to protect against Chip Erase. See Comet Lake LP SPI Programming guide for further details. **Note:** This setting should be set to '0' if there are not Invalid instructions.	CML-Y CML-U	0x00000060 0x00000060
	Invalid Instruction 3 - This setting allows the customer to configure invalid instruction to protect against Chip Erase. See Comet Lake LP SPI Programming guide for further details. **Note:** This setting should be set to '0' if there are not Invalid instructions.	CML-Y CML-U	0x000000AD 0x000000AD
	Invalid Instruction 4 - This setting allows the customer to configure invalid instruction to protect against Chip Erase. See Comet Lake LP SPI Programming guide for further details. **Note:** This setting should be set to '0' if there are not Invalid instructions.	CML-Y CML-U	0x000000B7 0x000000B7
	Invalid Instruction 5 - This setting allows the customer to configure invalid instruction to protect against Chip Erase. See Comet Lake LP SPI Programming guide for further details. **Note:** This setting should be set to '0' if there are not Invalid instructions.	CML-Y CML-U	0x000000B9 0x000000B9
	Invalid Instruction 6 - This setting allows the customer to configure invalid instruction to protect against Chip Erase. See Comet Lake LP SPI Programming guide for further details. **Note:** This setting should be set to '0' if there are not Invalid instructions.	CML-Y CML-U	0x000000C4 0x000000C4
	Invalid Instruction 7 - This setting allows the customer to configure invalid instruction to protect against Chip Erase. See Comet Lake LP SPI Programming guide for further details. **Note:** This setting should be set to '0' if there are not Invalid instructions.	CML-Y CML-U	0x000000C7 0x000000C7
	Quad I/O Read Enabled **Values: Yes/No** - This setting allows the customer to enable support for Quad I/O Read capabilities for flash components. See Comet Lake LP SPI Programming guide for further details.	CML-Y CML-U	Yes Yes
	Quad Output Read Enabled **Values: Yes/No** - This setting allows the customer to enable support for Quad Output Read capabilities for flash components. See Comet Lake LP SPI Programming guide for further details.	CML-Y CML-U	Yes Yes
	Read ID and Read Status clock frequency **Values: 17MHz, 30MHz, 48MHz** - This setting allows the customer to configure the flash component clock frequency setting for Read ID and Read Status. See Comet Lake LP SPI Programming guide for further details.	CML-Y CML-U	48MHz 48MHz
	Write and Erase clock frequency **Values: 17MHz, 30MHz, 48MHz** - This setting allows the customer to configure the flash component clock frequency setting for Write and Erase. See Comet Lake / Coffee Lake LP SPI Programming guide for further details.	CML-Y CML-U	48MHz 48MHz
Click on Flash Settings in the left tabs menu> Legacy VSCC Table is expanded by default:			

Table 2-4. - Flash Settings (Sheet 9 of 11)



#	Parameter	Platform	Settings
7	**Flash Settings - VSCC Table** **VSCC Entries**		
	W25Q128BV		
8	**VSCC Entry**	CML-Y CML-U	
	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.	CML-Y CML-U	Winbond Winbond
	Vendor ID - This configures the JEDEC vendor specific byte ID of the SPI flash component. See Comet Lake LP SPI Programming guide for further details.	CML-Y CML-U	0xEF 0xEF
	Device ID 0 - This configures the JEDEC device specific byte ID 0 of the SPI flash component. See Comet Lake LP SPI Programming guide for further details.	CML-Y CML-U	0x40 0x40
	Device ID 1 - This configures the JEDEC device specific byte ID 1 of the SPI flash component. See Comet Lake LP SPI Programming guide for further details.	CML-Y CML-U	0x18 0x18
9	**+ Add VSCC Entry**		
Click on Flash Settings in the left tabs menu> BIOS Configuration is expanded by default:			

Table 2-4. - Flash Settings (Sheet 10 of 11)

Bios Configuration 10

Parameter	Value	Help Text
Top Swap Block Size	64KB	This configures the Top Swap Block size for the platform.
Write Protection Enable	No	Base/limit are inclusive
Protected Range Limit	0x0000	This field corresponds to FLA (Flash Linear Address) addı
Read Protection Enable	No	Base/limit are inclusive
Protected Range Base	0x0000	This field corresponds to FLA (Flash Linear Address) addı

#	Parameter	Platform	
10	**BIOS Configuration**		
	Top Swap Block Size **Values: 64KB, 128KB, 256KB, 512KB, 1MB** - This configures the Top Swap Block size for the platform. For further details see Comet Lake LP Platform Controller Hub EDS.	CML-Y CML-U	128KB 128KB
	Write Protection Enable	***Note:*** Leave settings at Intel® FIT default values	
	Protected Range Limit		
	Read Protection Enable		
	Protected Range Base		

Click on Flash Settings in the left tabs menu> OEM and Platform IDs is expanded by default:

OEM and Platform IDs 11

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

#	Parameter	Platform	
11	**OEM and Platform IDs**		
	OEM Vendor ID This setting allows OEMs to configure their Unique ID into the platform image.	CML-Y CML-U	0x0 0x0
	OEM Platform ID This setting allows OEMs to configure a Unique Platform ID into the base image.	CML-Y CML-U	0x0 0x0

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

Table 2-4. - Flash Settings (Sheet 11 of 11)

12	**FPF Configuration**		
	FPF Hardware Binding Enabled **Values: Enabled / Disabled** This setting configures the FPF Hardware binding behavior for the platform image. If this setting is enabled FPF Hardware binding will occur when platform close manufacturing flow is executed with Intel® FPT. If this setting is disabled FPF Hardware binding will not take place when close manufacturing flow is executed. ***Note:*** For Revenue parts this setting will be ignored and FPF Hardware binding will take place when close manufacturing flow is executed.	CML-Y CML-U	Disabled Disabled

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

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

▼ Processor (1)

Parameter	Value	Help Text
Processor Emulation	No Emulation	-

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

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

▼ Intel (R) ME Firmware Update (2)

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

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

▼ Intel (R) Services Configuration 3

Parameter	Value	Help Text
ODM ID used by Intel(R) Servi...	0x00000000	-
System Integrator ID used by I...	0x00000000	-
Reserved ID used by Intel(R) S...	0x00000000	-

#	Parameter	Platform	
3	**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.	CML-Y CML-U	0x00000000 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.	CML-Y CML-U	0x00000000 0x00000000
	Reserved ID used by Intel® Services - This setting is for entering the Reserved ID for Intel® Services currently not used.	CML-Y CML-U	0x00000000 0x00000000

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

▼ Image Identification 4

Parameter	Value	Help Text
OEM Tag	0x00000000	-

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

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

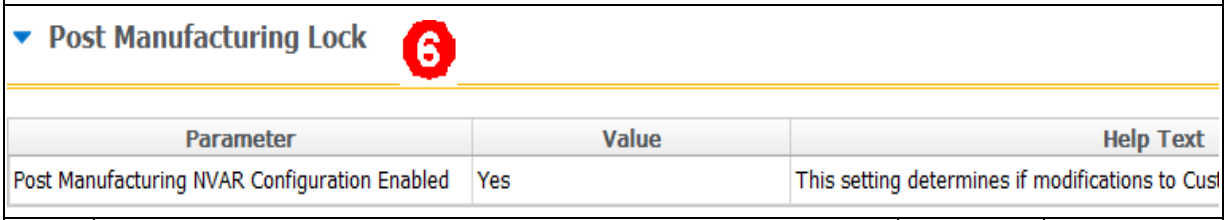
▼ Firmware Diagnostics 5

Parameter	Value	Help Text
Automatic Built in Self Test	Disabled	-

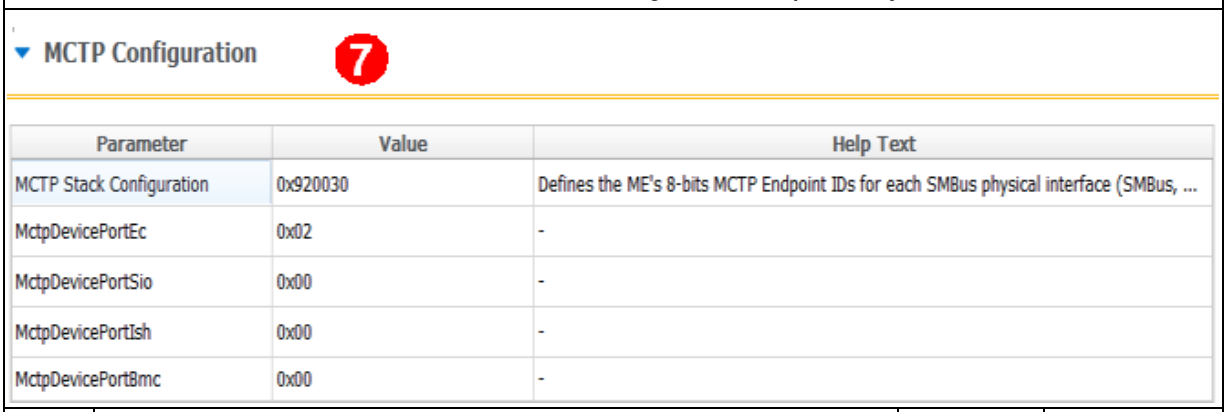
#	Parameter	Platform	Settings
5	**Firmware Diagnostics**		

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

	Automatic Built in Self Test **Values: Enabled / Disabled** This setting enables the firmware Automatic Built in Self Test which is executed during first platform boot after initial image flashing.	CML-Y CML-U	Disabled Disabled
Click on Intel® ME Kernel in the left tabs menu> Post Manufacturing Lock is expanded by default:			

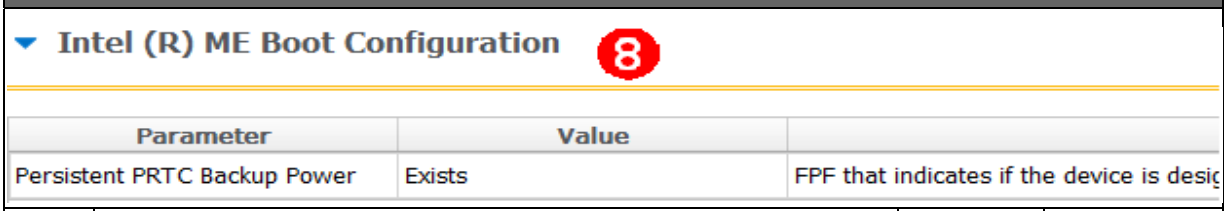


#	Parameter	Platform	Settings
6	**Post Manufacturing Lock**		
	Post Manufacturing NVAR Configuration Enabled - This setting determines if modifications to Customer configurable NVARs is to be allowed after close of manufacturing.	CML-Y CML-U	Yes Yes
Click on Intel® ME Kernel in the left tabs menu> MCTP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

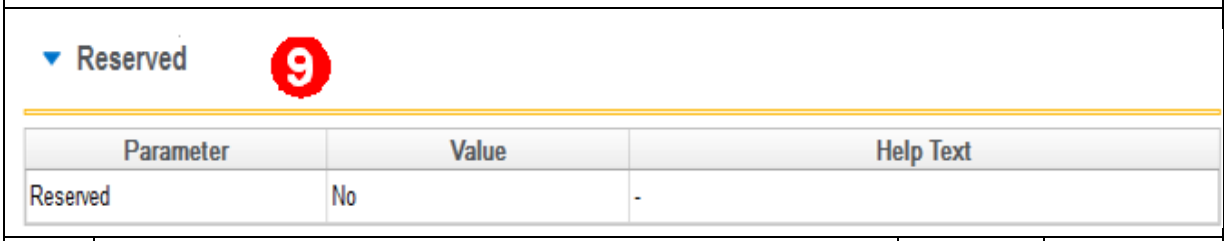


#	Parameter	Platform	Settings
7	**Intel® ME Kernel - MCTP Configuration**		
	MCTP Stack Configuration Defines the Intel® ME's 8-bits MCTP Endpoint ID's for each SMBus physical interface (SMBus, SMLink0, and SMLink1). These values are needed for FW to communicate with MCTP end points. For each of these 3 bytes, a value of 0x00 means not used, and values 0xFF or 0x01 - 0x07 or 0x20 - 0x2F are not allowed.	CML-Y CML-U	0x920030 0x920030
	MctpDevicePortEc	CML-Y CML-U	0x02 0x02
	MctpDevicePortSio	CML-Y CML-U	0x00 0x00
	MctpDevicePortIsh	CML-Y CML-U	0x00 0x00
	MctpDevicePortBmc	CML-Y CML-U	0x00 0x00
Click on Intel® ME Kernel in the left tabs menu> Intel® ME Boot Configuration is expanded by default:			

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



#	Parameter	Platform	Settings
8	**Intel® ME Boot Configuration**		
	Persistent PRTC Backup Power **Values: None / Exists** FPF that indicates if the device is designed such that it may lose PRTC power more than 10 times throughout the normal life-cycle of the product and hence has no persistent time or AR protection. At EOM this value is burned to the FPF, and can never be changed	CML-Y CML-U	Exists Exists
Click on Intel® ME Kernel in the left tabs menu> Reserved is expanded by default:			



9	**Intel® ME Kernel - Reserved**		
	Reserved **Values: Yes / No**	CML-Y CML-U	No No

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

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

Intel(R) AMT Configuration (1)

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

#	Parameter	Platform	Settings
1	**Intel® AMT Configuration**		
	Intel® AMT Supported **Values: Yes/No** - This setting allows customers to disable Intel® AMT on the platform and force the platform into Standard Manageability mode. **Note:** If this setting has been set to disabled Intel® AMT cannot be re-enabled once the descriptor has been locked. This setting applies to Desktop and Workstation only.	CML-Y CML-U	No No
	Intel® ME Network Services Supported **Values: Yes/No -** This setting allows customers to enable / disable Intel® ME Network Services on the platform. **Note:** This setting and TLS needs to be enabled for proper operation of Intel® Authenticate (Corporate Only). In addition if this setting is disabled Intel® AMT will also be disabled.	CML-Y CML-U	No No
	Intel® Manageability Application Supported **Values: Yes/No -** This setting allows customers to force Intel® AMT enabled platforms to operate in Standard Manageability mode. **Note:** This setting only applies to Desktop and Workstation platforms.	CML-Y CML-U	No No
	Manageability Application initial power-up state **Values: Enabled/Disabled** This setting allows customers to determine the power up state for Intel® AMT or Standard Manageability. **Note:** If this setting is disabled Intel® AMT or Standard Manageability can still be re-enabled through the Intel® MEBx interface.	CML-Y CML-U	Disabled Disabled
	Intel® AMT Idle Timeout **Values: 0xFFFF** - This setting configures the idle timeout value before Intel® AMT enters into an off state.	CML-Y CML-U	0xFFFF 0xFFFF
	Intel® AMT Watchdog Automatic Reset Enabled **Values: Yes/No** - This setting allows customers to enable the Intel® ME firmware to trigger an automatic platform reset if either the MEI or Agent Presence are in a hung state. **Note:** This feature only allows one reset at a time when the watchdog expires. After this feature has triggered a reset, it must be re-armed for reuse via management console.	CML-Y CML-U	No No

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

KVM Configuration (2)

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

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

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

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

Provisioning Configuration 3

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

#	Parameter	Platform	
3	**Provisioning Configuration**		
	Embedded Host Based Configuration **Values: Yes / No** - This setting allows customers to enable / disable Embedded Host Based Configuration. Important - EHBC is primarily intended for use in embedded systems as it offers less user privacy/security protection than may be appropriate for business client systems. ***Note:*** The Intel® FIT tool will not adjust the Redirection Privacy/Security value based on selection here. Please set security level as needed.	CML-Y CML-U	No No
	PKI Domain Name Suffix - This setting allow OEMs to pre-configure the Domain Name Suffix used for PKI provisioning in their firmware image. **Note:** For normal out-of-box provisioning functionality this setting should be left empty.	CML-Y CML-U	- -

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

OEM Customizable Certificate 1 4

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

#	Parameter	Platform	Settings
4	**OEM Customizable Certificate 1**		

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

	Certificate Enabled **Values: Yes/No** - This setting allows customers to enable PKI provisioning Custom Certificate 1.	CML-Y CML-U	No No
	Certificate Friendly Name - This setting allows customers to assign a user friendly name for PKI provisioning Custom Certificate 1. Maximum of 32 characters.	CML-Y CML-U	- -
	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.	CML-Y CML-U	- -
Click on Intel® AMT in the left tabs menu> OEM Customizable Certificate 2 is expanded by default:			

#	Parameter	Platform	Settings
5	**OEM Customizable Certificate 2**		
	Certificate Enabled **Values: Yes/No** - This setting allows customers to enable PKI provisioning Custom Certificate 2.	CML-Y CML-U	No No
	Certificate Friendly Name - This setting allows customers to assign a user friendly name for PKI provisioning Custom Certificate 2. Maximum of 32 characters.	CML-Y CML-U	- -
	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.	CML-Y CML-U	- -
Click on Intel® AMT in the left tabs menu> OEM Customizable Certificate 3 is expanded by default:			

#	Parameter	Platform	Settings
6	**OEM Customizable Certificate 3**		
	Certificate Enabled **Values: Yes/No** - This setting allows customers to enable PKI provisioning Custom Certificate 3.	CML-Y CML-U	No No

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

	Certificate Friendly Name - This setting allows customers to assign a user friendly name for PKI provisioning Custom Certificate 3. Maximum 32 characters.	CML-Y CML-U	- -
	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.	CML-Y CML-U	- -
Click on Intel® AMT in the left tabs menu> OEM Default Certificate 1 is expanded by default:			

OEM Default Certificate 1 (7)

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

#	Parameter	Platform	Settings
7	**OEM Default Certificate 1**		
	Certificate Enabled **Values: Yes/No** - This setting allows customers to enable PKI provisioning Default certificate 1.	CML-Y CML-U	No No
	Certificate Friendly Name - This setting allows customers to assign a user friendly name for PKI provisioning Default Certificate 1. Maximum 32 characters.	CML-Y CML-U	- -
	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.	CML-Y CML-U	- -
Click on Intel® AMT in the left tabs menu> OEM Default Certificate 2 is expanded by default:			

OEM Default Certificate 2 (8)

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

#	Parameter	Platform	Settings
8	**OEM Default Certificate 2**		
	Certificate Enabled **Values: Yes/No** - This setting allows customers to enable PKI provisioning Default certificate 2.	CML-Y CML-U	No No
	Certificate Friendly Name - This setting allows customers to assign a user friendly name for PKI provisioning Default Certificate 2. Maximum 32 characters.	CML-Y CML-U	- -

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

	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.	CML-Y CML-U	- -
Click on Intel® AMT in the left tabs menu> OEM Default Certificate 3 is expanded by default:			
OEM Default Certificate 3 (9)			

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

#	Parameter	Platform	Settings
9	**OEM Default Certificate 3**		
	Certificate Enabled **Values: Yes/No** - This setting allows customers to enable PKI provisioning Default certificate 3.	CML-Y CML-U	No No
	Certificate Friendly Name - This setting allows customers to assign a user friendly name for PKI provisioning Default Certificate 3. Maximum 32 characters.	CML-Y CML-U	- -
	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.	CML-Y CML-U	- -
Click on Intel® AMT in the left tabs menu> OEM Default Certificate 4 is expanded by default:			
OEM Default Certificate 4 (10)			

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

#	Parameter	Platform	Settings
10	**OEM Default Certificate 4**		
	Certificate Enabled **Values: Yes/No** - This setting allows customers to enable PKI provisioning Default certificate 4.	CML-Y CML-U	No No
	Certificate Friendly Name - This setting allows customers to assign a user friendly name for PKI provisioning Default Certificate 4.	CML-Y CML-U	- -

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

	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.	CML-Y CML-U	- -
Click on Intel® AMT in the left tabs menu> OEM Default Certificate 5 is expanded by default:			
OEM Default Certificate 5 (11)			

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

#	Parameter	Platform	Settings
11	**OEM Default Certificate 5**		
	Certificate Enabled **Values: Yes/No** - This setting allows customers to enable PKI provisioning Default certificate 5.	CML-Y CML-U	No No
	Certificate Friendly Name - This setting allows customers to assign a user friendly name for PKI provisioning Default Certificate 5.	CML-Y CML-U	- -
	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.	CML-Y CML-U	- -
Click on Intel® AMT in the left tabs menu> Redirection Configuration is expanded by default:			
Redirection Configuration (12)			

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

#	Parameter	Platform	Settings
12	**Redirection Configuration**		
	Redirection Localized Language - This setting allows customers to configure which localized language will be used initially by firmware for user consent output information (Examples: May be displayed before SOL / KVM session starts).	CML-Y CML-U	English English

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

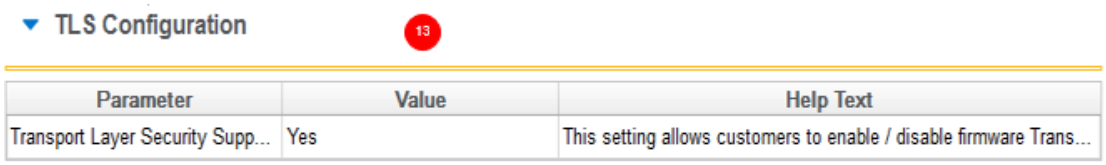
	Redirection Privacy / Security Level - This setting allows customers to configure the Privacy and Security level for redirection operations. **Default** enables all redirection ports (User consent is configurable). **Enhanced** - Enables all redirection ports. (User consent is required and cannot be disabled). **Extreme -** Disables Redirection and Remote Configuration / Client Control Mode. **Note:** The Intel® FIT tool will not adjust the Embedded Host Based Configuration value based on selection here. Please set EHBC to yes or no as needed.	CML-Y CML-U	Default Default
Click on Intel® AMT in the left tabs menu> TLS Configuration is expanded by default:			
			
#	**Parameter**	**Platform**	**Settings**
13	**TLS Configuration**		
	Transport Layer Security Supported **Values: Yes / No** - This setting allows customers to enable / disable firmware Transport Layer Security support. **Note:** If this is disabled TLS will be permanently disabled in the firmware image. This setting needs to be enabled along with along with the Intel® ME Network Services Supported for proper operation of the Intel® Authenticate (Corporate Only) feature.	CML-Y CML-U	No No

Table 2-7. - Platform Protection (Sheet 1 of 8)

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

Content Protection 1

Parameter	Value	Help Text
PAVP Supported	Yes	This setting determines if the Protected Audio Video P
LSPCON Internal Display Port 1 ...	None	This setting determines which port for LSPCON will be
HDCP Internal Display Port 1 - 5K	PortA	This setting determines which port is connected for 5
HDCP Internal Display Port 2 - 5K	None	This setting determines which port is connected for 5

#	Parameter	Platform	Settings
1	**Content Protection**		
	PAVP Supported **Values: Yes/No** This setting determines if the Protected Audio Video Path (PAVP) feature will be permanently disabled in the FW image.	CML-Y CML-U	Yes Yes
	LSPCON Internal Display Port 1 - LSPCON / 4K **values: PortB, PortC, PortD** This setting determines which port for LSPCON will be connected to the HDCP 2.2 bridge adapter Display 1.	CML-Y CML-U	None None
	HDCP Internal Display Port 1 - 5K **Values: None, Port A, Port B, Port C, Port D** This setting determines which port is connected for 5K output on the Internal Display 1. **Note:** Both Display Port 1 & 2 need to be configured for proper operation.	CML-Y CML-U	PortA PortA
	HDCP Internal Display Port 2 - 5K **Values: None, Port A, Port B, Port C, Port D** This setting determines which port is connected for 5K output on the Internal Display 2. **Note:** Both Display Port 1 & 2 need to be configured for proper operation.	CML-Y CML-U	None None

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

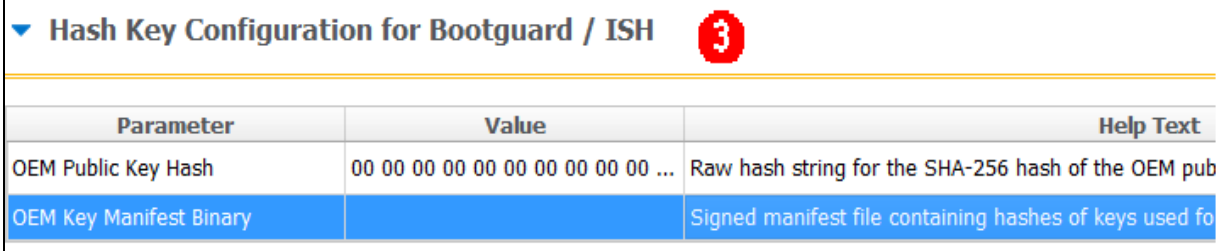
Graphics uController 2

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

#	Parameter	Platform	Settings

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

2	**Graphics UController**		
	GuC Encryption Key **Values:** This option is for entering the raw hash 256 bit string or certificate file for the Graphics uController.	CML-Y CML-U	0x00000000 0x00000000
Click on Platform Protection in the left tabs menu> Hash Key Configuration for Bootguard / ISH is expanded by default:			



#	Parameter	Platform	
3	**Hash Key Configuration for Bootguard / ISH**		
	OEM Public Key Hash **Values:** This option is for entering the raw hash string or certificate file for Boot Guard and ISH. This 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.	CML-Y CML-U	0x00000000 0x00000000
	OEM Key Manifest Binary Signed manifest file containing hashes of keys used for signing components of image. This setting is only configurable when OEM signing is enabled (See PlatformIntegrity / OemPublicKeyHash).	CML-Y CML-U	OEM KM Binary (Optional)
Click on Platform Protection in the left tabs menu> Exclusion Ranges is expanded by default:			

Table 2-7. - Platform Protection (Sheet 3 of 8)

Exclusion Ranges 4

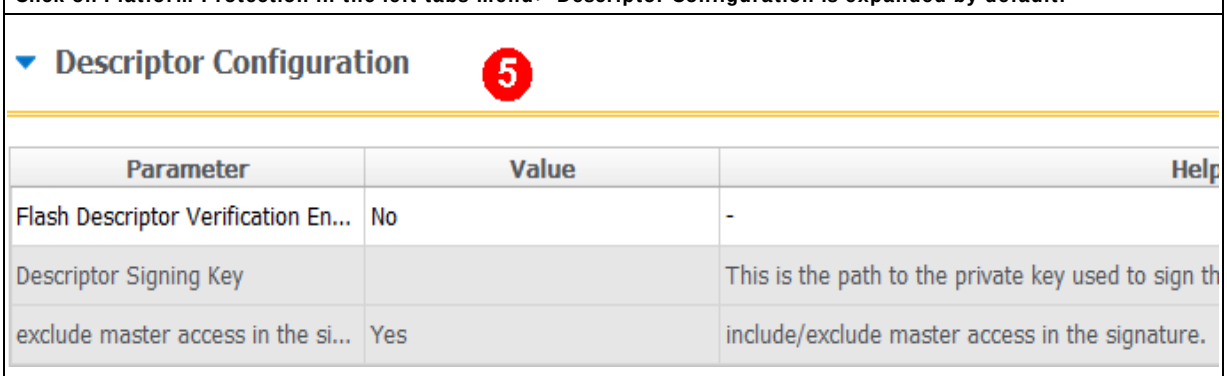
Parameter	Value	Help
Range 1 offset	0x800	Range 1 offset covers manifest, cannot be chang
Range 1 size	0x400	Range 1 size covers manifest, cannot be change
Range 2 offset	0x80	Range 2 offset covers OEM defined unprotected
Range 2 size	0x20	Range 2 size covers OEM defined unprotected ra
Range 3 offset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

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

Table 2-7. - Platform Protection (Sheet 4 of 8)

	Range 4 size **Values:** This offset covers Range 4OEM defined unprotected range length	CML-Y CML-U	0x0 0x0
	Range 5 offset **Values:** This offset covers Range 5 OEM defined unprotected range start	CML-Y CML-U	0x0 0x0
	Range 5 size **Values:** This offset covers Range 5 OEM defined unprotected range length	CML-Y CML-U	0x0 0x0
	Range 6 offset **Values:** This offset covers Range 6 OEM defined unprotected range start	CML-Y CML-U	0x0 0x0
	Range 6 size **Values:** This offset covers Range 6 OEM defined unprotected range length	CML-Y CML-U	0x0 0x0
	Range 7 offset **Values:** This offset covers Range 7 OEM defined unprotected range start	CML-Y CML-U	0x0 0x0
	Range 7 size **Values:** This offset covers Range 7 OEM defined unprotected range length	CML-Y CML-U	0x0 0x0
	Range 8 offset **Values:** This offset covers Range 8 OEM defined unprotected range start	CML-Y CML-U	0x0 0x0
	Range 8 size **Values:** This offset covers Range 8 OEM defined unprotected range length	CML-Y CML-U	0x0 0x0

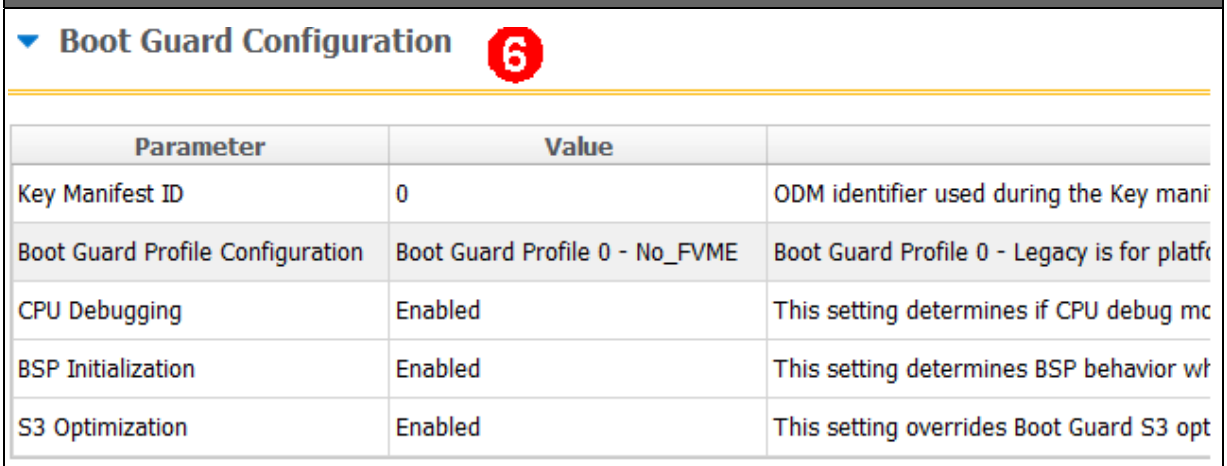
Click on Platform Protection in the left tabs menu> Descriptor Configuration is expanded by default:



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

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

Table 2-7. - Platform Protection (Sheet 5 of 8)

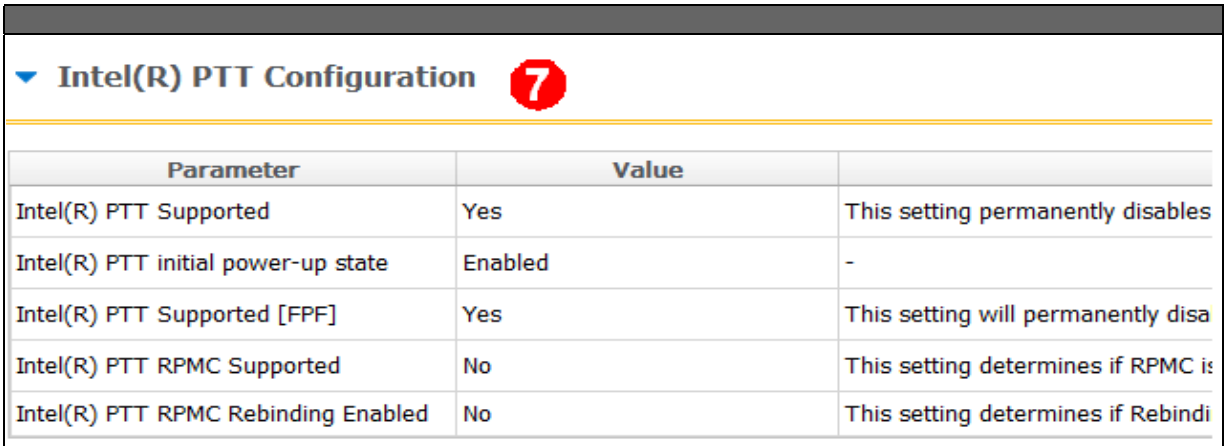


Boot Guard Configuration 6

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

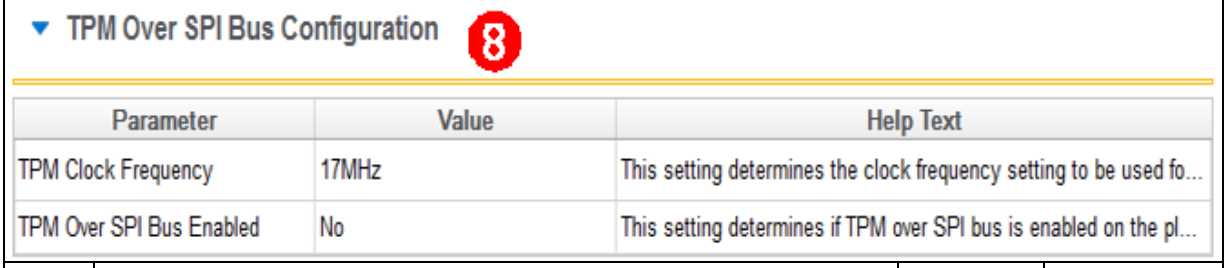
#	Parameter	Platform	Settings
6	**Boot Guard Configuration**		
	Key Manifest ID **Values:** This option is for entering the hash of another public key, used by the ACM to verify the Boot Policy Manifest.	CML-Y CML-U	0x0 0x0
	Boot Guard Profile Configuration **Values: Boot Guard Profile 0 - No_FVME** **Boot Guard Profile 3 - VM** **Boot Guard Profile 4 - FVE** **Boot Guard Profile 5 - FVME** This option configures which Boot Guard Policy Profile will be used.	CML-Y CML-U	Boot Guard Profile 0 - No_FVME Boot Guard Profile 0 - No_FVME
	CPU Debugging **Values: Enabled / Disabled** This setting determines if CPU debug modes will be displayed. When set to 'Enabled' CPU debugging is enabled.	CML-Y CML-U	Enabled Enabled
	BSP Initialization **Values: Enabled / Disabled** This setting determines BSP behavior when it receives an INIT signal. When set to 'Enabled' BSP will behave normally if it receives an INIT (Disabled BSP Initialization (DBI) bit=0). When set to 'Disabled' BSP will shutdown if it receives an INIT ("DBI" bit=1).	CML-Y CML-U	Enabled Enabled
	S3 Optimization **Values: Enabled / Disabled** This setting overrides Boot Guard S3 optimization. ***Note:*** Used for testing only.	CML-Y CML-U	Enabled Enabled
Click on Platform Protection in the left tabs menu> Intel® PTT Configuration is expanded by default:			

Table 2-7. - Platform Protection (Sheet 6 of 8)



#	Parameter	Platform	Settings
7	**Intel® PTT Configuration**		
	Intel® PTT initial power-up state **Values: Enabled / Disabled** - This setting determines if Intel® PTT is enabled on platform power-up.	CML-Y CML-U	Yes Yes
	Intel® PTT Supported **Values: Yes / No** - This setting permanently disables Intel® PTT in the firmware image.	CML-Y CML-U	Enabled Enabled
	Intel® PTT Supported [FPF] **Values: Yes / No** - This setting will permanently disable Intel® PTT through platform FPFs. **Caution:** Using this option will permanently disable Intel® PTT on the platform hardware.	CML-Y CML-U	Yes Yes
	Intel® PTT RPMC Supported **Values: Yes / No** - This setting determines if RPMC is enabled for Intel® PTT. ***Note:*** The SPI parts being used need to support RPMC in order to use this feature.	CML-Y CML-U	No No
	Intel® PTT RPMC Rebinding Enabled **Values: Yes / No** - This setting determines if Rebinding of RPMC enabled SPI parts is supported.	CML-Y CML-U	No No

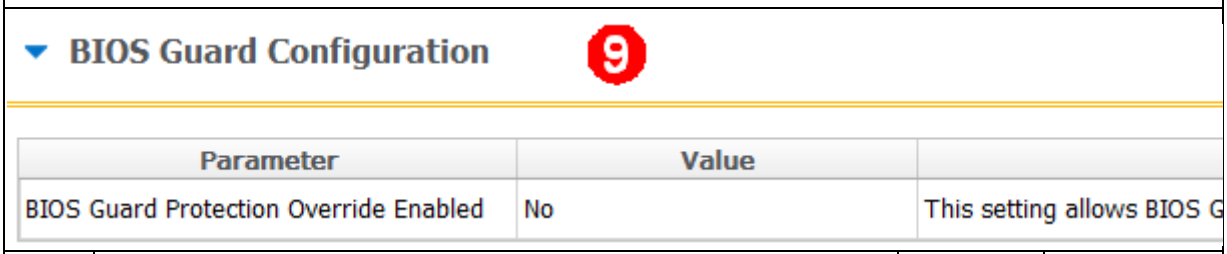
Click on Platform Protection in the left tabs menu> TPM Over SPI Bus Configuration is expanded by default:



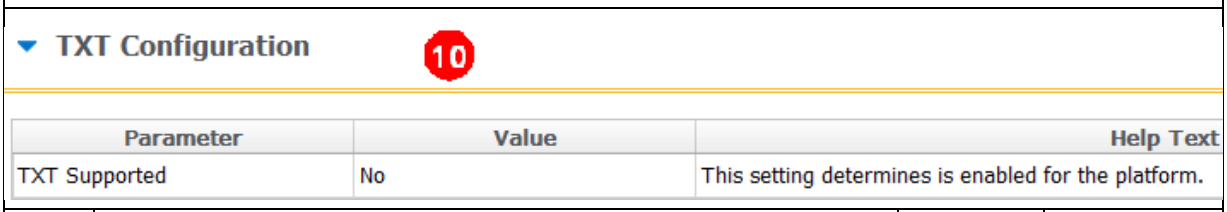
#	Parameter	Platform	Settings
8	**TPM Over SPI Bus Configuration**		
	TPM Clock Frequency **Values: 17MHz, 30MHz, 48MHz** - This setting determines the clock frequency setting to be used for the TPM over SPI bus.	CML-Y CML-U	17MHz 17MHz

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

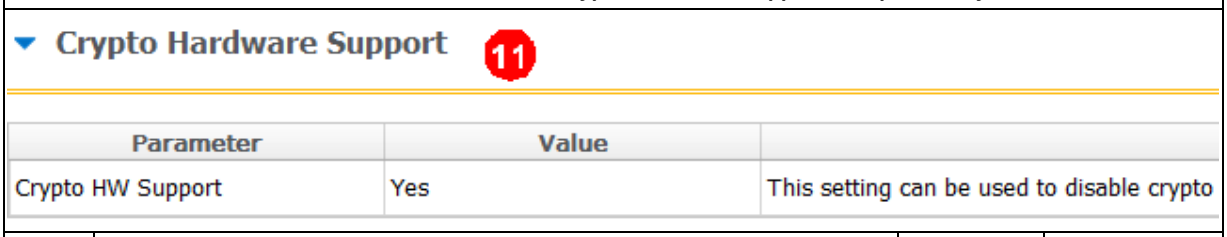
	TPM Over SPI Bus Enabled **Values: Yes / No** - This setting determines if TPM over SPI bus is enabled on the platform.	CML-Y CML-U	Yes Yes
Click on Platform Protection in the left tabs menu> BIOS Guard Configuration is expanded by default:			



#	Parameter	Platform	Settings
9	**BIOS Guard Configuration**		
	BIOS Guard Protection Override Enabled This setting allows BIOS Guard to bypass SPI flash controller protections (i.e. Protected Range Registers and Top Swap).	CML-Y CML-U	Yes Yes
Click on Platform Protection in the left tabs menu> TXT Configuration is expanded by default:			



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



#	Parameter	Platform	Settings
11	**Crypto HW Support**		
	Crypto HW Support **Values: Yes / No** - This setting can be used to disable crypto functionality. This setting disables all crypto related features.	ICL-Y ICL-U	Yes Yes
Click on Platform Protection in the left tabs menu> Platform trusted Device Setup Support is expanded by default:			

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

Platform Trusted Device Setup Support 12

Parameter	Value	Help
Enable TDS Capabilities	No	This setting enables Intel(R) Trusted Device Setu

#	Parameter	Platform	Settings
12	**Platform Trusted Device Setup Support**		
	Enable TDS Capabilities **Values: Yes / No** This setting enables Intel® Trusted Device Setup on the platform	CML-Y CML-U	No No

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

Intel FPF Anti-Rollback Configuration 13

Parameter	Value	Help
FPF SVN Enabled	Disabled	This option enables usage of Intel FPF for Antirolll
RBE SVN Enabled	Disabled	This option enables usage of Intel FPF for Antirolll
IDLM SVN Enabled	Disabled	This option enables usage of Intel FPF for Antirolll

#	Parameter	Platform	Settings
13	**Intel FPF Anti-Rollback Configuration**		
	FPF SVN Enabled This option enables the Intel FPF Anti-Rollback mechanism for all firmware components.	CML-Y CML-U	Enabled Enabled
	RBE SVN Enabled This option enables the Intel FPF Anti-Rollback mechanism for selected firmware components.	CML-Y CML-U	Enabled Enabled
	IDLM SVN Enabled This option enables the Intel FPF Anti-Rollback mechanism for selected firmware components.	CML-Y CML-U	Enabled Enabled

Table 2-8. - Integrated Clock Controller (Sheet 1 of 6)

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

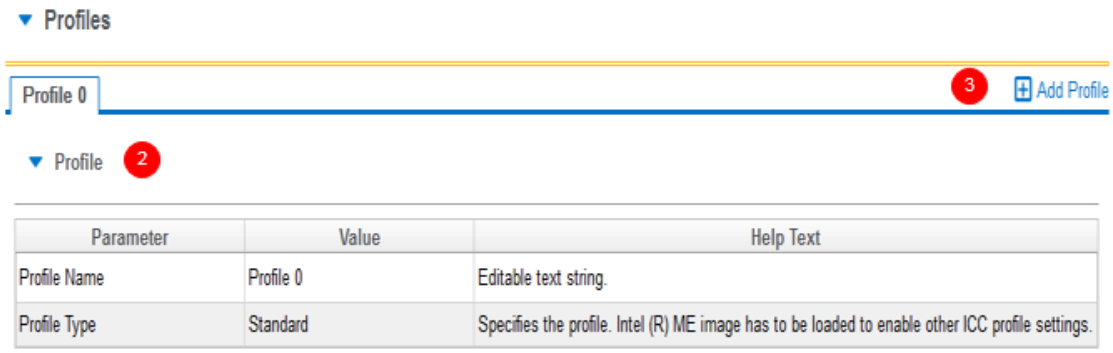
Integrated Clock Controller Policies 1

Parameter	Value	Help
Boot Profile	Profile 0	Profile applied during each boot.
Failsafe Boot Profile	Profile 0	Boot profile used when system instability is detect
Profile Changeable	true	True = Allows user to change boot profile via BIO

#	Parameter	Platform	Settings
1	**Integrated Clock Controller Policies**		
	Boot Profile This parameter allows user to select default profile to be used by the final generated SPI Flash binary image for the target platform at boot time. Selection is limited to the profiles defined under "Integrated Clock Controller | Profiles "up to maximum 16 profiles. Profiles can be added by clicking on "Add profile" button under "Integrated Clock Controller | Profiles". The 'Record #' refers to profile created under the "Integrated Clock Controller | Profiles". Default boot profile for system is Profile 0. Double click on value column of this parameter to choose from available options.	CML-Y CML-U	Profile 0 Profile 0
	Failsafe Profile This parameter specifies the profile index of the fail-safe profile. On boot failure detection or CMOS clear the Intel® ME Firmware will revert to this profile if "**Integrated Clock Controller |Integrated Clock Controller Policies - Profile Changeable "** is set to True. If profile Changeable parameter is set to False, User can not select Failsafe Boot Profile and profile 0 will be selected as a fail safe boot profile by default. The 'Record #' refers to profile created under the "Integrated Clock Controller | Profiles". Default Failsafe boot profile for system is Profile 0. Double click on value column of this parameter to choose from available options.	CML-Y CML-U	Profile 0 Profile 0
	Profile Changeable **Values: true / false** This setting allows the user to change the boot profile via BIOS menu or 3rd party application. ***Note:*** When this set to 'false' both the Failsafe Profile and Boot Profile must match.	CML-Y CML-U	true 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 6)



#	Parameter	Platform	Settings
2	**Profile 0** **Note:** Intel® CSME image has to be loaded to enable other ICC profile settings. For CML-Y/U, Intel® FIT provides 2 pre- defined ICC profiles to choose from. •**Standard**: This profile provides default settings for standard configuration, no adaptive clocking is allowed. Platform clocks output internal and external are driven from USB3PCIE clock. Default clock frequency is 100 MHz with 0.47%DownSpread. BCLK clock source should be turned off in this case to save power. •**Adaptive**: This profile provides Wimax/3G friendly configuration. This profile will configure the platform based on the Adaptive profile allowing adaptive clocking adjustment for BCLK clock source to reduce EMI interference. It supports default clock frequency of 98.875 MHz with 0.48% Downspread. **For** CML-Y/U**,** Intel® FIT provides 5 pre-defined ICC profiles to choose from. •**Standard** •**Adaptive** **Note**: User can select pre-defined profiles via **"Integrated Clock Controller | Profiles - Profile Type "** parameter User can add up to maximum 16 profiles.To add new profile, please use **"Integrated Clock Controller | Profiles - + Add Profile Button"**	CML-Y CML-U	Standard Standard
	Profile Name This parameter allows user to customize profile name for easy identification. By default it uses pre-defined profile name like Profile 0.	CML-Y CML-U	Profile 0 Profile 0
	Profile Type Available ICC profiles for CML-Y/U are Standard, Adaptive. This parameter indicates which pre- defined profile selected for each profile#. Double click on value column of this parameter to choose from available options.	CML-Y CML-U	Standard Standard
3	**+ Add Profile Button** This button is used to add new ICC profile. User can add up to maximum 16 profiles. New profile will be added under **"Integrated Clock Controller | Profiles"** tab**.**	CML-Y CML-U	
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 6)

▼ BclkClockConfiguration 4

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

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

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

▼ ClockRangeDefinitionRecord 5

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

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

Table 2-8. - Integrated Clock Controller (Sheet 4 of 6)

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

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

Clock Output Configuration 6

Parameter	Value	Help Te
ITPXDP	Enabled	Enable/Disable the CLKOUT_ITPXDP differe
SRC0	Enabled	Enable/Disable the CLKOUT_SRC0 differen
SRC1	Enabled	Enable/Disable the CLKOUT_SRC1 differen
SRC2	Enabled	Enable/Disable the CLKOUT_SRC2 differen
SRC3	Enabled	Enable/Disable the CLKOUT_SRC3 differen
SRC4	Enabled	Enable/Disable the CLKOUT_SRC4 differen
SRC5	Enabled	Enable/Disable the CLKOUT_SRC5 differen
LPC0	Enabled	Enable/Disable the CLKOUT_LPC0 single er
LPC1	Enabled	Enable/Disable the CLKOUT_LPC1 single er
CLKOUT CPUNSSC P/N Clock Path Generation	Direct XTAL IN / Out Path	This setting determines if CLKOUT_CPUNS

#	Parameter	Platform	Settings
6	**Clock Output Configuration**		

Table 2-8. - Integrated Clock Controller (Sheet 5 of 6)

	ITPXDP,SRC[0:5] **Values: Enabled / Disabled** These parameters come under the Power Management section and they control Enabling /Disabling of specific Output Clocks at boot time. These settings should match with platform hardware design. For CRB, recommend keeping defaults for bring up with Intel® CSME FW. These parameters are specifically used to Enable/Disable the respective CLKOUT_XXX differential output buffers	CML-Y CML-U	Enabled Enabled
	SRC0[6:15] **Values: Enabled / Disabled** These parameters come under the Power Management section and they control Enabling /Disabling of specific Output Clocks at boot time. These settings should match with platform hardware design. For CRB, recommend keeping defaults for bring up with Intel® CSME FW. These parameters are specifically used to Enable/Disable the respective CLKOUT_XXX differential output buffers	CML-Y CML-U	Enabled Enabled
	SRC1 **Values: Enabled / Disabled** Enables or Disables the CLKOUT_SRC1 differential output buffer.	CML-Y CML-U	Enabled Enabled
	SRC2 **Values: Enabled / Disabled** Enables or Disables the CLKOUT_SRC2 differential output buffer.	CML-Y CML-U	Enabled Enabled
	SRC3 **Values: Enabled / Disabled** Enables or Disables the CLKOUT_SRC3 differential output buffer.	CML-Y CML-U	Enabled Enabled
	SRC4 **Values: Enabled / Disabled** Enables or Disables the CLKOUT_SRC4 differential output buffer.	CML-Y CML-U	Enabled Enabled
	SRC5 **Values: Enabled / Disabled** Enables or Disables the CLKOUT_SRC5 differential output buffer.	CML-Y CML-U	Enabled Enabled
	LPC0[1:0] **Values: Enabled / Disabled** These parameters are used to control Enabling/Disabling of CLKRUN support for CLKOUT_LPC clocks. For CRB, recommend keeping defaults for bring up with Intel® CSME FW	CML-Y CML-U	Enabled Enabled
	LPC1 **Values: Enabled / Disabled** Enables or Disables the CLKOUT_LPC1 single ended output buffer.	CML-Y CML-U	Enabled Enabled
	CLKOUT CPUSSC P/N Clock Path Generation **Values: HDA PLL Path / Direct XTAL IN / Out Path** This setting determines if CLKOUT CPUSSC P/N Clock Path is generated through the HDA_PLL or from Direct XTAL IN/OUT.	CML-Y CML-U	Direct XTAL IN / Out Path 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 6 of 6)

Power Management Configuration 7

Parameter	Value	
SRC0 CLKREQ# Mapping	GPP_B5	Assign the CLKREQ# signal associated with C
SRC1 CLKREQ# Mapping	GPP_B6	Assign the CLKREQ# signal associated with C
SRC2 CLKREQ# Mapping	GPP_B7	Assign the CLKREQ# signal associated with C
SRC3 CLKREQ# Mapping	GPP_B8	Assign the CLKREQ# signal associated with C
SRC4 CLKREQ# Mapping	GPP_B9	Assign the CLKREQ# signal associated with C
SRC5 CLKREQ# Mapping	GPP_B10	Assign the CLKREQ# signal associated with C
24Mhz Crystal Shutdown Wait I...	8us	Enable Dynamic power management of Cryst

#	Parameter	Platform	Settings
7	**Power Management Configuration** Configuring CLKREQ# and assigning GPIO depends on how CLKOUT_SRCx configuration via FIT is done (Enabled or Disabled) and if CLKREQ is required or not. **Please refer to Appendix B.3 (How to configure CLKREQ# parameters)** for the detail of CLKREQ configuration for SRC Output clocks. Please configure CLKREQ parameters accordingly.		
	SRC0[5:0] CLKREQ# Mapping Possible configuration: Select one of the GPIOs from the list to map it as a CLKREQ# for specific SRC# Output clock. This parameter controls association of dynamic CLKREQ control with SRC (PCIe) clocks. **SRC[15:6] CLKREQ# Mapping - CNL/CFL H/S Only** Possible configuration: Select one of the GPIOs from the list to map it as a CLKREQ# for specific SRC# Output put clock. This parameter controls association of dynamic CLKREQ control with SRC (PCIe) clocks.	CML-Y CML-U	GPP_B5 GPP_B5
	SRC1 CLKREQ# Mapping Assign the CLKREQ# signal associated with CLKOUT_SRC1.	CML-Y CML-U	GPP_B6 GPP_B6
	SRC2 CLKREQ# Mapping Assign the CLKREQ# signal associated with CLKOUT_SRC2.	CML-Y CML-U	GPP_B7 GPP_B7
	SRC3 CLKREQ# Mapping Assign the CLKREQ# signal associated with CLKOUT_SRC3.	CML-Y CML-U	GPP_B8 GPP_B8
	SRC4 CLKREQ# Mapping Assign the CLKREQ# signal associated with CLKOUT_SRC4.	CML-Y CML-U	GPP_B9 GPP_B9
	SRC5 CLKREQ# Mapping Assign the CLKREQ# signal associated with CLKOUT_SRC5.	CML-Y CML-U	GPP_B10 GPP_B10
	24MHz Crystal Shutdown Wait Interval This parameter allows user to Enable Dynamic power management of Crystal. Upon the event that all conditions (other than this wait timer itself) are satisfied for iSCLK crystal shutdown, a timer is started. Once it expires and there are no wake events, iSCLK will shutdown crystal. **Note:** Recommendation is to leave setting at default value.	CML-Y CML-U	8us 8us

Table 2-9. - Networking & Connectivity (Sheet 1 of 3)

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

Platform vPro NIC 1

Parameter	Value	He
Platform Discrete vPro NIC Enabled	No	YES = Discrete NIC enabled in platform NO = Int
Platform Discrete vPro NIC SMBUS slave address	0x49	Platform discrete NIC slave address Note: Input

#	Parameter	Platform	Settings
1	**Platform vPro NIC**		
	Platform Discrete vPro NIC Enabled This setting enables Intel® vPro with discrete NIC on the platform.	CML-Y CML-U	No No
	Platform Discrete vPro NIC SMBus slave address This setting configures the discrete NIC SMBus slave address.	CML-Y CML-U	0x49 0x49

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

Docking Station 2

Parameter	Value	Help T
vPro Dock Enabled	No	YES = Enables communication with, vPro supporting NIC,
vPro NIC on dock slave SMBUS Address	0x69	Dock NIC slave address Note: Input needs to be in HEX fo
Type-C Port1 Re-Timer I2C Address	0x20	This setting configures the Intel(R) SMBus I2C Address. N
Type-C Port2 Re-Timer I2C Address	0x21	This setting configures the Intel(R) SMBus I2C Address. N
Type-C Port3 Re-Timer I2C Address	0x22	This setting configures the Intel(R) SMBus I2C Address. N
Type-C Port4 Re-Timer I2C Address	0x23	This setting configures the Intel(R) SMBus I2C Address. N

#	Parameter	Platform	Settings
2	**Docking Station**		
	vPro Dock Enabled This setting enables Intel® vPro communication over supported NIC in a Thunderbolt™ Dock.	CML-Y CML-U	No No
	vPro NIC on dock slave SMBus Address This setting configures the NIC SMBus slave address.	CML-Y CML-U	0x69 0x69
	Type-C Port1 Re-Timer I2C Address This setting configures Intel® SMBus I2C Address.	CML-Y CML-U	0x20 0x20
	Type-C Port2 Re-Timer I2C Address This setting configures Intel® SMBus I2C Address.	CML-Y CML-U	0x21 0x21
	Type-C Port3 Re-Timer I2C Address This setting configures Intel® SMBus I2C Address.	CML-Y CML-U	0x22 0x22
	Type-C Port4 Re-Timer I2C Address This setting configures Intel® SMBus I2C Address.	CML-Y CML-U	0x23 0x23

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

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

Wired LAN Configuration 3

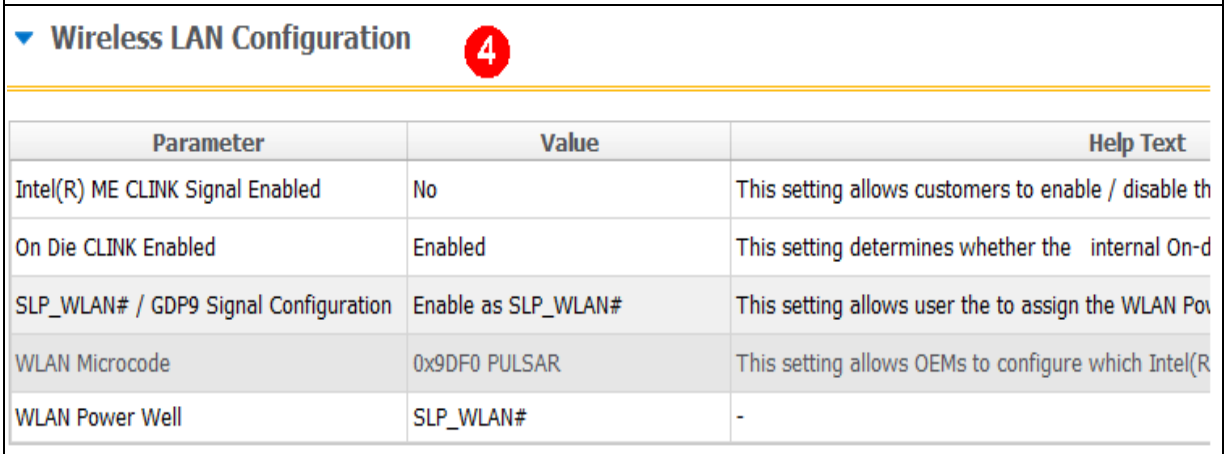
Parameter	Value	Help Text
LAN Power Well	SLP_LAN#	This setting allows the customer to configure
LAN PHY Power Up Time	100 ms	This bit determines how long the delay for L
Intel(R) Integrated Wired LAN Enabled	Yes	This setting allows customers to enable / dis
GbE PCIe Port Select	Port13	This setting allows customers to configure th
GbE PHY SMBus Address	0x64	This is the Intel PHY's SMBus address. This
GbE MAC SMBus Address Enabled	Yes	This enables the Intel(R) Integrated Wired L
GbE MAC SMBus Address	0x70	This setting configures Intel(R) Integrated W
Intel(R) PHY over PCIe Enabled	Yes	This setting allows customers to enable / dis
PHY Connection	PHY on SMLink0	This selects which SMBus network is used to
LAN PHY Power Control GPD11 Signal Configuration	Enable as LANPHYPC	This setting allows the user to assign the LAI

#	Parameter	Platform	Settings
3	**Wired LAN Configuration**		
	LAN Power Well **Values: Core Well, Sus Well, ME Well, SLP_LAN** - This setting allows customers to configure the power well that will be used by Intel® Integrated LAN. **Note:** Recommended setting is SLP_LAN#.	CML-Y CML-U	SLP_LAN# SLP_LAN#
	LAN PHY Power Up Time **Values: 50ms, 100ms**	CML-Y CML-U	100ms 100ms
	Intel® Integrated Wired LAN Enable **Values: Enabled/Disabled -** This setting enables or disables the Intel® Integrated LAN.	CML-Y CML-U	Yes Yes
	GbE PCIe Port Select **Values: PORT7, PORT8, PORT9, PORT13, PORT14** - This setting allows customers to configure the PCIe Port that will Intel® Integrated LAN will operate on.	CML-Y CML-U	Port13 Port13
	GbE PHY SMBus Address This setting configures Intel® Integrated Wired LAN SMBus address to accept SMBus cycles from the MAC. **Note:** Recommended setting is 64h.	CML-Y CML-U	0x64 0x64
	GbE SMBus Address Enabled **Values: Yes/No** - This enables the Intel® Integrated Wired LAN MAC SMBus address. **Note:** This setting must be enabled if using Intel® Integrated LAN.	CML-Y CML-U	Yes Yes
	GbE MAC SMBus Address	CML-Y CML-U	0x70 0x70
	Intel® PHY over PCIe Enabled **Values: Yes/No** - This setting allows customers to enable / disable Intel® Integrated LAN operation over the PCIe Port selected by the GbE PCIe Port Select option.	CML-Y CML-U	Yes Yes
	PHY Connection **Values: No PHY connected, PHY on SMLink0**	CML-Y CML-U	PHY on SMLink0 PHY on SMLink0

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

	LAN PHY Power Control GPD11 Signal Configuration **Values: GPD11, LANPHYPC -** This setting allows the customer to assign the LAN PHY Power Control signal to GbE or as GDP11. **Note:** If using Intel® Integrated LAN this setting should be set to "Enable as LANPHYPC".	CML-Y CML-U	LANPHYPC LANPHYPC

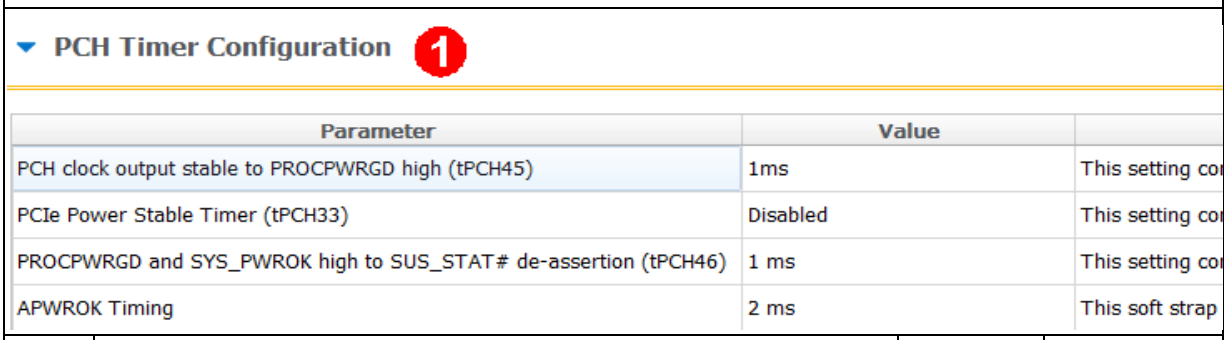
Click on Networking & Connectivity in the left tabs menu> Wireless LAN Configuration is expanded by default:



#	Parameter	Platform	Settings
4	**Wireless LAN Configuration**		
	CLINK Enabled **Values: Yes/No** - This setting allows customers to enable / disable the Wireless LAN CLINK signal through Intel® ME firmware. **Note:** For using Intel® vPro™ Wireless solutions this should be set to "Yes".	CML-Y CML-U	No No
	SLP_WLAN# / GPD9 Signal Configuration **Values: SLP_WLAN#, GPD9** - This setting allows the customer to assign the WLAN Power Control signal to WLAN or as GDP9. **Note:** If using Intel® Wireless LAN this setting should be set to "Enable as SLP_WLAN#".	CML-Y CML-U	Enable as SLP_WLAN# Enabled as SLP_WLAN #
	WLAN Microcode - This setting allow OEMs to configure which Intel® Wireless LAN card microcode to load into the firmware image.	CML-Y CML-U	0x2526 0x2526
	WLAN Power Well **Values: Disabled, Sus Well, ME Well, SLP_M#||SPDA, SLP_WLAN#** - This setting allows OEMs to configure the power well that will be used by Intel® Wireless LAN. WLAN Sleep via SLP_WLAN# (default) **Note:** Recommended setting is SLP_WLAN#.	CML-Y CML-U	SLP_WLAN# 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	**PCH Timer Configuration**		
	PCH clock output stable to PROCPWRGD high (tPCH45) **Values: 100ms, 50ms, 5ms, 1ms** - This setting configures the minimum timing from XCK_PLL locked to CPUPWRGD high. For further details see Comet Lake LP Platform Controller Hub EDS.	CML-Y CML-U	1ms 1ms
	PCIe Power Stable Timer (tPCH33) **Values: Enabled / Disabled** - This setting configures the enables / disables the t36 timer. When enabled PCH will count 99ms from PWROK assertion before PLTRST# is de-asserted. **Note:** The recommended setting is "Disabled".	CML-Y CML-U	Disabled Disabled
	PROCPWRGD and SYS_PWROK high to SUS_STAT# de-assertion (tPCH46) **Values: 1ms, 2ms, 5ms** - This setting configures the minimum timing from CPUPWRGD assertion to SUS_STAT#. For further details see Comet Lake LP Platform Controller Hub EDS.	CML-Y CML-U	1ms 1ms
	APWROK Timing **Values: 2ms, 4ms, 8ms, 16ms** - This soft strap determines the time between the SLP_A# pin de-asserting and the APWROK timer expiration. For further details see Comet Lake LP Platform Controller Hub EDS.	CML-Y CML-U	2ms 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

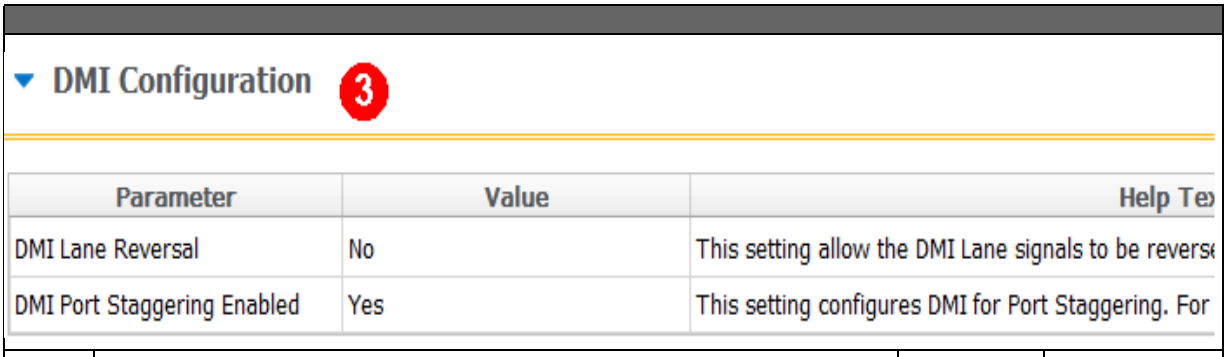
Parameter	Value	
Intel(R) SMBus ASD Address	0x0	This setting configures the Intel(R)
Intel(R) SMBus ASD Address Enabled	No	This setting enables / disables the
Intel(R) SMBus Subsystem Vendor and Device ID for ASF	0x0	This setting configures the Intel(R)
Intel(R) SMBus I2C Address	0x0	This setting configures the Intel(R)
Intel(R) SMBus I2C Address Enabled	No	This setting enables / disables the
Intel(R) SMBus MCTP Address	0x0	This setting configures the Intel(R)
Intel(R) SMBus MCTP Address Enabled	No	This setting enables / disables the
SMBus / SMLink TCO Slave Connection	Intel(R) SMBus	This setting configures the TCO Sl
SMLink0 Enabled	Yes	This setting enables / disables SM
SMLink0 Frequency	1 MHz	This setting determines the freque
SMLink1 I2C Target Address	0x0	This setting configures SMLink1 I2
SMLink1 I2C Target Address Enabled	No	This setting configures SMLink1 I2
SMLink1 GP Target Address	0x0	This setting configures SMLink1 GF
SMLink1 GP Target Address Enabled	No	This setting enables / disables SM
SMLink1 Enabled	No	This setting enables / disables SM
SMLink1 Frequency	100 KHz	This setting determines the freque
Intel(R) SMBus ASD Mode Configuration	Enable as GPP_C2	This setting determines the native
Intel(R) SMLink0 MCTP Address	0x0	This setting configures the Intel(R)

#	Parameter	Platform	Settings
2	**SMBus / SMLink Configuration**		
	Intel® SMBus ASD Address - This setting configures the Intel® SMBus Alert Sending Device Address. For details see Comet Lake LP SPI Programming guide for further details.	CML-Y CML-U	0x00000000 0x00000000
	Intel® SMBus ASD Address Enable **Values: Yes / No** - This setting enables / disables the Intel® SMBus Alert Sending Device. For details see Comet Lake LP SPI Programming guide for further details.	CML-Y CML-U	No No
	Intel® SMBus Subsystem Vendor & Device ID for ASF - This setting configures the Intel® SMBus Subsystem Vendor & Device ID for ASF. For details see Comet Lake LP SPI Programming guide further details.	CML-Y CML-U	0x00000000 0x00000000

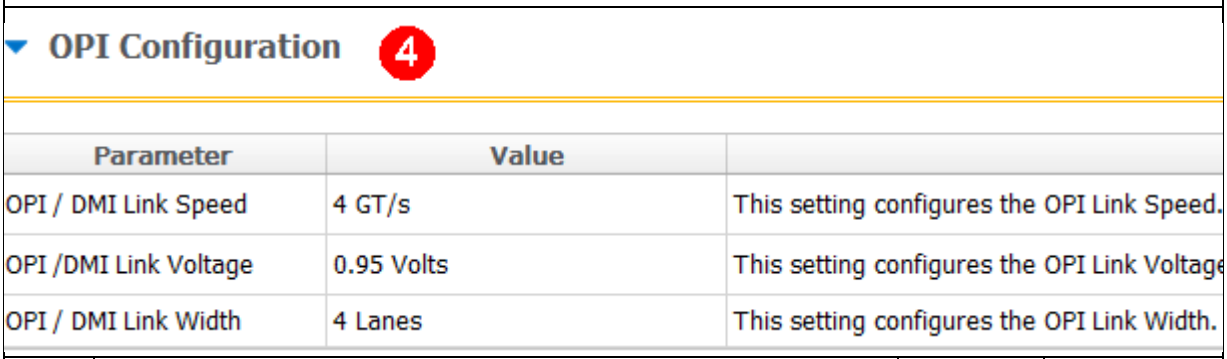
Table 2-10. - Internal PCH Buses (Sheet 3 of 5)

	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".	CML-Y CML-U	0x00000000 0x00000000
	Intel® SMBus I2C Address Enabled **Values: Yes/No** - This setting enables / disables the Intel® SMBus I2C Address. Note: This setting is only used for testing purposes. The recommended setting is "No".	CML-Y CML-U	No No
	Intel® SMBus MTCP Address - This setting configures the Intel® SMBus MCTP Address. **Note:** This setting is only used for testing purposes. The default setting is "0000000".	CML-Y CML-U	0x00000000 0x00000000
	Intel® SMBus MCTP Address Enabled **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".	CML-Y CML-U	No No
	SMBus / SMLink TCO Slave Connection **Values: Intel® SMBus, SMLink0** - This setting configures the TCO Slave connection to ether the Intel® SMBus or SMLink0. For further details see Comet Lake LP Platform Controller Hub EDS.	CML-Y CML-U	Intel® SMBus Intel® SMBus
	SMLink0 Enabled **Values: Yes/No** - This setting enables / disables SMLink0 interface. For further details see Comet Lake LP Platform Controller Hub EDS.	CML-Y CML-U	Yes Yes
	SMLink0 Frequency **Values: 100KHz, 400KHz, 1 MHz** - This setting determines the frequency at which the SMLink0 will operate. **Note:** The recommended setting is "1MHz".	CML-Y CML-U	1 MHz 1 MHz
	SMLink1 I2C Target Address - This setting configures SMLink1 I2C Target Address. For further details see Comet Lake LP Platform Controller Hub EDS.	CML-Y CML-U	0x00000000 0x00000000
	SMLink1 I2C Target Address Enabled **Values: Yes/No** - This setting configures SMLink1 I2C Target Address. For further details see Comet Lake LP Platform Controller Hub EDS.	CML-Y CML-U	No No
	SMLink1 Enabled **Values: Yes/No** - This setting enables / disables SMLink1 interface. For further details see Comet Lake LP Platform Controller Hub EDS. **Note:** This setting must be set to "Yes" if using PCH / MCP Thermal reporting.	CML-Y CML-U	No No
	SMLink1 GP Target Address - This setting configures SMLink1 GP Target Address. For further details see Comet Lake LP Platform Controller Hub EDS.	CML-Y CML-U	0x00000000 0x00000000
	SMLink1 GP Target Address Enabled **Values: Yes/No** - This setting enables / disables SMLink1 GP Target Address interface. For further details see Comet Lake LP Platform Controller Hub EDS. **Note:** This setting must be set to "Yes" if using PCH / MCP Thermal reporting.	CML-Y CML-U	Yes Yes
	SMLink1 Frequency **Values: 100KHz, 400KHz, 1 MHz** - This setting determines the frequency at which the SMLink1 will operate. **Note:** The recommended setting is "100KHz".	CML-Y CML-U	100 KHz 100 KHz
	Intel® SMBus ASD Mode Configuration This setting determines the native mode of operation for the Intel® SMBus ASD signal.	CML-Y CML-U	Enable as GPP_C2 Enable as GPP_C2
	Intel® SMLink0 MCTP Address This setting configures the Intel® SMLink0 MCTP Address.	CML-Y CML-U	0x0 0x0
Click on Internal PCH Buses in the left tabs menu> DMI Configuration is expanded by default:			

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



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



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

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

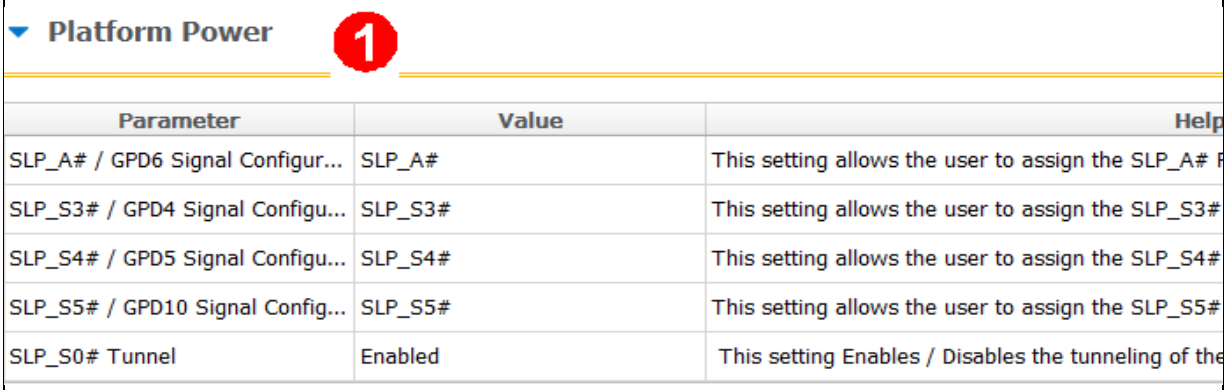
eSPI Configuration 5

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

#	Parameter	Platform	Settings
5	**eSPI Configuration**		
	eSPI / EC Bus Frequency **20MHz, 24MHz, 30MHz, 40MHz, 60MHz**	CML-Y CML-U	60MHz 60MHz
	eSPI / EC Maximum I/O Mode **Values: Single, Single and Dual, Single and Quad, Single Dual and Quad**	CML-Y CML-U	Single, Dual and Quad Single, Dual and Quad
	eSPI / EC CRC Check Enabled **Values: Yes/No**	CML-Y CML-U	Yes Yes
	eSPI / EC Max Outstanding Request for Master Attached Flash Channel	CML-Y CML-U	2 2
	eSPI / EC Slave Attached Flash Multiple Outstanding Requests Enable	CML-Y CML-U	Single Single
	eSPI / EC Slave Attached Flash Channel OOO Enable	CML-Y CML-U	In-Order In-Order

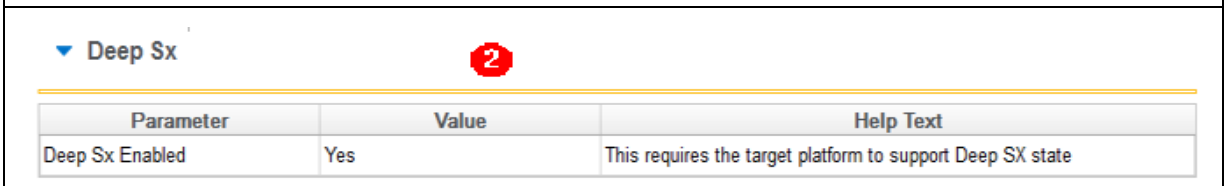
Table 2-11. - Power (Sheet 1 of 2)

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



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

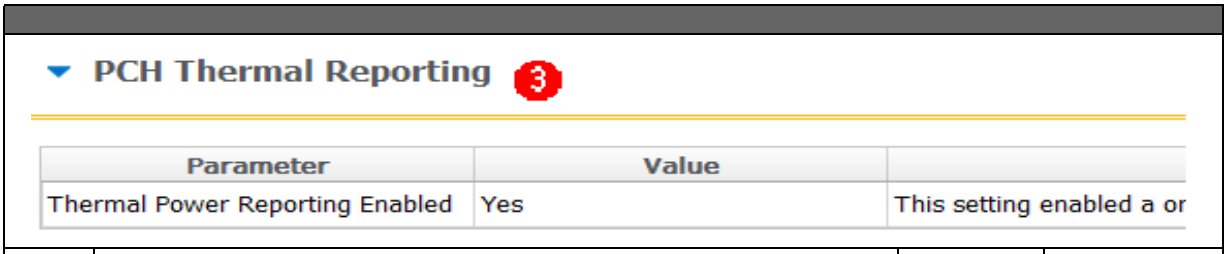
Click on Power in the left tabs menu> Deep Sx is expanded by default:



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

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

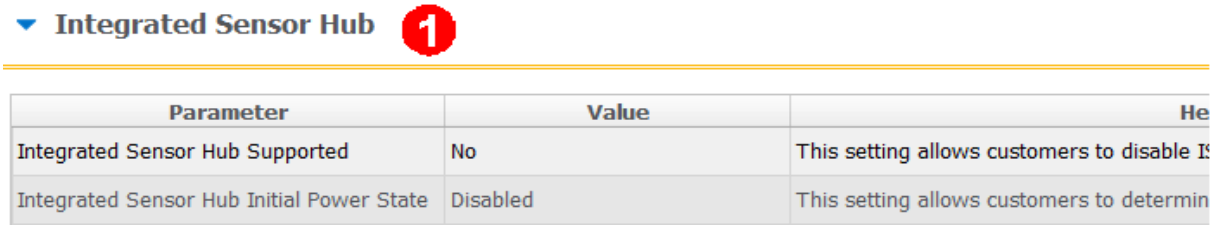
Table 2-11. - Power (Sheet 2 of 2)



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

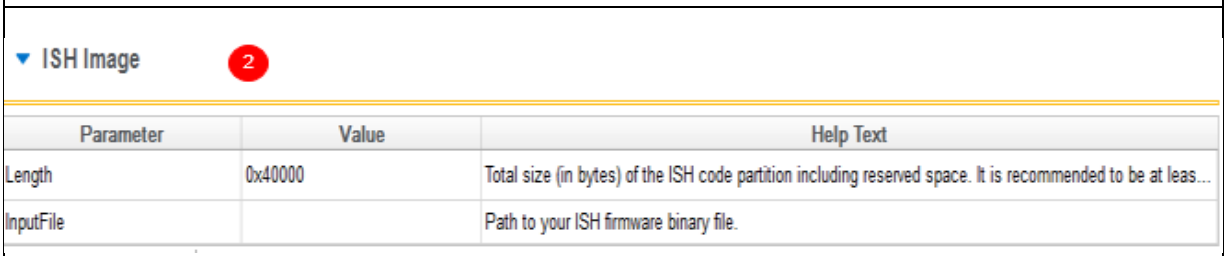
Table 2-12. - Integrated Sensor Hub (Sheet 1 of 2)

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



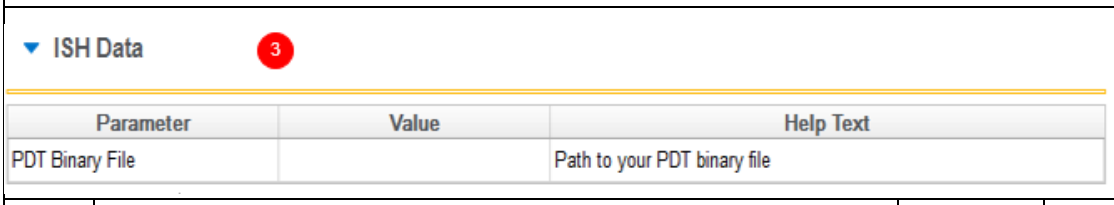
#	Parameter	Platform	Settings
1	**Integrated Sensor Hub**		
	Integrated Sensor Hub Supported **Values: Yes / No** This setting allows customers to disable ISH on the platform.	CML-Y CML-U	No No
	Integrated Sensor Hub Power Up State **Values: Enabled / Disabled** Field is enabled for editing if "Integrated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

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



#	Parameter	Platform	Settings
2	**ISH Image**		
	Length - Total size (in bytes) of the ISH code partition including reserved space. It is recommended to be at least 256kb.	CML-Y CML-U	
	ISH Input File	CML-Y CML-U	

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



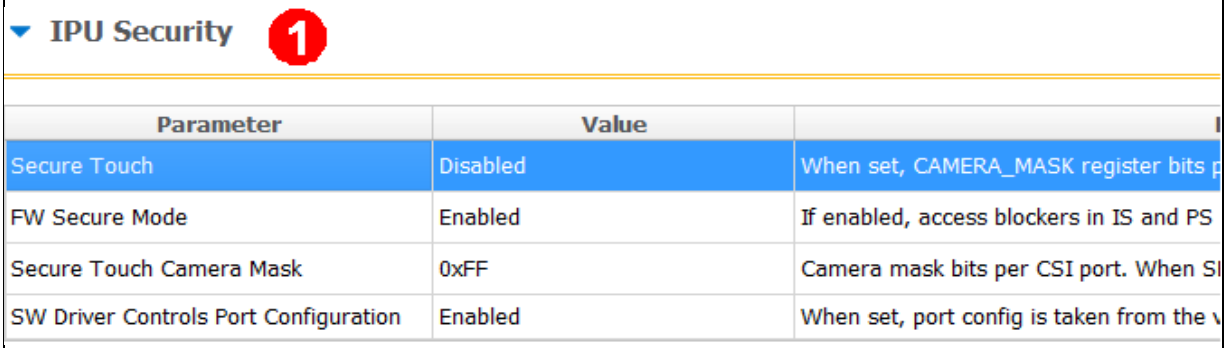
#	Parameter	Platform	Settings
3	**Integrated Sensor Hub - ISH Data**		

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

	PDT Binary File	CML-Y CML-U	Path for PDT Binary file Path for PDT Binary file

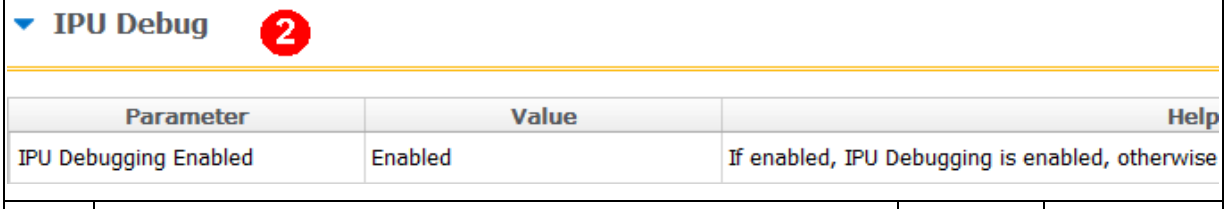
Table 2-13. - Camera (Sheet 1 of 2)

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



#	Parameter	Platform	Settings
1	**IPU Security**		
	Secure Touch When set, CAMERA_MASK register bits per CSI port are used to mask the data of cameras. When cleared, camera data is not masked.	CML-Y CML-U	Disabled Disabled
	FW Secure Mode If enabled, access blockers in IS and PS are enabled, and FW is read from IMR. Must be enabled for FW authentication flow and execution of authenticated FW.	CML-Y CML-U	Enabled Enabled
	Secure Touch Camera Mask Camera mask bits per CSI port. When SECURE_TOUCH is set each set bit masks a CSI port for secure touch. When SECURE_TOUCH is cleared this register has no impact on the CSI ports.	CML-Y CML-U	0xFF 0xFF
	SW Driver Controls Port Configuration When set, port config is taken from the value IPU driver configures in IPU. When cleared, port config is taken from: CSI2_PORT_CONFIG_MSB.PORT_ID and CSI2_PORT_CONFIG_LSB.PORT_ID	CML-Y CML-U	Enabled Enabled

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



#	Parameter	Platform	Settings
2	**IPU Debug**		
	IPU Debugging Enabled If enabled, IPU Debugging is enabled, otherwise internal setup is checked to see if the IPU Debugging feature should be enabled or not.	CML-Y CML-U	Enabled Enabled

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

Table 2-13. - Camera (Sheet 2 of 2)

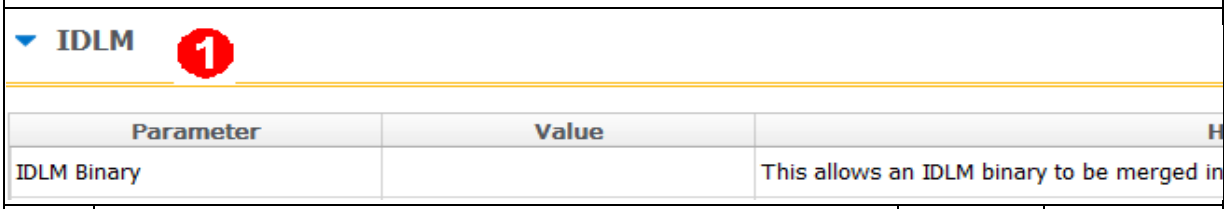
IPU PHY 3

Parameter	Value	He
Port Configuration For 8 LSB Lanes	0x0000	When CSI2_CNL.CR_OVRD is cleared this determ
Port Configuration For 8 MSB Lanes	0x0000	When CSI2_CNL.CR_OVRD is cleared this determ

#	Parameter	Platform	Settings
3	**IPU PHY**		
	Port Configuration for 8 LSB Lanes	CML-Y CML-U	0x0000 0x0000
	Port Configuration for 8 MSB Lanes	CML-Y CML-U	0x0000 0x0000

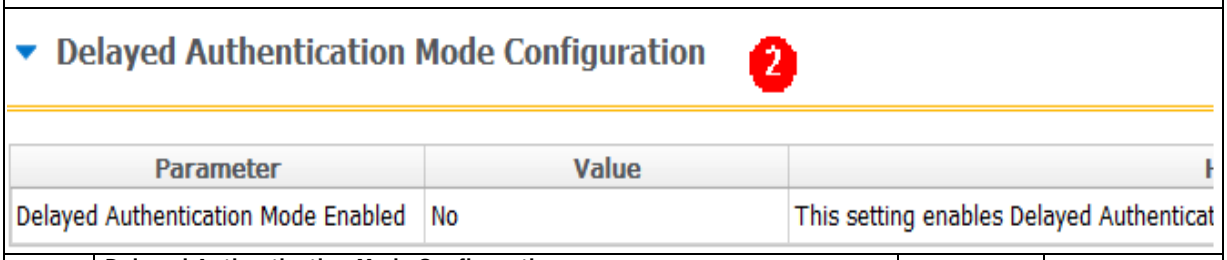
Table 2-14. - Debug (Sheet 1 of 5)

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



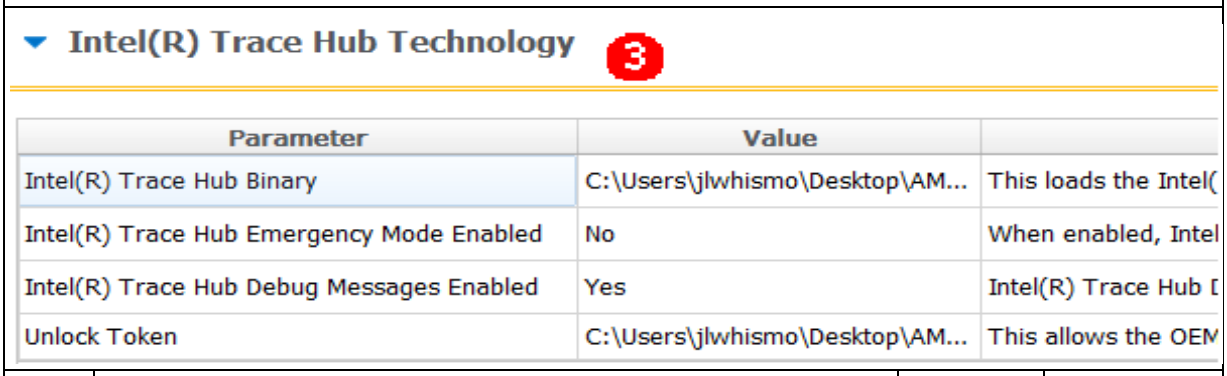
#	Parameter	Platform	Settings
1	**IDLM**		
	IDLM Binary This allows an IDLM binary to be merged into output image built by Intel® FIT.	CML-Y CML-U	

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



2	**Delayed Authentication Mode Configuration**		
	Delayed Authentication Mode Enabled **Values: Yes / No** - This setting enables Delayed Authentication Mode on the platform.	CML-Y CML-U	No No

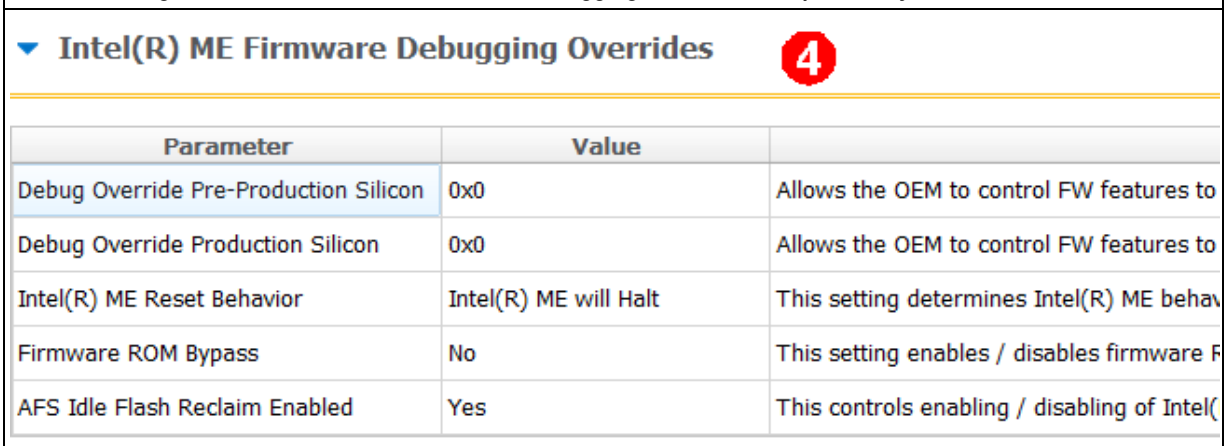
Click on Debug in the left tabs menu> Intel® Trace Hub Technology is expanded by default:



#	Parameter	Platform	Settings
3	**Intel® Trace Hub Technology**		
	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.	CML-Y CML-U	Trace Hub Binary Trace Hub Binary

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

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

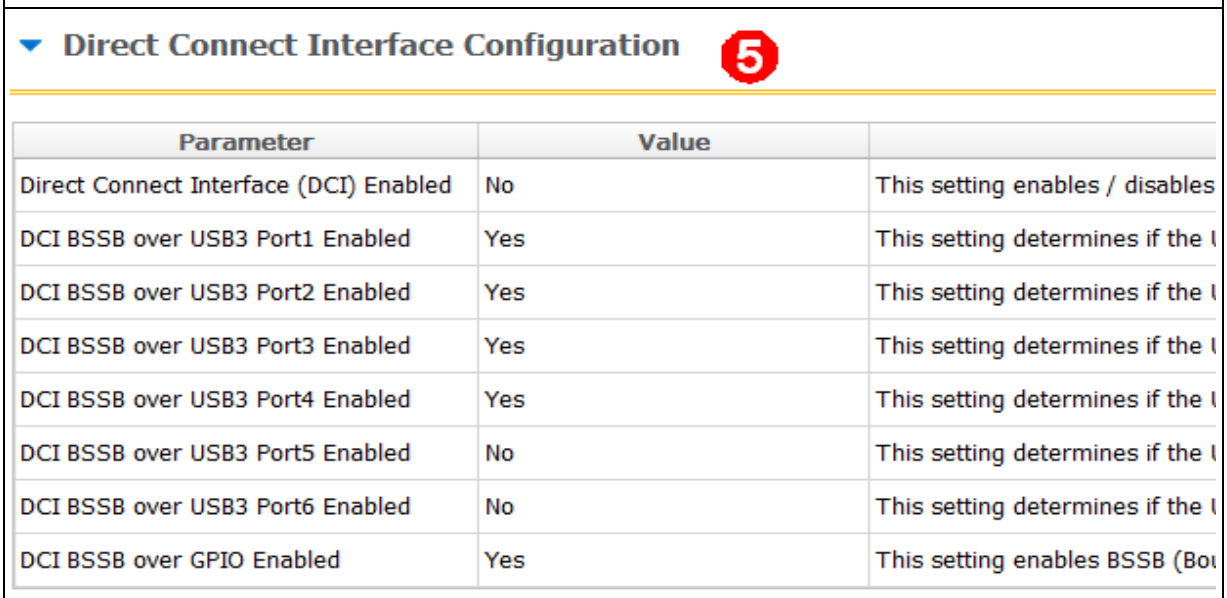


#	Parameter	Platform	Settings
4	**Intel® ME Firmware Debugging Overrides**		
	Debug Override Pre-Production Silicon - Allows the OEM to control FW features to assist with pre-production platform debugging. This control has no effect if used on production silicon. **Bit 0:** Disable DRAM_INIT_DONE (default timeout 60 seconds) **Bit 1:** Disable Host Reset Timer **Bit 2:** Disable CPU_RESET_DONE timeout **Bit 3:** Reserved **Bit 4:** Disable Intel® ME Power Gating **Bit 5:** Reserved **Bit 6:** Secure Boot debug hook. Used to shorten wait time before ENF shutdown. **Bit 7:** Force real FPFs on preproduction (default is to use flash) **Bit 8:** Secure Boot debug hook. Used to reduce S3 or FFS optimization tries. **Bit 9:** Reserved **Bit 10:** Override power package to always enter M3. **Note:** Certain options do not work when the descriptor is locked.	CML-Y CML-U	0x00000000 0x00000000
	Debug Override Production Silicon - Allows the OEM to control FW features to assist with production platform debugging. **Bit 0:** Extend DRAM_INIT_DONE timeout to 30 minutes (default timeout 15 seconds) **Bit 1:** Disable Host Reset Timer **Bit 2:** Disable CPU_RESET_DONE timeout **Note:** Certain options do not work when the descriptor is locked.	CML-Y CML-U	0x00000000 0x00000000
	Intel® ME Reset Behavior This setting determines Intel® ME behavior when boot image errors are encountered. Warning: This setting should be used for debug purposes only. ***Note:*** This may block normal Firmware functional flows.	CML-Y CML-U	Intel® ME will Halt Intel® ME will Halt

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

	Firmware ROM Bypass **Values: Yes/No** - This setting enables / disables firmware ROM bypass. **Note:** This setting only has affect when the firmware being used has ROM Bypass code present.	CML-Y CML-U	No No
	ASF Idle Flash Reclaim Enabled **Values: Yes / No** This controls enabling / disable the Intel® AFS Idle flash reclaim capabilities. ***Note:*** This setting should be used for debug purposes only.	CML-Y CML-U	Yes Yes

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



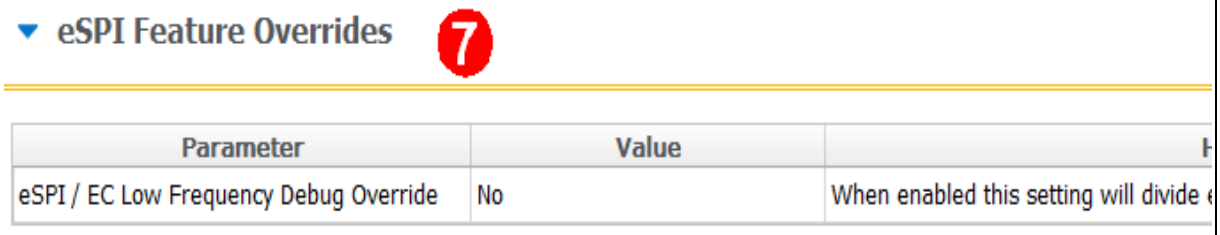
Direct Connect Interface Configuration 5

Parameter	Value	
Direct Connect Interface (DCI) Enabled	No	This setting enables / disables
DCI BSSB over USB3 Port1 Enabled	Yes	This setting determines if the U
DCI BSSB over USB3 Port2 Enabled	Yes	This setting determines if the U
DCI BSSB over USB3 Port3 Enabled	Yes	This setting determines if the U
DCI BSSB over USB3 Port4 Enabled	Yes	This setting determines if the U
DCI BSSB over USB3 Port5 Enabled	No	This setting determines if the U
DCI BSSB over USB3 Port6 Enabled	No	This setting determines if the U
DCI BSSB over GPIO Enabled	Yes	This setting enables BSSB (Bou

#	Parameter	Platform	Settings
5	**Direct Connection Interface Configuration** ***Note:*** When any of the DCI BSSB USB3 Port interfaces are enabled the associated USB3 port selection control will be greyed out under the USB3 Port Configuration settings section under the Flex I/O tab		
	Direct Connect Interface (DCI) Enabled **Values: Yes/No** - This setting enables / disables the DCI interface used for Intel® Trace Hub debugging.	CML-Y CML-U	No No
	DCI BSSB over USB3 Port 1 Enabled This setting determines if the USB port 1 has BSSB (Boundary Scan Side Band) enabled. ***Note:*** For S0ix and reset flows BSSB should be enabled. ***Note:*** When this setting is enabled the corresponding USB3 Combo Port in the Flex I/O Tab will be Grayed out.	CML-Y CML-U	Yes Yes
	DCI BSSB over USB3 Port 2 Enabled This setting determines if the USB port 2 has BSSB (Boundary Scan Side Band) enabled. ***Note:*** For S0ix and reset flows BSSB should be enabled. ***Note:*** When this setting is enabled the corresponding USB3 Combo Port in the Flex I/O Tab will be Grayed out.	CML-Y CML-U	No No

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

	DCI BSSB over USB3 Port 3 Enabled This setting determines if the USB port 3 has BSSB (Boundary Scan Side Band) enabled. ***Note:*** For S0ix and reset flows BSSB should be enabled. ***Note:*** When this setting is enabled the corresponding USB3 Combo Port in the Flex I/O Tab will be Grayed out.	CML-Y CML-U	Yes Yes
	DCI BSSB over USB3 Port 4 Enabled This setting determines if the USB port 4 has BSSB (Boundary Scan Side Band) enabled. ***Note:*** For S0ix and reset flows BSSB should be enabled. ***Note:*** When this setting is enabled the corresponding USB3 Combo Port in the Flex I/O Tab will be Grayed out.	CML-Y CML-U	Yes Yes
	DCI BSSB over USB3 Port 5 Enabled This setting determines if the USB port 5 has BSSB (Boundary Scan Side Band) enabled. ***Note:*** For S0ix and reset flows BSSB should be enabled. ***Note:*** When this setting is enabled the corresponding USB3 Combo Port in the Flex I/O Tab will be Grayed out.	CML-Y CML-U	No No
	DCI BSSB over USB3 Port 6 Enabled This setting determines if the USB port 5 has BSSB (Boundary Scan Side Band) enabled. ***Note:*** For S0ix and reset flows BSSB should be enabled. ***Note:*** When this setting is enabled the corresponding USB3 Combo Port in the Flex I/O Tab will be Grayed out.	CML-Y CML-U	No No
	DCI BSSB over GPIO Enabled This setting enables BSSB (Boundary Scan Side Band) over GPIO for DCI operations. ***Note:*** If this setting is enabled the DCI BSSB over USB3 Port1 Enabled also needs to be set to 'Yes'. ***Note:*** For S0ix and reset flows BSSB should be enabled.	CML-Y CML-U	Yes Yes
Click on Debug in the left tabs menu> eSPI Feature Overrides is expanded by default:			



#	Parameter	Platform	Settings
6	**eSPI Feature Overrides**		
	eSPI / EC Low Frequency Debug Override When enabled this setting will divide eSPI clock frequency by 8. ***Note:*** This setting should only be used for debugging purposes. Leaving this setting enable will impact eSPI performance.	CML-Y CML-U	No No
Click on Debug in the left tabs menu> Early USB DBC Type-A Configuration is expanded by default:			

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

Early USB DBC over Type-A Configuration 7

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

#	Parameter	Platform	Settings
7	**Early USB DBC Type-A Configuration**		
	Intel® ME Boot Stall Enabled This setting enables a delay during Intel® ME FW bring-up to allow USB DCI to be established and Early DbC arbitration to be granted.	CML-Y CML-U	No Boot Stall No Boot Stall
	USB2 DbC port enable This setting determines which USB2 ports are enabled for Early DbC debugging.	CML-Y CML-U	No USB2 Ports No USB2 Ports
	USB3 DbC port enable This setting determines which USB3 ports are enabled for Early DbC debugging.	CML-Y CML-U	No USB3 Ports No USB3 Ports

Table 2-15. - 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 thre
Number of Active Cores	All Cores Active	This setting controls the number of active processor
BIST Initialization	No	This setting determines if BIST will be run at platforn
Flex Ratio	0x0	This setting controls the maximum processor non-tur
Processor Boot Max Frequency	Yes	This setting determines if the processor will operate
JTAG Power Disable	No JTAG Power on C10 and Lo...	This setting determines if JTAG power will be mainta
SA VR Type	SVID	This setting determines the SA core domain VR type.
IA Power Plane VR	SVID	This setting determines the IA core domain VR type.
Ring VR Type	SVID	This setting determines the Ring domain VR type. Se
GT_US VR Type	SVID	This setting determines the GT Unslice domain VR typ
SVID Presence	SVID is present	This setting determine if SVID rails are present on th
Platform IMON	Enabled	This strap should be left at the recommended default
GT_S VR Type	SVID	This setting determines the GT slice domain VR type.
Six Core CPU Configuration	Not Six Core	This setting determines if the board supports six core
IA VR Offset VID	Above 1.52v Not Allowed	This setting determines if output higher than 1.52v is
GT_S SVID Address	0x1	This setting determines the GT slice SVID Address. S
GT_US SVID Address	0x1	This setting determines the GT Unslice SVID Address
Ring SVID Address	0x0	This setting determines the Ring SVID address. See F
IA SVID Address	0x0	This setting determines the IA SVID address. See Pro
SA SVID Address	0x2	This setting determines the SA SVID address. See Pr

#	Parameter	Platform	Settings
1	**CPU Straps**		

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

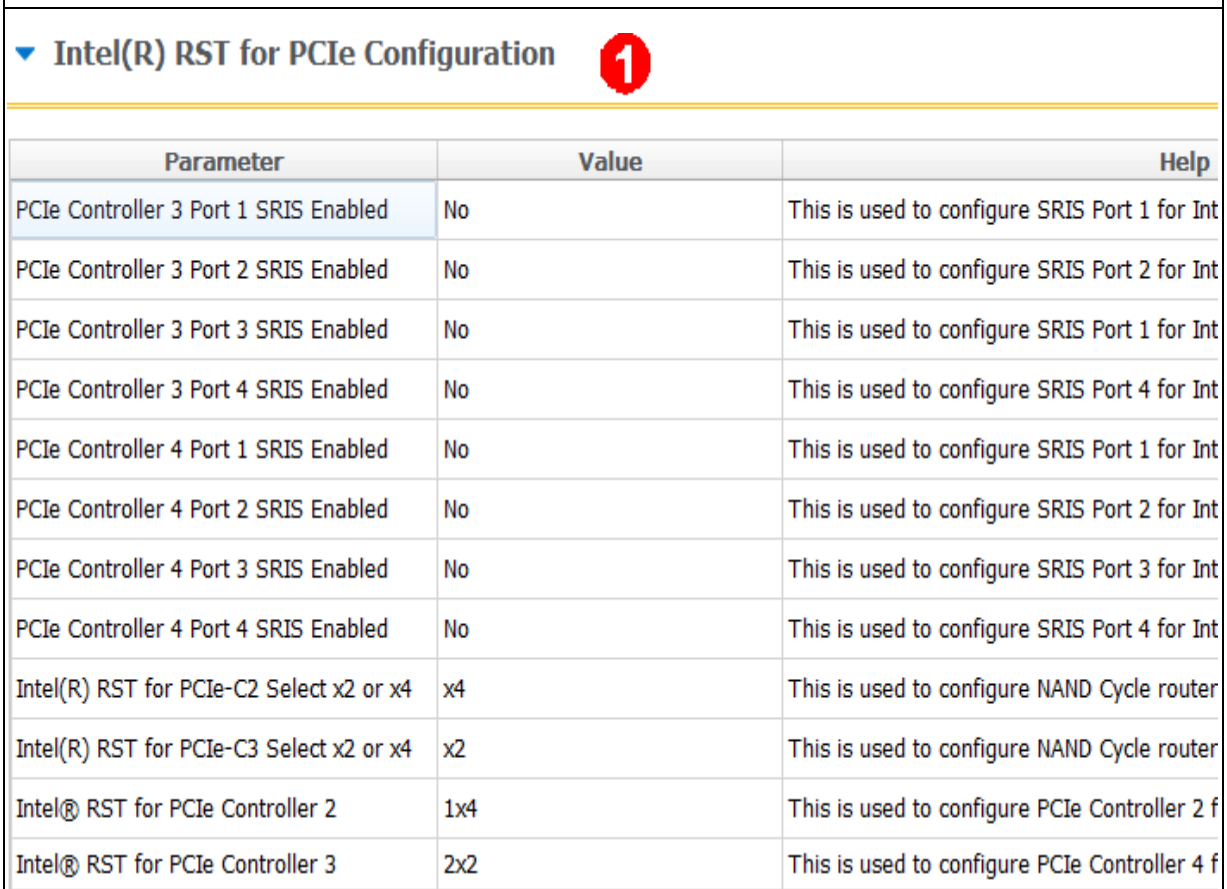
	Disable Hyperthreading **Values: Yes/No** This setting controls enabling or disabling of Hyper threading. **Note:** This strap is intended for debugging purposes only. See BIOS Spec for more details on enabling / disabling Hyper-threading.	CML-Y CML-U	No No
	Number of Active Cores **Values: All, 1, 2, 3, 4, 5, 6** 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.	CML-Y CML-U	All All
	BIST Initialization **Values: Yes/No** This setting determines if BIST will be run at platform reset after BIOS requested actions. **Note:** This strap is intended for debugging purposes only.	CML-Y CML-U	No No
	Flex Ratio This setting controls the maximum processor non-turbo ratio. **Note:** This strap is intended for debugging purposes only. See BIOS Spec for more details on maximum processor non-turbo ratio configuration.	CML-Y CML-U	0x0 0x0
	Processor Boot Max Frequency **Values: Yes/No** This setting determines if the processor will operate at maximum frequency at power-on and boot. **Note:** This strap is intended for debugging purposes only.	CML-Y CML-U	Yes Yes
	JTAG Power Disable **Values: Yes - JTAG Power on C10 and Lower/No - No Power on C10 and Lower** This setting determines if JTAG power will be maintained on C10 or lower power states. **Note:** This strap is intended for debugging purposes only.	CML-Y CML-U	No No
	SA VR Type **Value: SVID/Fixed VR** This setting determines the SA core domain VR type. See Processor EDS for details.	CML-Y CML-U	SVID SVID
	IA Power Plane VR **Value: SVID/Fixed VR** This setting determines the IA core domain VR type. See Processor EDS for details.	CML-Y CML-U	SVID SVID
	Ring VR Type **Value: SVID/Fixed VR** This setting determines the Ring domain VR type. See Processor EDS for details.	CML-Y CML-U	SVID SVID
	GT_US VR Type **Value: SVID/Fixed VR** This setting determines the GT Unslice domain VR type. See Processor EDS for details.	CML-Y CML-U	SVID SVID
	SVID Presence **Value: SVID Present/SVID Not Present** This setting determines if SVID rails are present on the platform. See Processor EDS for details.	CML-Y CML-U	SVID Present SVID Present
	Platform IMON This strap should be left at the recommended default setting.	CML-Y CML-U	Enabled Enabled
	GT_S VR Type **Value: SVID/Fixed VR** This setting determines the GT slice domain VR type. See Processor EDS for details.	CML-Y CML-U	SVID SVID
	Six Core CPU Configuration **Value: Not Six Core/Six Core** This setting determines if the board supports six core processor configuration.	CML-Y CML-U	Not Six Core Not Six Core
	IA VR Offset VID **Value: Above 1.52v Not Allowed/Above 1.52v Allowed** This setting determines if output voltage higher than 1.52v is allowed for 8 or higher core count processors.	CML-Y CML-U	Above 1.52v Not Allowed Above 1.52v Not Allowed

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

	GT_S SVID Address This setting determines the GT slice SVID Address. See Processor EDS for details. **Note:** This strap should be left at the recommended default setting.	CML-Y CML-U	0x8 0x1
	GT_US SVID Address This setting determines the GT Unslice SVID Address. See Processor EDS for details. **Note:** This strap should be left at the recommended default setting. **FOR CML-U 23e GT3 Only** - if using GT merged power plane the value should be 0x1.	CML-Y CML-U	0x8 0x1
	Ring SVID Address This setting determines the Ring SVID Address. See Processor EDS for details. **Note:** This strap should be left at the recommended default setting.	CML-Y CML-U	0x6 0x0
	IA Power Plane Topology This setting determines the IA SVID Address. See Processor EDS for details. **Note:** This strap should be left at the recommended default setting.	CML-Y CML-U	0x6 0x0
	SA SVID Address This setting determines the SA SVID Address. See Processor EDS for details. **Note:** This strap should be left at the recommended default setting.	CML-Y CML-U	0x2 0x2

Table 2-16. - Flex I/O Straps (Sheet 1 of 9)

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



Intel(R) RST for PCIe Configuration

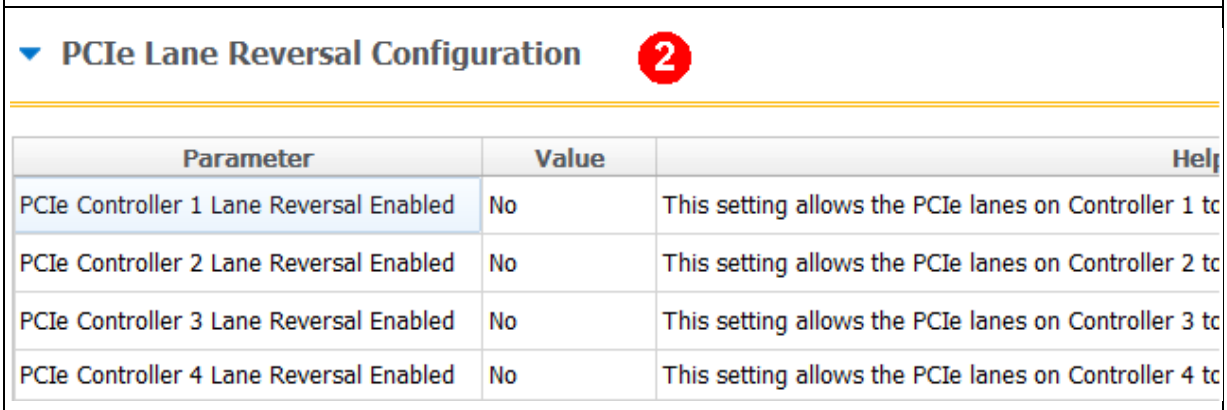
Parameter	Value	Help
PCIe Controller 3 Port 1 SRIS Enabled	No	This is used to configure SRIS Port 1 for Int
PCIe Controller 3 Port 2 SRIS Enabled	No	This is used to configure SRIS Port 2 for Int
PCIe Controller 3 Port 3 SRIS Enabled	No	This is used to configure SRIS Port 1 for Int
PCIe Controller 3 Port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

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

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

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

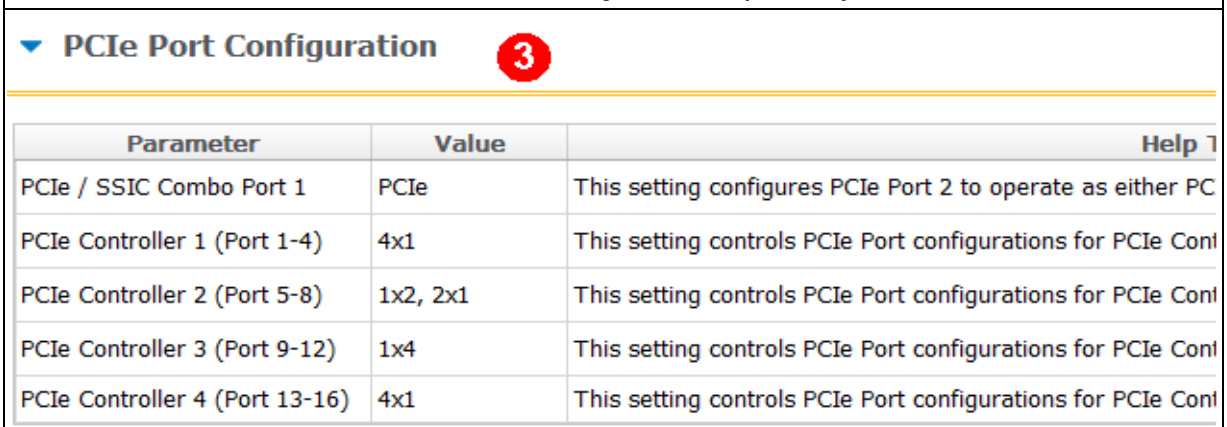
Click on Flex I/O in the left tabs menu> PCIe Lane Reversal Configuration is expanded by default:



#	Parameter	Platform	Settings
2	**PCIe Lane Reversal Configuration**		

Table 2-16. - Flex I/O Straps (Sheet 3 of 9)

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



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

Table 2-16. - Flex I/O Straps (Sheet 4 of 9)

SATA / PCIe Combo Port Configuration 4

Parameter	Value	Help Te
SATA / PCIe Combo Port 0 Mode Select	PCIe CLKREQ#	The corresponding CLKREQ# GPIO can only function a
SATA / PCIe Combo Port 1 Mode Select	PCIe CLKREQ#	The corresponding CLKREQ# GPIO can only function a
SATA / PCIe Combo Port 2 Mode Select	PCIe CLKREQ#	The corresponding CLKREQ# GPIO can only function a
SATA / PCIe Combo Port 0	PCIe (or GbE)	This setting configures the PCIe port to operate as eit
SATA / PCIe Combo Port 1	GPIO Polarity Control	This setting configures the PCIe port to operate as eit
SATA / PCIe Combo Port 2	PCIe (or GbE)	This setting configures the PCIe port to operate as eit
SATA / PCIe Combo Port 3	SATA	This setting configures the PCIe port to operate as eit

#	Parameter	Platform	Settings
4	**SATA / PCIe Combo Port Configuration**		
	SATA / PCIe Combo Port 0 Mode Select 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	CML-Y CML-U	PCIe CLKREQ# PCIe CLKREQ#
	SATA / PCIe Combo Port 1 Mode Select The corresponding CLKREQ# GPIO can only function as DEVSLP# if SATA / PCIe Combo Port 1 or Combo Port 2 is assigned to SATA, and SATA / PCIe Combo Port 1 or Combo Port 2 Mode Select is configured to SATA	CML-Y CML-U	PCIe CLKREQ# PCIe CLKREQ#
	SATA / PCIe Combo Port 2 Mode Select The corresponding CLKREQ# GPIO can only function as DEVSLP# if SATA / PCIe Combo Port 2 is assigned to SATA, and SATA / PCIe Combo Port 2 Mode Select is configured to SATA ***Note:*** Applicable to Premium U SKUs only	CML-Y CML-U	PCIe CLKREQ# PCIe CLKREQ#
	SATA / PCIe Combo Port 0 **Values: SATA, PCIe, GPIO Polarity PCIe, GPIO Polarity SATA** - This setting configures the PCIe port to operate as either: PCIe Port 11 or SATA Port 0 For further details on Flex I/O see Comet Lake LP Platform Controller Hub EDS.	CML-Y CML-U	GPIO Polarity PCIe PCIe
	SATA / PCIe Combo Port 1 **Values: SATA, PCIe, GPIO Polarity PCIe, GPIO Polarity SATA** - This setting configures the PCIe port to operate as either: PCIe Port 12 or SATA Port 1 For further details on Flex I/O see Comet Lake LP Platform Controller Hub EDS.	CML-Y CML-U	GPIO Polarity PCIe GPIO Polarity PCIe
	SATA / PCIe Combo Port 2 **Values: SATA, PCIe, GPIO Polarity PCIe, GPIO Polarity SATA** - This setting configures the PCIe port to operate as either: PCIe Port 15 or SATA Port 1 For further details on Flex I/O see Comet Lake LP Platform Controller Hub EDS. ***Note:*** Applicable to Premium U SKUs only	CML-Y CML-U	NA PCIe

Table 2-16. - Flex I/O Straps (Sheet 5 of 9)

	SATA / PCIe Combo Port 3 **Values: SATA, PCIe, GPIO Polarity PCIe, GPIO Polarity SATA -** This setting configures the PCIe port to operate as either: PCIe Port 16 or SATA Port 2 For further details on Flex I/O see Comet Lake LP Platform Controller Hub EDS. ***Note:*** Applicable to Premium U SKUs only	CML-Y CML-U	NA SATA
Click on Flex I/O in the left tabs menu> USB3 Port Configuration is expanded by default:			

Table 2-16. - Flex I/O Straps (Sheet 6 of 9)

USB3 Port Configuration 6

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

Table 2-16. - Flex I/O Straps (Sheet 7 of 9)

#	Parameter	Platform	Settings
6	**USB3 Port Configuration** ***Note:*** USB Type-C Mux Control: On Comet 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 Coffee Lake Platform USB Type-C Mux Control Over eSPI doc # 570737.		
	USB3 / PCIe Combo Port 0 **Values: PCIe, USB3 -** This setting configures the PCIe port to operate as either: PCIe Port 1 or USB3 Port 1 For further details on Flex I/O see Comet Lake LP Platform Controller Hub EDS. ***Note:*** If DCI BSSB for this USB3 Combo port it will be Grayed out.	CML-Y CML-U	USB3 USB3
	USB3 / PCIe Combo Port 1 **Values: PCIe, USB3 -** This setting configures the PCIe port to operate as either: PCIe Port 2 or USB3 Port 2 For further details on Flex I/O see Comet Lake LP Platform Controller Hub EDS. ***Note:*** If DCI BSSB for this USB3 Combo port it will be Grayed out.	CML-Y CML-U	PCIe PCIe
	USB3 / PCIe Combo Port 2 **Values: PCIe, USB3** - This setting configures the PCIe port to operate as either: PCIe Port 3 or USB3 Port 3 For further details on Flex I/O see Comet Lake LP Platform Controller Hub EDS. ***Note:*** If DCI BSSB for this USB3 Combo port it will be Grayed out.	CML-Y CML-U	USB3 USB3
	USB3 / PCIe Combo Port 3 **Values: PCIe, USB3** - This setting configures the PCIe port to operate as either: PCIe 4 or USB3 Port 4 For further details on Flex I/O see Comet Lake LP Platform Controller Hub EDS. ***Note:*** If DCI BSSB for this USB3 Combo port it will be Grayed out.	CML-Y CML-U	USB3 USB3
	USB3 / PCIe Combo Port 4 **Values: PCIe, USB3** - This setting configures the PCIe port to operate as either: PCIe Port 5 or USB3 Port 5 For further details on Flex I/O see Comet Lake LP Platform Controller Hub EDS. ***Note:*** If DCI BSSB for this USB3 Combo port it will be Grayed out.	CML-Y CML-U	PCIe PCIe
	USB3 / PCIe Combo Port 5 **Values: PCIe, USB3** - This setting configures the PCIe port to operate as either: PCIe Port 6 or USB3 Port 6 For further details on Flex I/O see Comet Lake LP Platform Controller Hub EDS. ***Note:*** If DCI BSSB for this USB3 Combo port it will be Grayed out.	CML-Y CML-U	PCIe PCIe
	USB3 Port 1 Connector Type Select This setting configures the physical connector type to be used for USB 3.0 / 3.1 Port 1.	CML-Y CML-U	Type-C Type-C
	USB3 Port 2 Connector Type Select This setting configures the physical connector type to be used for USB 3.0 / 3.1 Port 2.	CML-Y CML-U	Type-C Type-C
	USB3 Port 3 Connector Type Select This setting configures the physical connector type to be used for USB 3.0 / 3.1 Port 3.	CML-Y CML-U	Type-A Type-C

Table 2-16. - Flex I/O Straps (Sheet 8 of 9)

	USB3 Port 4 Connector Type Select This setting configures the physical connector type to be used for USB 3.0 / 3.1 Port 4.	CML-Y CML-U	Type-A Type-A
	USB3 Port 5 Connector Type Select This setting configures the physical connector type to be used for USB 3.0 / 3.1 Port 5.	CML-Y CML-U	Type-C Type-C
	USB3 Port 6 Connector Type Select This setting configures the physical connector type to be used for USB 3.0 / 3.1 Port 6.	CML-Y CML-U	Type-C Type-C
	USB3 Port 1 Initialization Speed Select This setting determines USB3 Port 1 speed during platform power-up.	CML-Y CML-U	USB3.1 Gen1 LBPM USB3.1 Gen1 LBPM
	USB3 Port 2 Initialization Speed Select This setting determines USB3 Port 2 speed during platform power-up.	CML-Y CML-U	USB3.1 Gen1 LBPM USB3.1 Gen1 LBPM
	USB3 Port 3 Initialization Speed Select This setting determines USB3 Port 3 speed during platform power-up.	CML-Y CML-U	USB3.1 Gen1 LBPM USB3.1 Gen1 LBPM
	USB3 Port 4 Initialization Speed Select This setting determines USB3 Port 4 speed during platform power-up.	CML-Y CML-U	USB3.1 Gen1 LBPM USB3.1 Gen1 LBPM
	USB3 Port 5 Initialization Speed Select This setting determines USB3 Port 5 speed during platform power-up.	CML-Y CML-U	USB3.1 Gen1 LBPM USB3.1 Gen1 LBPM
	USB3 Port 6 Initialization Speed Select This setting determines USB3 Port 6 speed during platform power-up.	CML-Y CML-U	USB3.1 Gen1 LBPM USB3.1 Gen1 LBPM
	USB3 Port 1 Speed Capability This setting determines the USB3 Port 1 speed capabilities.	CML-Y CML-U	USB 3.1 Gen2 USB 3.1 Gen2
	USB3 Port 2 Speed Capability This setting determines the USB3 Port 2 speed capabilities.	CML-Y CML-U	USB 3.1 Gen2 USB 3.1 Gen2
	USB3 Port 3 Speed Capability This setting determines the USB3 Port 3 speed capabilities.	CML-Y CML-U	USB 3.1 Gen2 USB 3.1 Gen2
	USB3 Port 4 Speed Capability This setting determines the USB3 Port 4 speed capabilities.	CML-Y CML-U	USB 3.1 Gen2 USB 3.1 Gen2
	USB3 Port 5 Speed Capability This setting determines the USB3 Port 5 speed capabilities.	CML-Y CML-U	USB 3.1 Gen2 USB 3.1 Gen2
	USB3 Port 6 Speed Capability This setting determines the USB3 Port 6 speed capabilities.	CML-Y CML-U	USB 3.1 Gen2 USB 3.1 Gen2
	USB Type AB Mode Select This setting determines how the USB Type AB connector switching is handled.	CML-Y CML-U	USB Type AB SW Select USB Type AB SW Select
Click on Flex I/O in the left tabs menu> USB2 Port Configuration is expanded by default:			

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

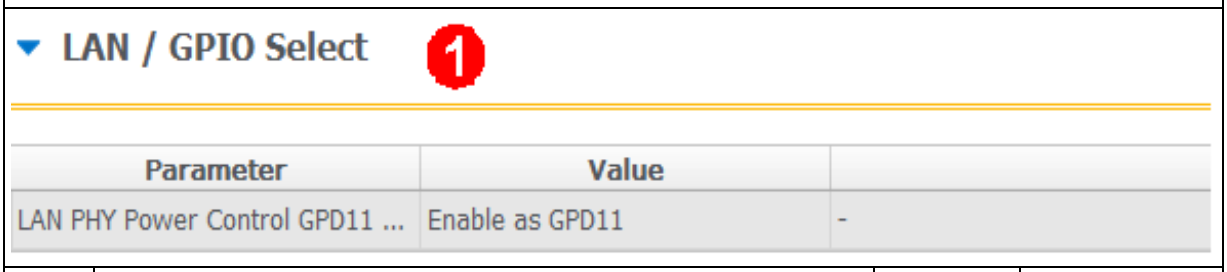
USB2 Port Configuration 7

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

#	Parameter	Platform	Settings
7	**USB2 Port Configuration**		
	USB2 Port 1 Connector Type This setting configures the physical connector type to be used for USB2 Port 1.	CML-Y CML-U	Type-C Type-C
	USB2 Port 2 Connector Type This setting configures the physical connector type to be used for USB2 Port 2.	CML-Y CML-U	Express Card / M.2 S2 Type-C
	USB2 Port 3 Connector Type This setting configures the physical connector type to be used for USB2 Port 3.	CML-Y CML-U	Type-C Type-A
	USB2 Port 4 Connector Type This setting configures the physical connector type to be used for USB2 Port 4.	CML-Y CML-U	Type-A Type-A
	USB2 Port 5 Connector Type This setting configures the physical connector type to be used for USB2 Port 5.	CML-Y CML-U	Express Card / M.2 S2 Type-A
	USB2 Port 6 Connector Type This setting configures the physical connector type to be used for USB2 Port 6.	CML-Y CML-U	Type-A Type-A
	USB2 Port 7 Connector Type This setting configures the physical connector type to be used for USB2 Port 7.	CML-Y CML-U	Type-A Type-A
	USB2 Port 8 Connector Type This setting configures the physical connector type to be used for USB2 Port 8.	CML-Y CML-U	Type-A Type-A
	USB2 Port 9 Connector Type This setting configures the physical connector type to be used for USB2 Port 9.	CML-Y CML-U	Type-A Type-A
	USB2 Port 10 Connector Type This setting configures the physical connector type to be used for USB2 Port 10.	CML-Y CML-U	Express Card / M.2 S2 Type-A

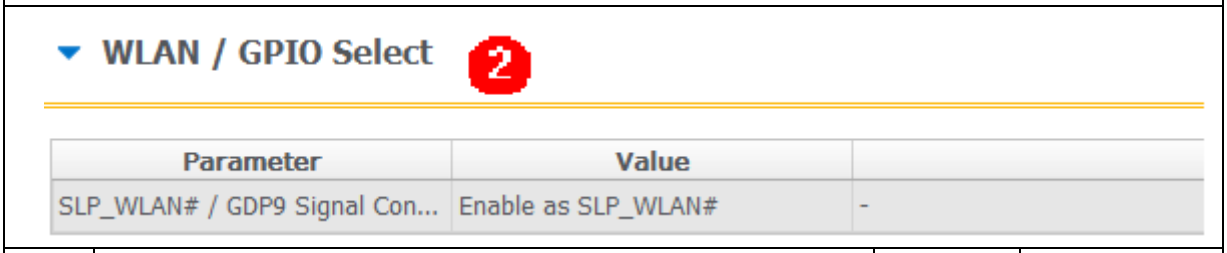
Table 2-17. - GPIO (Sheet 1 of 15)

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



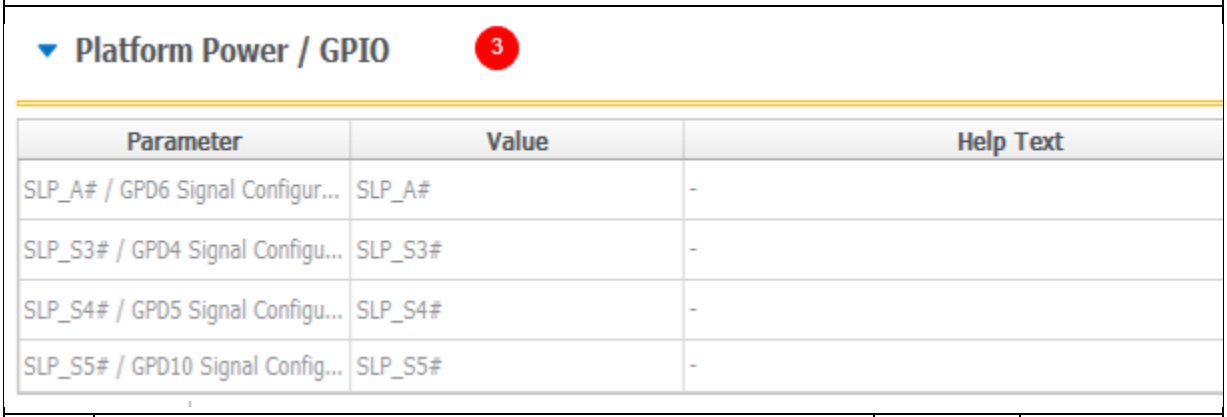
#	Parameter	Platform	Settings
1	**LAN / GPIO Select**		
	LAN PHY Power Control GPD11 Signal Configuration	CML-Y CML-U	LANPHYPC LANPHYPC

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



#	Parameter	Platform	Settings
2	**WLAN / GPIO Select**		
	SLP_WLAN# / GPD9 Signal Configuration	CML-Y CML-U	SLP_WLAN# SLP_WLAN#

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

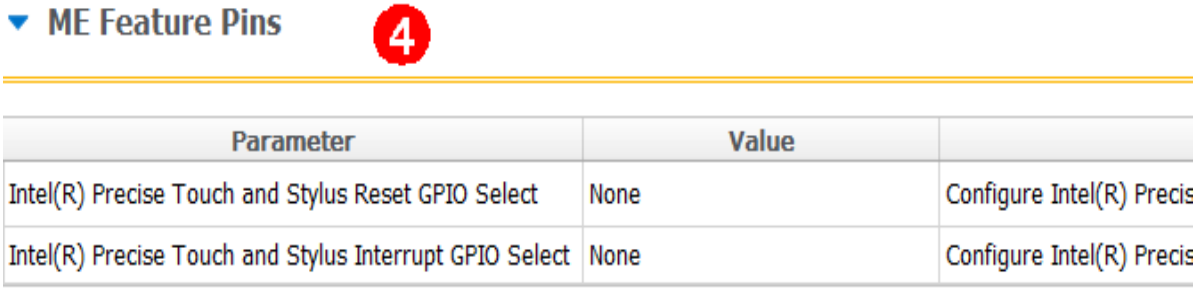


#	Parameter	Platform	Settings

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

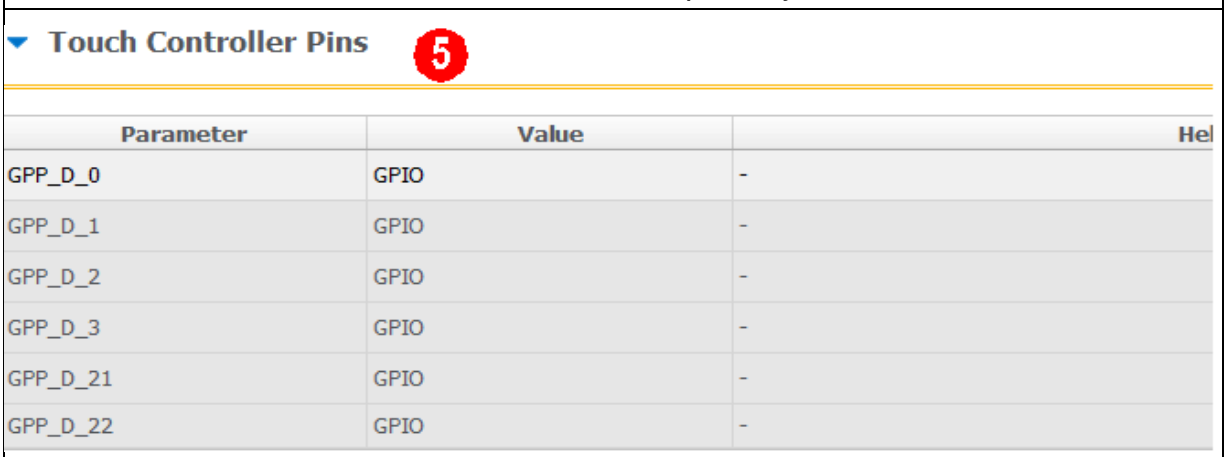
3	**Platform Power / GPIO**		
	SLP_A# / GPD6 Signal Configuration	CML-Y CML-U	SLP_A# SLP_A#
	SLP_S3# / GPD4 Signal Configuration	CML-Y CML-U	SLP_S3# SLP_S3#
	SLP_S4# / GPD5 Signal Configuration	CML-Y CML-U	SLP_S4# SLP_S4#
	SLP_S5# / GPD10 Signal Configuration	CML-Y CML-U	SLP_S5# SLP_S5#

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



#	Parameter	Platform	Settings
4	**ME Feature Pins**		
	Intel® Precise Touch and Stylus Reset GPIO Select Configure Intel® Precise Touch and Stylus Reset GPIO.	CML-Y CML-U	None None
	Intel® Precise Touch and Stylus Interrupt GPIO Select Configure Intel® Precise Touch and Stylus Interrupt GPIO.	CML-Y CML-U	None None

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

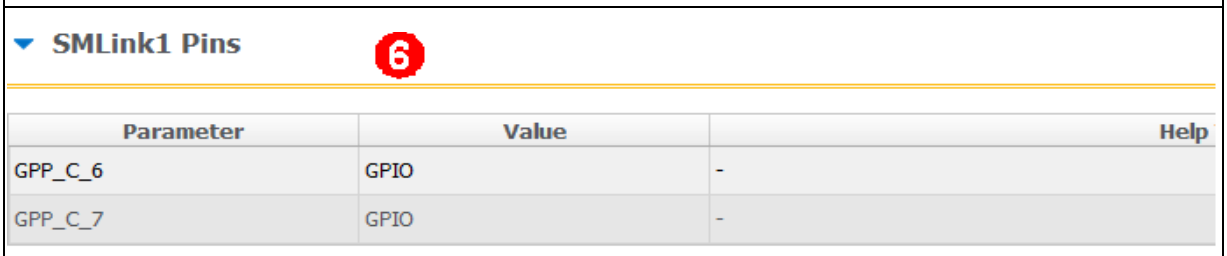


#	Parameter	Platform	Settings

Table 2-17. - GPIO (Sheet 3 of 15)

5	**Touch Controller Pins**		
	GPP_D_0	CML-Y CML-U	GPIO GPIO
	GPP_D_1	CML-Y CML-U	GPIO GPIO
	GPP_D_2	CML-Y CML-U	GPIO GPIO
	GPP_D_3	CML-Y CML-U	GPIO GPIO
	GPP_D_21	CML-Y CML-U	GPIO GPIO
	GPP_D_22	CML-Y CML-U	GPIO GPIO

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



#	Parameter	Platform	Settings
6	**SMLink1 Pins**		
	GPP_C_6	CML-Y CML-U	GPIO GPIO
	GPP_C_7	CML-Y CML-U	GPIO GPIO

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

Table 2-17. - GPIO (Sheet 4 of 15)

GPIO VCCIO Voltage Control 7

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

#	Parameter	Platform	Settings
7	**GPIO - GPIO VCCIO Voltage Control** ***Warning:*** Incorrectly configuring GPIO voltages may result in MCP damage.		
	GPP_A Group Master Voltage Select	CML-Y CML-U	3.3 Volts 3.3 Volts
	GPP_A0 Individual Voltage Select	CML-Y CML-U	3.3 Volts 3.3 Volts
	GPP_A1 Individual Voltage Select	CML-Y CML-U	1.8 Volts 1.8 Volts
	GPP_A2 Individual Voltage Select	CML-Y CML-U	1.8 Volts 1.8 Volts
	GPP_A3 Individual Voltage Select	CML-Y CML-U	1.8 Volts 1.8 Volts

Table 2-17. - GPIO (Sheet 5 of 15)

	GPP_A4 Individual Voltage Select	CML-Y CML-U	1.8 Volts 1.8 Volts
	GPP_A5 Individual Voltage Select	CML-Y CML-U	1.8 Volts 1.8 Volts
	GPP_A6 Individual Voltage Select	CML-Y CML-U	1.8 Volts 1.8 Volts
	GPP_A7 Individual Voltage Select	CML-Y CML-U	1.8 Volts 3.3 Volts
	GPP_A8 Individual Voltage Select	CML-Y CML-U	1.8 Volts 3.3 Volts
	GPP_A9 Individual Voltage Select	CML-Y CML-U	1.8 Volts 1.8 Volts
	GPP_A10 Individual Voltage Select	CML-Y CML-U	3.3 Volts 3.3 Volts
	GPP_A11 Individual Voltage Select	CML-Y CML-U	1.8 Volts 3.3 Volts
	GPP_A12 Individual Voltage Select	CML-Y CML-U	1.8 Volts 1.8 Volts
	GPP_A13 Individual Voltage Select	CML-Y CML-U	3.3 Volts 3.3 Volts
	GPP_A14 Individual Voltage Select	CML-Y CML-U	1.8 Volts 1.8 Volts
	GPP_A15 Individual Voltage Select	CML-Y CML-U	3.3 Volts 3.3 Volts
	GPP_A16 Individual Voltage Select	CML-Y CML-U	1.8 Volts 3.3 Volts
	GPP_A17 Individual Voltage Select	CML-Y CML-U	3.3 Volts 3.3 Volts
	GPP_A18 Individual Voltage Select	CML-Y CML-U	1.8 Volts 1.8 Volts
	GPP_A19 Individual Voltage Select	CML-Y CML-U	1.8 Volts 1.8 Volts
	GPP_A20 Individual Voltage Select	CML-Y CML-U	1.8 Volts 1.8 Volts
	GPP_A21 Individual Voltage Select	CML-Y CML-U	1.8 Volts 3.3 Volts
	GPP_A22 Individual Voltage Select	CML-Y CML-U	1.8 Volts 1.8 Volts
	GPP_A23 Individual Voltage Select	CML-Y CML-U	1.8 Volts 1.8 Volts

Table 2-17. - GPIO (Sheet 6 of 15)

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

#	Parameter	Platform	Settings
	GPP_B0 Individual Voltage Select	CML-Y CML-U	3.3 Volts 3.3 Volts
	GPP_B1 Individual Voltage Select	CML-Y CML-U	3.3 Volts 3.3 Volts
	GPP_B2 Individual Voltage Select	CML-Y CML-U	3.3 Volts 3.3 Volts
	GPP_B3 Individual Voltage Select	CML-Y CML-U	1.8 Volts 1.8 Volts
	GPP_B4 Individual Voltage Select	CML-Y CML-U	3.3 Volts 3.3 Volts
	GPP_B5 Individual Voltage Select	CML-Y CML-U	3.3 Volts 3.3 Volts
	GPP_B6 Individual Voltage Select	CML-Y CML-U	3.3 Volts 3.3 Volts
	GPP_B7 Individual Voltage Select	CML-Y CML-U	3.3 Volts 3.3 Volts
	GPP_B8 Individual Voltage Select	CML-Y CML-U	3.3 Volts 3.3 Volts
	GPP_B9 Individual Voltage Select	CML-Y CML-U	3.3 Volts 3.3 Volts
	GPP_B10 Individual Voltage Select	CML-Y CML-U	3.3 Volts 3.3 Volts

Table 2-17. - GPIO (Sheet 7 of 15)

	GPP_B11 Individual Voltage Select	CML-Y CML-U	3.3 Volts 3.3 Volts
	GPP_B12 Individual Voltage Select	CML-Y CML-U	3.3 Volts 3.3 Volts
	GPP_B13 Individual Voltage Select	CML-Y CML-U	3.3 Volts 3.3 Volts
	GPP_B14 Individual Voltage Select	CML-Y CML-U	3.3 Volts 3.3 Volts
	GPP_B15 Individual Voltage Select	CML-Y CML-U	3.3 Volts 3.3 Volts
	GPP_B16 Individual Voltage Select	CML-Y CML-U	1.8 Volts 1.8 Volts
	GPP_B17 Individual Voltage Select	CML-Y CML-U	1.8 Volts 1.8 Volts
	GPP_B18 Individual Voltage Select	CML-Y CML-U	3.3 Volts 3.3 Volts
	GPP_B19 Individual Voltage Select	CML-Y CML-U	1.8 Volts 1.8 Volts
	GPP_B20 Individual Voltage Select	CML-Y CML-U	1.8 Volts 1.8 Volts
	GPP_B21 Individual Voltage Select	CML-Y CML-U	1.8 Volts 1.8 Volts
	GPP_B22 Individual Voltage Select	CML-Y CML-U	1.8 Volts 1.8 Volts
	GPP_B23 Individual Voltage Select	CML-Y CML-U	3.3 Volts 3.3 Volts

Table 2-17. - GPIO (Sheet 8 of 15)

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

#	Parameter	Platform	Settings
	GPP_C0 Individual Voltage Select	CML-Y CML-U	3.3 Volts 3.3 Volts
	GPP_C1 Individual Voltage Select	CML-Y CML-U	3.3 Volts 3.3 Volts
	GPP_C2 Individual Voltage Select	CML-Y CML-U	3.3 Volts 3.3 Volts
	GPP_C3 Individual Voltage Select	CML-Y CML-U	3.3 Volts 3.3 Volts
	GPP_C4 Individual Voltage Select	CML-Y CML-U	3.3 Volts 3.3 Volts
	GPP_C5 Individual Voltage Select	CML-Y CML-U	3.3 Volts 3.3 Volts
	GPP_C6 Individual Voltage Select	CML-Y CML-U	3.3 Volts 3.3 Volts
	GPP_C7 Individual Voltage Select	CML-Y CML-U	3.3 Volts 3.3 Volts
	GPP_C8 Individual Voltage Select	CML-Y CML-U	1.8 Volts 1.8 Volts
	GPP_C9 Individual Voltage Select	CML-Y CML-U	3.3 Volts 3.3 Volts

Table 2-17. - GPIO (Sheet 9 of 15)

	GPP_C10 Individual Voltage Select	CML-Y CML-U	3.3 Volts 3.3 Volts
	GPP_C11 Individual Voltage Select	CML-Y CML-U	1.8 Volts 1.8 Volts
	GPP_C12 Individual Voltage Select	CML-Y CML-U	3.3 Volts 3.3 Volts
	GPP_C13 Individual Voltage Select	CML-Y CML-U	3.3 Volts 3.3 Volts
	GPP_C14 Individual Voltage Select	CML-Y CML-U	3.3 Volts 3.3 Volts
	GPP_C15 Individual Voltage Select	CML-Y CML-U	3.3 Volts 3.3 Volts
	GPP_C16 Individual Voltage Select	CML-Y CML-U	1.8 Volts 1.8 Volts
	GPP_C17 Individual Voltage Select	CML-Y CML-U	1.8 Volts 1.8 Volts
	GPP_C18 Individual Voltage Select	CML-Y CML-U	1.8 Volts 1.8 Volts
	GPP_C19 Individual Voltage Select	CML-Y CML-U	1.8 Volts 1.8 Volts
	GPP_C20 Individual Voltage Select	CML-Y CML-U	3.3 Volts 3.3 Volts
	GPP_C21 Individual Voltage Select	CML-Y CML-U	3.3 Volts 3.3 Volts
	GPP_C22 Individual Voltage Select	CML-Y CML-U	3.3 Volts 3.3 Volts
	GPP_C23 Individual Voltage Select	CML-Y CML-U	3.3 Volts 3.3 Volts

Table 2-17. - GPIO (Sheet 10 of 15)

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

#	Parameter	Platform	Settings
	GPP_D0 Individual Voltage Select	CML-Y CML-U	1.8 Volts 1.8 Volts
	GPP_D1 Individual Voltage Select	CML-Y CML-U	1.8 Volts 1.8 Volts
	GPP_D2 Individual Voltage Select	CML-Y CML-U	1.8 Volts 1.8 Volts
	GPP_D3 Individual Voltage Select	CML-Y CML-U	1.8 Volts 1.8 Volts
	GPP_D4 Individual Voltage Select	CML-Y CML-U	3.3 Volts 3.3 Volts
	GPP_D5 Individual Voltage Select	CML-Y CML-U	1.8 Volts 1.8 Volts
	GPP_D6 Individual Voltage Select	CML-Y CML-U	1.8 Volts 1.8 Volts
	GPP_D7 Individual Voltage Select	CML-Y CML-U	1.8 Volts 1.8 Volts
	GPP_D8 Individual Voltage Select	CML-Y CML-U	1.8 Volts 1.8 Volts
	GPP_D9 Individual Voltage Select	CML-Y CML-U	1.8 Volts 3.3 Volts

Table 2-17. - GPIO (Sheet 11 of 15)

	GPP_D10 Individual Voltage Select	CML-Y CML-U	1.8 Volts 1.8 Volts
	GPP_D11 Individual Voltage Select	CML-Y CML-U	3.3 Volts 3.3 Volts
	GPP_D12 Individual Voltage Select	CML-Y CML-U	3.3 Volts 3.3 Volts
	GPP_D13 Individual Voltage Select	CML-Y CML-U	3.3 Volts 3.3 Volts
	GPP_D14 Individual Voltage Select	CML-Y CML-U	1.8 Volts 1.8 Volts
	GPP_D15 Individual Voltage Select	CML-Y CML-U	3.3 Volts 3.3 Volts
	GPP_D16 Individual Voltage Select	CML-Y CML-U	3.3 Volts 3.3 Volts
	GPP_D17 Individual Voltage Select	CML-Y CML-U	1.8 Volts 1.8 Volts
	GPP_D18 Individual Voltage Select	CML-Y CML-U	1.8 Volts 1.8 Volts
	GPP_D19 Individual Voltage Select	CML-Y CML-U	1.8 Volts 1.8 Volts
	GPP_D20 Individual Voltage Select	CML-Y CML-U	1.8 Volts 1.8 Volts
	GPP_D21 Individual Voltage Select	CML-Y CML-U	1.8 Volts 1.8 Volts
	GPP_D22 Individual Voltage Select	CML-Y CML-U	1.8 Volts 1.8 Volts
	GPP_D23 Individual Voltage Select	CML-Y CML-U	1.8 Volts 1.8 Volts

Table 2-17. - GPIO (Sheet 12 of 15)

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

#	Parameter	Platform	Settings
	GPP_E0 Individual Voltage Select	CML-Y CML-U	3.3 Volts 3.3 Volts
	GPP_E1 Individual Voltage Select	CML-Y CML-U	3.3 Volts 3.3 Volts
	GPP_E2 Individual Voltage Select	CML-Y CML-U	3.3 Volts 3.3 Volts
	GPP_E3 Individual Voltage Select	CML-Y CML-U	3.3 Volts 3.3 Volts
	GPP_E4 Individual Voltage Select	CML-Y CML-U	3.3 Volts 3.3 Volts
	GPP_E5 Individual Voltage Select	CML-Y CML-U	3.3 Volts 3.3 Volts
	GPP_E6 Individual Voltage Select	CML-Y CML-U	3.3 Volts 3.3 Volts
	GPP_E7 Individual Voltage Select	CML-Y CML-U	1.8 Volts 1.8 Volts
	GPP_E8 Individual Voltage Select	CML-Y CML-U	3.3 Volts 3.3 Volts
	GPP_E9 Individual Voltage Select	CML-Y CML-U	3.3 Volts 3.3 Volts

Table 2-17. - GPIO (Sheet 13 of 15)

	GPP_E10 Individual Voltage Select	CML-Y CML-U	3.3 Volts 3.3 Volts
	GPP_E11 Individual Voltage Select	CML-Y CML-U	3.3 Volts 3.3 Volts
	GPP_E12 Individual Voltage Select	CML-Y CML-U	3.3 Volts 3.3 Volts
	GPP_E13 Individual Voltage Select	CML-Y CML-U	3.3 Volts 3.3 Volts
	GPP_E14 Individual Voltage Select	CML-Y CML-U	3.3 Volts 3.3 Volts
	GPP_E15 Individual Voltage Select	CML-Y CML-U	3.3 Volts 3.3 Volts
	GPP_E16 Individual Voltage Select	CML-Y CML-U	3.3 Volts 3.3 Volts
	GPP_E17 Individual Voltage Select	CML-Y CML-U	3.3 Volts 3.3 Volts
	GPP_E18 Individual Voltage Select	CML-Y CML-U	3.3 Volts 3.3 Volts
	GPP_E19 Individual Voltage Select	CML-Y CML-U	3.3 Volts 3.3 Volts
	GPP_E20 Individual Voltage Select	CML-Y CML-U	3.3 Volts 3.3 Volts
	GPP_E21 Individual Voltage Select	CML-Y CML-U	3.3 Volts 3.3 Volts
	GPP_E22 Individual Voltage Select	CML-Y CML-U	3.3 Volts 3.3 Volts
	GPP_E23 Individual Voltage Select	CML-Y CML-U	3.3 Volts 3.3 Volts

GPP_G0 Individual Voltage Select	3.3 Volts	This setting controls the VCCIO voltage for the GPP_G0 GPIO pin.
GPP_G1 Individual Voltage Select	3.3 Volts	This setting controls the VCCIO voltage for the GPP_G1 GPIO pin.
GPP_G2 Individual Voltage Select	3.3 Volts	This setting controls the VCCIO voltage for the GPP_G2 GPIO pin.
GPP_G3 Individual Voltage Select	3.3 Volts	This setting controls the VCCIO voltage for the GPP_G3 GPIO pin.
GPP_G4 Individual Voltage Select	3.3 Volts	This setting controls the VCCIO voltage for the GPP_G4 GPIO pin.
GPP_G5 Individual Voltage Select	3.3 Volts	This setting controls the VCCIO voltage for the GPP_G5 GPIO pin.
GPP_G6 Individual Voltage Select	3.3 Volts	This setting controls the VCCIO voltage for the GPP_G6 GPIO pin.
GPP_G7 Individual Voltage Select	3.3 Volts	This setting controls the VCCIO voltage for the GPP_G7 GPIO pin.

#	Parameter	Platform	Settings
	GPP_G0 Individual Voltage Select	CML-Y CML-U	3.3 Volts 3.3 Volts
	GPP_G1 Individual Voltage Select	CML-Y CML-U	3.3 Volts 3.3 Volts
	GPP_G2 Individual Voltage Select	CML-Y CML-U	3.3 Volts 3.3 Volts
	GPP_G3 Individual Voltage Select	CML-Y CML-U	3.3 Volts 3.3 Volts
	GPP_G4 Individual Voltage Select	CML-Y CML-U	3.3 Volts 3.3 Volts

Table 2-17. - GPIO (Sheet 14 of 15)

	GPP_G5 Individual Voltage Select	CML-Y CML-U	3.3 Volts 3.3 Volts
	GPP_G6 Individual Voltage Select	CML-Y CML-U	3.3 Volts 3.3 Volts
	GPP_G7 Individual Voltage Select	CML-Y CML-U	3.3 Volts 3.3 Volts

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

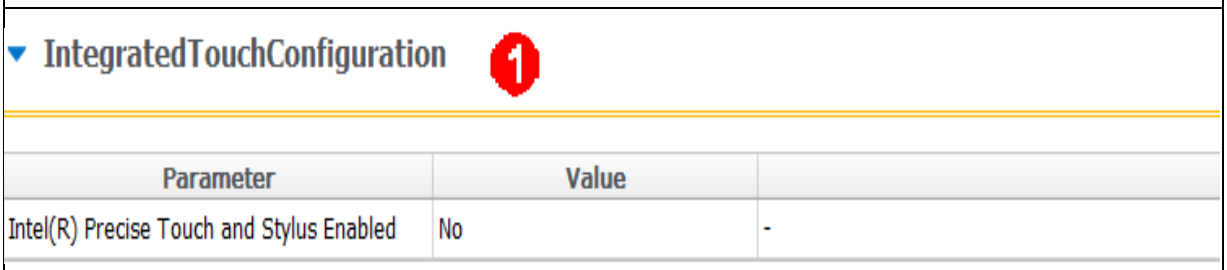
#	Parameter	Platform	Settings
	GPP_H0 Individual Voltage Select	CML-Y CML-U	1.8 Volts 1.8 Volts
	GPP_H1 Individual Voltage Select	CML-Y CML-U	1.8 Volts 1.8 Volts
	GPP_H2 Individual Voltage Select	CML-Y CML-U	1.8 Volts 1.8 Volts
	GPP_H3 Individual Voltage Select	CML-Y CML-U	1.8 Volts 1.8 Volts
	GPP_H4 Individual Voltage Select	CML-Y CML-U	1.8 Volts 1.8 Volts
	GPP_H5 Individual Voltage Select	CML-Y CML-U	1.8 Volts 1.8 Volts

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

	GPP_H6 Individual Voltage Select	CML-Y CML-U	1.8 Volts 1.8 Volts
	GPP_H7 Individual Voltage Select	CML-Y CML-U	1.8 Volts 1.8 Volts
	GPP_H8 Individual Voltage Select	CML-Y CML-U	3.3 Volts 3.3 Volts
	GPP_H9 Individual Voltage Select	CML-Y CML-U	3.3 Volts 3.3 Volts
	GPP_H10 Individual Voltage Select	CML-Y CML-U	3.3 Volts 3.3 Volts
	GPP_H11 Individual Voltage Select	CML-Y CML-U	1.8 Volts 1.8 Volts
	GPP_H12 Individual Voltage Select	CML-Y CML-U	1.8 Volts 3.3 Volts
	GPP_H13 Individual Voltage Select	CML-Y CML-U	3.3 Volts 3.3 Volts
	GPP_H14 Individual Voltage Select	CML-Y CML-U	1.8 Volts 1.8 Volts
	GPP_H15 Individual Voltage Select	CML-Y CML-U	1.8 Volts 1.8 Volts
	GPP_H16 Individual Voltage Select	CML-Y CML-U	3.3 Volts 1.8 Volts
	GPP_H17 Individual Voltage Select	CML-Y CML-U	3.3 Volts 1.8 Volts
	GPP_H18 Individual Voltage Select	CML-Y CML-U	3.3 Volts 3.3 Volts
	GPP_H19 Individual Voltage Select	CML-Y CML-U	3.3 Volts 3.3 Volts
	GPP_H20 Individual Voltage Select	CML-Y CML-U	1.8 Volts 3.3 Volts
	GPP_H21 Individual Voltage Select	CML-Y CML-U	3.3 Volts 3.3 Volts
	GPP_H22 Individual Voltage Select	CML-Y CML-U	1.8 Volts 3.3 Volts
	GPP_H23 Individual Voltage Select	CML-Y CML-U	3.3 Volts 3.3 Volts
	Intel® HD Audio Voltage Select	CML-Y CML-U	1.8 Volts 1.8 Volts

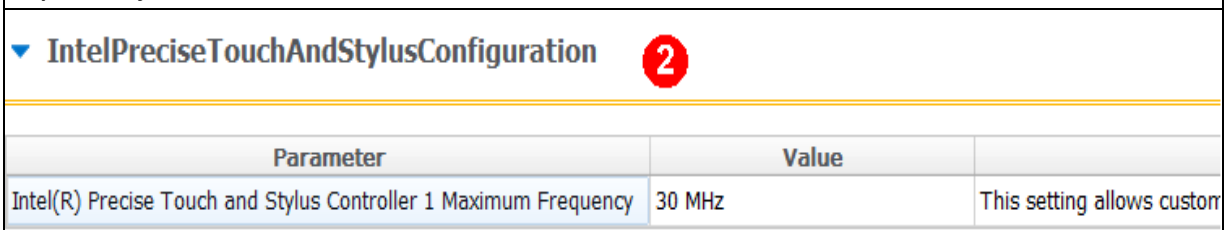
Table 2-18. - Intel® Precise Touch and Stylus

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



#	Parameter	Platform	Settings
1	**IntegratedTouchConfiguration**		
	Intel® Precise Touch and Stylus Enabled	CML-Y CML-U	No No

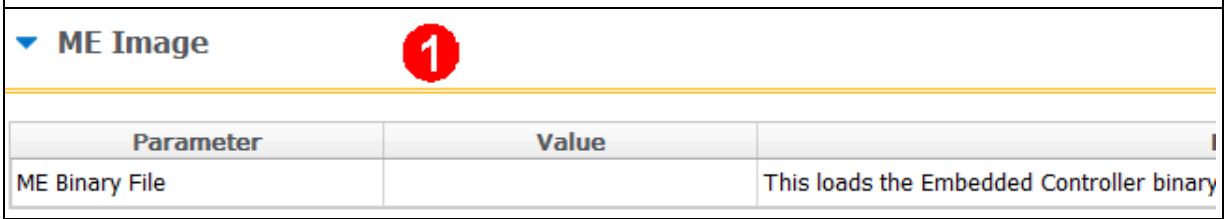
Click on Intel® Precise Touch and Stylus in the left tabs menu> IntegratedTouchAndStylusConfiguration is expanded by default:



2	**Intel® Precise Touch and Stylus - IntelPerciseTouchandStylusConfiguration**		
	Intel® Precise Touch and Stylus Controller 1 Maximum Frequency	CML-Y CML-U	30MHz 30MHz

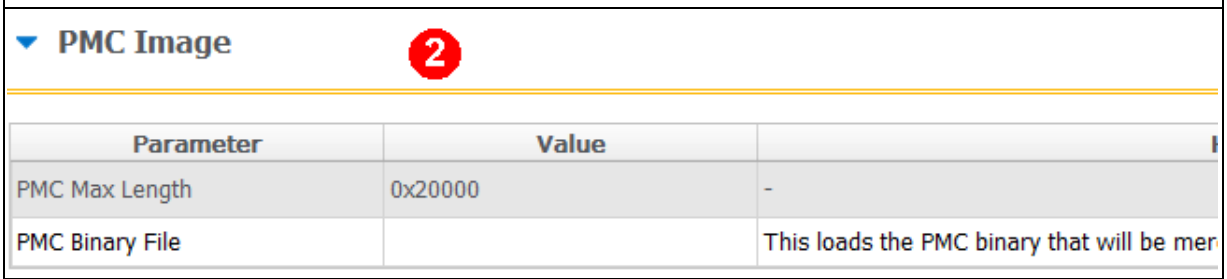
Table 2-19. - FW Update Image Build

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



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

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



#	Parameter	Platform	Settings
2	**PMC Image**		
	PMC Max Length **Note:** This value will be automatically populated by Intel® FIT during image build.		
	PMC Binary Image **Values: Binary File** This loads the PMC binary that will be merged into the FWUpdate image generated by the Intel® FIT tool.	CML-Y CML-U	PMC Binary PMC Binary

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

Table 2-19. - FW Update Image Build

OEM KM Image 3

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

#	Parameter	Platform	Settings
3	**OEM KM Image**		
	OEM KM Enable **Values: Enabled / Disabled** This setting Enables / Disables OEM KM in the FWUpdate image.	CML-Y CML-U	Enabled Enabled
	OEM KM Max Length **Note:** This value will be automatically populated by Intel® FIT during image build.		
	OEM Key Manifest Binary File **Values: Binary File** This loads the OEM Key manifest binary merged into the output image generated by the Intel® FIT tool.	CML-Y CML-U	OEM KM Binary OEM KM Binary
Click on FW Update Image Build in the left tabs menu> ISH Image is expanded by default:			

ISH Image 4

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

#	Parameter	Platform	Settings
4	**ISH Image**		
	ISH Enable **Values: Enabled / Disabled** This setting Enables / Disables ISH in the FWUpdate image.	CML-Y CML-U	Enabled Enabled
	ISH Max Length **Note:** This value will be automatically populated by Intel® FIT during image build.		
	ISH Binary File **Values: Binary File** This loads the ISH binary merged into the output image generated by the Intel® FIT tool.	CML-Y CML-U	ISH Binary ISH Binary
Click on FW Update Image Build in the left tabs menu> IUNIT Image is expanded by default:			

Table 2-19. - FW Update Image Build

IUNIT Image 5

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

#	Parameter	Platform	Settings
5	**IUNIT Image**		
	IUnit Enable **Values: Enabled / Disabled** This setting Enables / Disables IUNIT in the FWUpdate image.	CML-Y CML-U	Enabled Enabled
	IUnit Max Length **Note:** This value will be automatically populated by Intel® FIT during image build.		
	IUnit Binary File **Values: Binary File** This loads the IUnit binary merged into the output image generated by the Intel® FIT tool.	CML-Y CML-U	IUnit Binary IUnit Binary

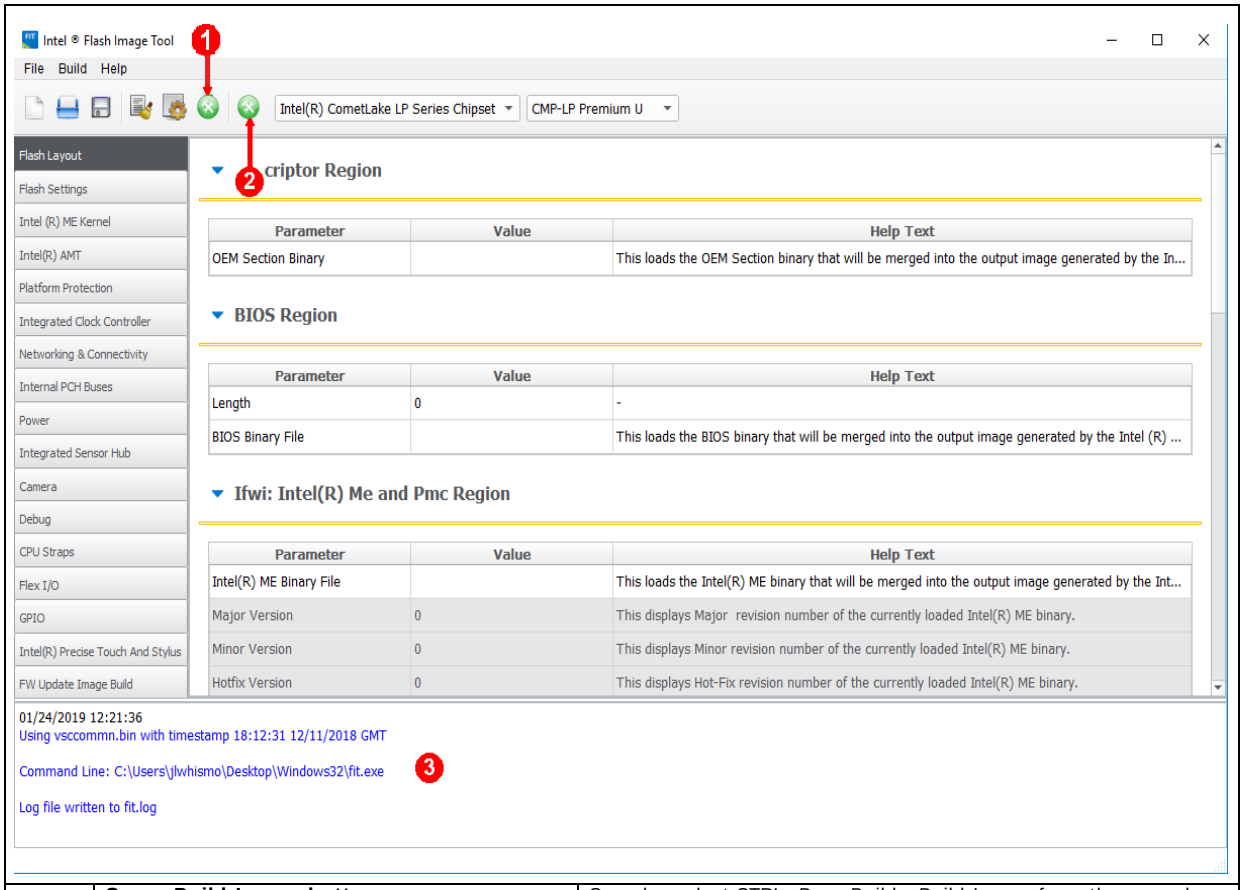
Click on FW Update Image Build in the left tabs menu> PCHC Image is expanded by default:

PCHC Image 6

Parameter	Value	
PCH Configuration Enable	Enabled	This setting Enables / Disables PCHC in the FWUpdate image.
PCH Configuration Max Length	0x1000	-
PCH Configuration File		This loads the PCH Configuration binary merged into the outp

#	Parameter	Platform	Settings
6	**PCHC Image**		
	PCH Configuration Enable **Values: Enabled / Disabled** This setting Enables / Disables PCHC in the FWUpdate image.	ICL-Y ICL-U	Enabled Enabled
	PCH Configuration Max Length		
	Values: Binary File This loads the PCHC binary merged into the output image generated by the Intel® FIT tool.	ICL-Y ICL-U	PCHC Binary PCHC Binary

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



1	**Green Build Image button**	Can also select CTRL+B, or Build> Build Image from the menu bar along the top of the screen
2	**Green Build Image for FWUpdate button**	Directs the Intel® FIT tool to build a firmware update image based in the binaries provided under the FW Update Image Build tab.
3	**Console shows status of build and path where saved**	

3 Programming SPI Flash Devices and Checking Firmware Status

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

3.1 Flash Burner/Programmer

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

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

   If two total SPI Flash devices were specified during the build process, then additional image files will be saved, one for each SPI Flash 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: 14.0.0.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, 1. Enter BIOS menu, then go to the 'Boot' screen 2. Change 'Boot Option #1' to be your USB key (ensure USB key is formatted to be DOS bootable) 3. Press 'F4' to save settings and reboot
Hear 3 beeps when platform powers on	Possible device is disconnected or device not found, check • platform power and MCP fan power connectors • DIMM memory modules (if applicable for memory down modules • USB devices (keyboard, mouse, USB key) may be plugged into inactive USB port • missing/incorrect jumpers • missing or poorly socketed MCP
No display on monitor	Ensure Corporate FW SKU supports integrated graphics. Try external graphics card.
USB device not detected or does not work	USB device may be plugged into inactive USB port
System does not boot (Post Code 00)	Incorrect Flash image – possible reasons: • wrong FW selected during Flash image build process • wrong Flash size selected Re-build image with correct settings and re-flash using Flash burner.

§ §

A Appendix — Flash Configurations

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

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

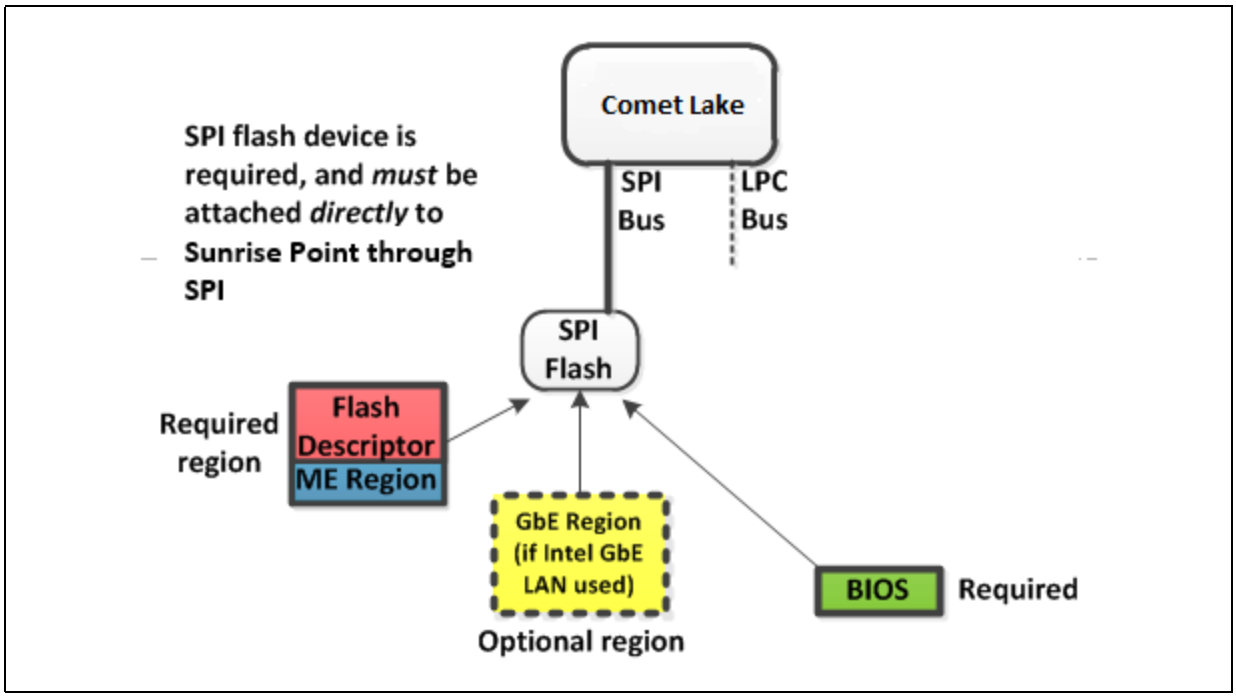
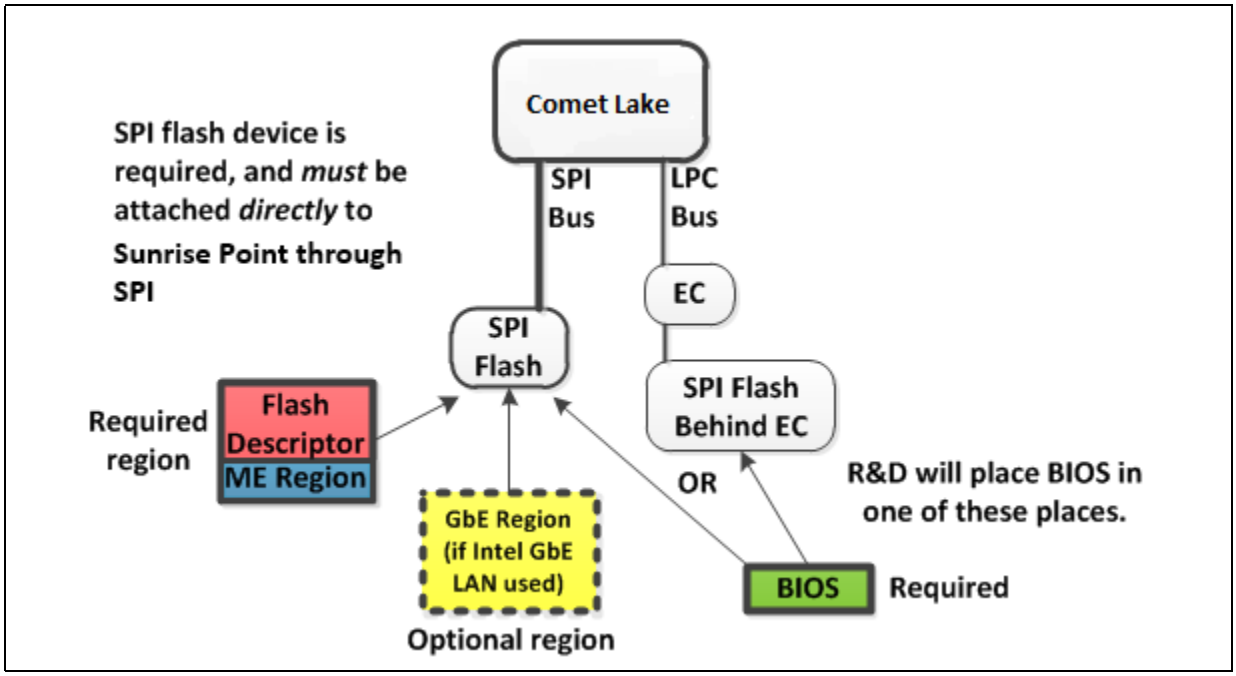


Figure A-2. Configuration "B" — Mobile Only



§ §

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 Comet Lake-LP SKUs.

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

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

Table B-1. Intel® ICCS SKU Matrix - CNP-LP

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

C Appendix — Boot Guard Configuration

C.1 Boot Guard Profiles

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

Table C-1. Profile Description

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

C.2 Enforcement Policies

Table C-2. Enforcement Policy Description

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

C.3 OEM Profile Parameters

Table C-3. Profile Parameters Description

Parameter	Description	Settings
Force Boot Guard ACM Enabled (F)	Force Boot Guard Boot determines if the platform starts the Force Boot Guard Boot timer. If it successfully starts it indicates success. When the Force Boot Guard timer stops, it starts the Protect Bios Environment timer, if indicated by the boot policy restrictions. Anchor ACM then jumps to the Initial Boot Block(IBB) with the Force Boot Guard Boot time stopped and the Protect BIOS enable timer running.	**false** - Allow the CPU to jump to the legacy reset vector if the Boot Guard Module cannot be successfully loaded. (default) **true -** Force the Boot Guard ACM to execute.
Verified Boot Enabled (V)	Boot Guard cryptographically verifies the platform Initial Boot Block (IBB) using the boot policy key. On successful verification, Boot Guard executes Initial Boot Block (IBB) using the boot policy key. If the verification fails, Anchor signals or enters Remediation.	**false** - Platform does not perform verified boot (default) **true** - Platform performs verified boot
Measured Boot Enabled (M)	Boot Guard measures the Initial Boot Block (IBB) into the TPM. Boot Guard perform no verification that the IBB is correct or from the platform manufacturer. The Slylake implementation of Boot Guard will support measurements into TPM or Intel's Platform Trust Technology.	**false** - Platform does not perform measured boot (default) **true** - Platform performs measured boot
Protect Bios Environment Enabled (PBE)	Platform manufacturer may want Initial boot block to be protected between verification/ measurement and execution from attacks on buses and non-CPU components. Boot Guard accomplishes this by allowing the initial boot block to be verified and executed in LLC in NEM if PBE is enabled.	**false** - Take no actions to control the environment during execution of the BIOS components (default) **true** - Takes actions to control the environment during the execution of the BIOS components.
Error Enforcement Policy (ENF)	Boot Guard invokes the Enforcement Policy when a fatal error is encountered. The action taken by ENF is determined by the OEM set persistent policies. Like, • Allowing platform to continue to boot • Immediate Shutdown • Shutdown with Timeout intervals When the ENF logic is invoked, PTT or TPM also disconnects.	See Section C-2 for details.

D Appendix — Intel® Platform Trust Technology

D.1 Intel® Platform Trust Technology

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

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

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

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

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

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