

Comet Lake-V

# Intel® Converged Security and Converged Security and Management Engine Firmware 14.5

Consumer Firmware Bring Up Guide

*December 2019*

| Revision 1.2

**Intel Confidential**



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

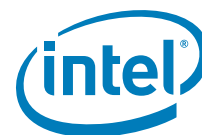
Intel processor numbers are not a measure of performance. Processor numbers differentiate features within each processor family, not across different processor families. See [http://www.intel.com/products/processor\\_number](http://www.intel.com/products/processor_number) for details. I2C is a two-wire 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

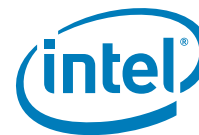
<b>1</b>	<b>Introduction</b>	<b>6</b>
1.1	Related Documentation	6
1.2	Intel® ME FW Features	6
1.3	Prerequisites	6
1.4	Acronyms and Definitions	7
1.4.1	General	7
1.4.2	Intel® Converged Security and Management Engine	8
1.4.3	System States and Power Management	9
1.5	Reference Documents	9
1.6	Format and Notation	9
1.7	Kit Contents	11
1.8	External Hardware Requirements for Bring Up	18
<b>2</b>	<b>Image Creation: Intel® Flash Image Tool</b>	<b>19</b>
2.1	Start Intel® FIT	19
2.2	Step-by-Step Guide to Build SPI Flash Image with Intel® FIT Interface	19
<b>3</b>	<b>Programming SPI Flash Devices and Checking Firmware Status</b>	<b>106</b>
3.1	Flash Burner/Programmer	106
3.1.1	In-Circuit SPI Flash Programming for CRB	106
3.2	Flash Programming Tool (Intel® FPT)	106
3.2.1	Intel® FPT Windows* Version	107
3.3	Checking Intel® ME Firmware Status	108
3.4	Common Bring Up Issues and Troubleshooting Table	110
<b>A</b>	<b>Appendix — Flash Configurations</b>	<b>111</b>
<b>B</b>	<b>Appendix — Intel® ICCS SKU Support Matrix</b>	<b>113</b>
B.1	Intel® ICCS SKU Matrix - CNP-H	113
B.2	How to configure CLKREQ# parameters	114
<b>C</b>	<b>Appendix — Boot Guard Configuration</b>	<b>115</b>
C.1	Boot Guard Profiles	115
C.2	Enforcement Policies	115
C.3	OEM Profile Parameters	116
<b>D</b>	<b>Appendix — Intel® Platform Trust Technology</b>	<b>117</b>
D.1	Intel® Platform Trust Technology	117
<b>E</b>	<b>Appendix — Integrated Sensor Hub (ISH) Public Key Settings</b>	<b>118</b>



## Figures

## Tables

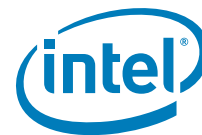
1-1 Number Format Notation.....	10
1-2 Data Format Notation .....	10
1-3 Kit Contents .....	11
2-1 - Initial Screen Layout .....	20
2-2 - Build Settings.....	29
2-3 - Flash Layout .....	31
2-4 - Flash Settings .....	36
2-5 - Intel® ME Kernel .....	45
2-6 - Intel® AMT .....	49
2-7 - Platform Protection .....	56
2-8 - Integrated Clock Controller .....	64
2-9 - Networking & Connectivity .....	75
2-10- Internal PCH Buses .....	78
2-11- Power .....	83
2-12- Debug.....	85
2-13- CPU Straps .....	89
2-14- Flex I/O Straps.....	92
2-15- GPIO.....	99
2-16- Intel® Precise Touch and Stylus.....	102
2-17- FW Update Image Build .....	103
2-18- Intel® FIT - Build Image .....	105
3-1 Common Bring Up Issues and Troubleshooting Table .....	110



## Revision History

Document Number	Revision Number	Description	Revision Date
	1.0	Initial Release	September 2019
	1.1	Updated Anti-Rollback default setting to Enabled	November 2019
	1.2	Corrected recommended timing values for USB3Gen2PCIe PLL OFF Wait, USB3Gen2PCIe PLL PG Wait, Run-time S0 SUS PG Wait, BCLK PLL Shutdown Wait Interval and 24MHz Crystal Shutdown Wait Interval Corrected recommended value for Crystal Oscillator Fast Restart Mode	December 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-V SPI Programming Guide** SPI Programming Guide and [Appendix A](#). Once the SPI Flash image is built, it will be programmed to the target based platform and the platform will be booted. This document also covers any tests and checks required to ensure that this boot process is successful and that Intel® ME Consumer FW is operating as expected.

## 1.1 Related Documentation

VIP: Kit# 106913 - Intel® Ethernet Network Connections (20.1 OEM Gen) - LAN Software Production Candidate 20.1

CDI # 559465 Intel® Ethernet Connection i219 [Jacksonville]

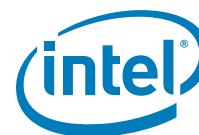
## 1.2 Intel® ME FW Features

This firmware release includes the following applications:

- Platform Clocks – Tune clock silicon to the parameters of a specific board, configure clocks at run time, and power management clocks. **Benefit:** Allows extensive customizability and soft control of “Third generation” clock solution and makes clocks available before CPU powers up.
- Silicon Workaround Capability – Intel® 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.

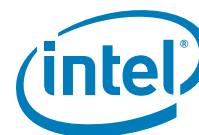
This document makes only the following limited assumptions regarding hardware:

- The platform is Comet Lake-V 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® 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® Converged Security and Management Engine Interface (Intel® MEI)	Interface between the Management Engine and the Host system
Intel® MEI driver	Intel® ME host driver that runs on the host and interfaces between ISV Agents and the Intel® ME HW.
IT User	Information Technology User. Typically very technical and uses a management console to ensure functionality of multiple PCs on a network.
LMS	Local Management Service: A SW application which runs on the host machine and provide a secured communication between the ISV agent and the Intel® Management Engine Firmware.
Intel® ME	Intel® Management Engine: The embedded processor residing in the chipset MCP
MECI	ME-VE Communication Interface
NVM	Non-Volatile Memory: A type of memory that will retain its contents even if power is removed. In the Intel® AMT current implementation, this is achieved using a FLASH memory device.
OOB Interface	Out Of Band interface: This is WSMAN interface over secure or non-secure TCP protocol.
OS not Functional	The Host OS is considered non-functional in Sx power state and any one of the following cases when system is in S0 power state: <ul style="list-style-type: none"> <li>• OS is hung</li> <li>• After PCI reset</li> <li>• OS watch dog expires</li> <li>• OS is not present</li> </ul>
System States	Operating System power states such as S0. See detailed definitions in System States and Power Management section.



### 1.4.3 System States and Power Management

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

## 1.5 Reference Documents

Document	Doc Number/ Location*
<i>Comet Lake Intel® Converged Security and Management Engine (Intel® CSME) and Embedded Controller Interaction Product Specification Revision 0.5</i>	TBD / CDI
<i>Intel® Converged Security and Management Engine BIOS Writers Guide</i>	TBD / *
<i>Intel® Converged Security and Management Engine (Intel® CSME) 14 SKU Firmware Consumer Compliance Guide for Comet Lake PCH-V Chipset Family - Comet Lake Platform Compliancy and Testing Guide - Revision 1.1</i>	TBD / CDI

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

## 1.6 Format and Notation

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

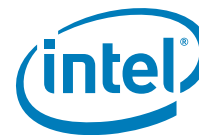


Table 1-1. Number Format Notation

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

Table 1-2. Data Format Notation

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



## 1.7 Kit Contents

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

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

File or [Directory]	Content Description
[root]	Root directory
[CNP-H]	
CML-V Consumer Bring Up Guide.pdf	Firmware Bring-up for Comet Lake-V.
CML-V Client SPI Programming Guide.pdf	How to program SPI device parameters and descriptor region details. Also contains a complete SPI Flash softstrap reference.
[Image Components]	
[3rd party Licenses in FW]	Third Party Licenses used in firmware
Apache Harmony Apache Version 2.0, January 2004 w header.txt	
Apache-Xerces-Java-XML-Parser.txt	
ConvertUTF unicode license.txt	
CxImage license complete.txt	
HTTP Client C MIT license.txt	
Ilvm.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]	
[PreProduction]	Intel® ME firmware image ( <b>Non Production FW Rom Bypass</b> ) - supports <b>unfused</b> Icelake PCH-V Platform I/O MCP steppings: <ul style="list-style-type: none"> <li>Unfused (Super SKU)</li> </ul> <p><b>Note: For PAVP Testing,</b> you must match Production FW with Production Part and Non Production FW with Non Production Parts.</p>
CSME_FW_Consumer_14.5.0.xxxx.bin	

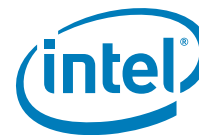


Table 1-3. Kit Contents (Sheet 2 of 7)

File or [Directory]	Content Description
[Production]	Intel® ME firmware image ( <b>Non Production FW</b> ) - supports <b>unfused</b> Ice Lake PCH-V Platform I/O MCP steppings: <ul style="list-style-type: none"> <li>Unfused (Super SKU)</li> </ul> <b>Note: For PAVP Testing</b> , you must match Production FW with Production Part and Non Production FW with Non Production Parts.
CSME_FW_Consumer_14.5.0.xxxx_Production.bin	
[PCHC]	
[PreProduction]	
[Production]	
[PMC]	
[PreProduction]	
[Production]	
[Prestitched]	
[PreProduction]	
[Production]	
[Installers]	
Intel®_ME SW Installation Guide.pdf	Intel® CSME Software installation Guide.
[3rd party Licenses SW]	Third Party Licenses used in software
ACE-TAO-CIAO.pdf	
Apache-Xerces-C++-XML-Parser.txt	
libxml2.txt	
Microsoft Windows Classic Samples.txt	
openwsman.pdf	
Windows driver samples.txt	
WixLicenseNote.txt	
[ME_SW_MSI]	
IntelMEFWVer.dll	DLL file
MUP	XML file
SetupME	Intel® CSME software installer
[MEI-Only Installer MSI]	
IntelMEFWVer.dll	DLL file
MEI Setup	MEI software installer
MUP	XML file



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

File or [Directory]	Content Description
[WindowsDriverPackages]	Windows* driver packages
[ICLS]	Intel® Capability Licensing Service drivers
iclsClient.cat	
iclsClient.inf	
[icls]	
[conf]	
cacert.pem	
epid_paramcert.dat	
epid2_paramcert.dat	
EPI DGroupCertLegacy.cer	
EPI DGroupdCertX509.cer	
iclsProxy.conf	
[Documents]	Documents for Intel® Capability Licensing Service
development_tools.txt	
License.txt	
Readme.txt	
redist.txt	
Third Party Licenses.txt	
[x64]	x64 drivers
iclsClient.dll	
iclsClientInternal.dll	
iclsProxy.dll	
iclsProxyInternal.dll	
IntelPTTEKRecertification.exe	
libcrypto-1_1-x64.dll	
libssl-1_1-x64.dll	
SocketHeciServer.exe	
TPMProvisioningService.exe	
[x86]	x86 drivers
x86_iclsClient.dll	
x86_iclsClientInternal.dll	
x86_iclsProxy.dll	
x86_iclsProxyInternal.dll	
x86_IntelPTTEKRecertification.exe	
x86_libcrypto-1_1-x64.dll	
x86_libssl-1_1-x64.dll	
x86_SocketHeciServer.exe	
x86_TPMProvisioningService.exe	
[vs2015]	

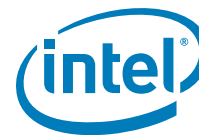


Table 1-3. Kit Contents (Sheet 4 of 7)

File or [Directory]	Content Description
[x64]	x64 Visual Studio* runtime DLLs
msvcp140.dll	
vcruntime140.dll	
[x86]	x86 Visual Studio* runtime DLLs
x86_msvc140.dll	
x86_vcruntime140.dll	
[JHI]	
[win10]	Intel® Dynamic Application Loader drivers
bhPlugin.dll	
bhPluginV2.dll	
dal.cat	
DAL.inf	
JHI.dll	
jhi_service.exe	
JHI 64.dll	
SpoolerApplet.dalp	
TEEManagement.dll	
TEEManagement64.dll	
TEETransport.dll	
[MEI]	Intel® MEI drivers files
heci.cat	
heci.inf	
[x64]	x64 driver
TeeDriverW8x64.sys	
[x86]	x86 driver
TeeDriverW8.sys	
OemExtension]	OEM Extension driver
OemExtension.cat	
OemExtension.inf	
[Tools]	
[3rd party Licenses in Tools]	Third part Licenses in Tools
Android Autogenerated Files Apache 2.0.pdf	
C Make License.pdf	
EFI tool kit intel BSD 2 clause license.txt	
Expat XMLparser MIT license.txt	
Jquery MIT license.txt	
JsonCpp MIT license.txt	
MSDN Example code.pdf	
pugixml license.txt	
[ICC_Tools]	



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

File or [Directory]	Content Description
Intel® ME Firmware ICC Tools User Guide.pdf	ICC Tools User Guide
[CCT]	
cct	Exe file
cct	Ini file
cctDll.dll	
cctDllx64.dll	
cctWin	Exe file
[EFI]	
cct.efi	CCT for EFI
[System Tools]	
System Tools User Guide.pdf	System Tools User Guide
[FIT]	
[system32]	
fit.exe	Intel® Flash Image Tool (Intel® FIT)
vsccommn.bin	Binary containing the supported SPI parts
VSCCommn_bin Content.pdf	Documentation listing the SPI parts supported by vsccommn.bin
[FPT]	
[EFI 64]	
fparts.txt	List of supported SPI Flash devices with specific Flash parameters
fpt.efi	FPT for EFI
[Windows]	
fparts.txt	List of supported SPI Flash devices with specific Flash parameters
fptw.exe	FPT for Windows*
ldrvidll.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
ldrvidll32e.dll	
Pmxdll32e.dll	
[FWUpdate]	
[EFI 64]	
FWUpdLcl.efi	FW Update Tool (EFI version)
fwudef.h	
FwUpdateEfiLib.lib	
fwupdatelib.h	



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

File or [Directory]	Content Description
fwupdatelibdeprecated.h	
[Win]	
FWUpdLcl.exe	FW Update Tool (Windows* version 32bit)
ldrvidll.dll	
Pmxdll.dll	
errorlist.c	
errorlist.h	
fwudef.h	
fwupdatelib.h	
FWUpdateLib.lib	
fwupdatelibdeprecated.h	
FWUpdateSample.c	
[Win64]	
FWUpdLcl64.exe	FW Update Tool (Windows* version 64bit)
ldrvidll32e.dll	
Pmxdll32e.dll	
errorlist.c	
errorlist.h	
fwudef.h	
fwupdatelib.h	
FWUpdateLib.lib	
fwupdatelibdeprecated.h	
FWUpdateSample.c	
[FWUpdate_RS]	FW Update Tool API code
[Efi64]	
fwUpdLcl.efi	
errorlist.c	
errorlist.h	
fwudef.h	
fwupdatelib.h	
FWUpdateLib.lib	
fwupdatelibdeprecated.h	
FWUpdateSample.c	
[MEInfo]	
[EFI64]	
MEInfo.efi	Intel® ME Information Tool (EFI version)
[Windows]	
MEInfoWin.exe	Intel® ME Information Tool (Windows* version 32bit)






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

File or [Directory]		Content Description
	I drv.dll	
	Pmxdll.dll	
	[Windows64]	
	MEInfoWin64.exe	Intel® ME Information Tool (Windows* version 64bit)
	I drv.dll32e.dll	
	Pmxdll32e.dll	
	[MEManuf]	
	[EFI64]	
	MEManuf.efi	Intel® ME Manufacturing Tool (EFI version)
	[Windows]	
	I drv.dll	
	MEManufWin.exe	Intel® ME Manufacturing Tool (Windows* version 32bit)
	Pmxdll.dll	
	[Windows64]	
	I drv.dll32e.dll	
	MEManufWin64.exe	Intel® ME Manufacturing Tool (Windows* version 64bit)
	Pmxdll32e.dll	
	(empty)	
	[Manifest Extension Utility]	
	[Win]	
	Signing and Manifesting Guide.pdf	
	[Windows32]	
	meu.exe	Intel® Manifest Extension Utility (MEU) executable file that allows input of FW binary and outputs and independent updatable partition that is compressed and signed.

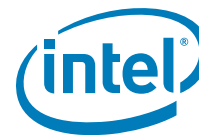


## 1.8 External Hardware Requirements for Bring Up

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

Windows* OS System	Flash Burner	DOS Bootable USB Key
		
<p><b>Equipment:</b></p> <ul style="list-style-type: none"> <li>Laptop or desktop that supports win32 applications</li> </ul> <p><b>Purpose:</b></p> <ul style="list-style-type: none"> <li>Will run firmware image assembly and build process software.</li> </ul>	<p><b>Equipment:</b></p> <ul style="list-style-type: none"> <li>(Optional) For platforms that don't boot, a Flash Chip Programmer will be required</li> <li>For platforms that can boot to DOS or Windows*, a Intel® FPT is provided in this kit</li> </ul> <p><b>Purpose:</b></p> <ul style="list-style-type: none"> <li>Will burn firmware images onto the target system Flash device(s).</li> </ul>	<p><b>Equipment:</b></p> <ul style="list-style-type: none"> <li>A DOS Bootable USB Key (Size &gt; 512 MB)</li> </ul> <p><b>Purpose:</b></p> <ul style="list-style-type: none"> <li>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.</li> <li>Or will be used to transfer a firmware image onto a Flash burner.</li> </ul>

§ §



## 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 Intel® Flash Image Tool. Using Explorer\*, navigate to **[root]\Tools\System Tools\Flash Image Tool**. Verify that the directory contents are correct (see [Section 1.7](#)). Double-click **FIT.exe**.
2. **NOTE:** In the tables below, where default settings are listed for CML-V, 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

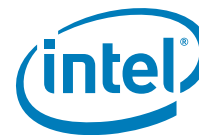


Table 2-1. - Initial Screen Layout (Sheet 1 of 9)

#	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

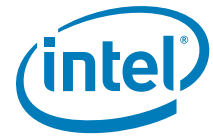


Table 2-1. - Initial Screen Layout (Sheet 3 of 9)

#	Label	Contents
	Flash Layout	9
	Flash Settings	10
	Intel(R) ME Kernel	11



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

#	Label	Contents
<b>9</b>	Flash Layout Tab	Flash Layout which contains (see <a href="#">Table 2-3</a> ): <ul style="list-style-type: none"> <li>• Descriptor Region</li> <li>• BIOS Region</li> <li>• IFWI: Intel® ME and PMC Region</li> <li>• EC Region</li> <li>• GBE Region</li> <li>• SubPartitions</li> <li>• PDR Region</li> </ul>
<b>10</b>	Flash Settings Tab	Flash Settings which contains (see <a href="#">Table 2-4</a> ): <ul style="list-style-type: none"> <li>• Flash Components</li> <li>• Host CPU/ BIOS Master Access</li> <li>• Intel® ME Master Access</li> <li>• GBE Master Access</li> <li>• EC Master Access</li> <li>• Flash Configuration</li> <li>• Legacy VSCC Table - VSCC Entries</li> <li>• BIOS Configuration</li> <li>• OEM and Platform IDs</li> <li>• FPF Configuration</li> </ul>
<b>11</b>	Intel® ME Kernel Tab	Intel® ME Kernel which contains (see <a href="#">Table 2-5</a> ): <ul style="list-style-type: none"> <li>• Processor</li> <li>• Intel® ME Firmware Update</li> <li>• Image Identification</li> <li>• Firmware Diagnostics</li> <li>• Post Manufacturing Lock</li> <li>• MCTP Configuration</li> <li>• Intel® ME Boot Configuration</li> <li>• Reserved</li> </ul>

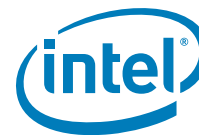


Table 2-1. - Initial Screen Layout (Sheet 5 of 9)

#	Label	Contents
12	Intel® AMT Tab	Intel® AMT which contains (see <a href="#">Table 2-6</a> ): <ul style="list-style-type: none"> <li>• Intel® AMT Configuration</li> <li>• KVM Configuration</li> <li>• Provisioning Configuration</li> <li>• OEM Customizable Certificates (1, 2, 3)</li> <li>• OEM Default Certificates (1, 2, 3, 4, 5)</li> <li>• Redirection Configuration</li> <li>• TLS Configuration</li> </ul>
13	Platform Protection Tab	Platform Protection which contains (see <a href="#">Table 2-7</a> ): <ul style="list-style-type: none"> <li>• Content Protection</li> <li>• Graphics uController</li> <li>• Hash Key Configuration for Bootguard / ISH</li> <li>• Exclusion Ranges</li> <li>• Descriptor Configuration</li> <li>• Boot Guard Configuration</li> <li>• Intel® PTT Configuration</li> <li>• TPM Over SPI Bus Configuration</li> <li>• BIOS Guard Configuration</li> <li>• TXT Configuration</li> <li>• Crypto Hardware Support</li> <li>• Platform Trusted Device Support</li> <li>• Intel FPF Anti-Rollback Configuration</li> </ul>



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

#	Label	Contents
<b>14</b>	Integrated Clock Controller Tab	Integrated Clock Controller which contains (see <a href="#">Table 2-8</a> ): <ul style="list-style-type: none"><li>• Integrated Clock Controller Policies</li><li>• Profiles</li></ul>
<b>15</b>	Networking & Connectivity Tab	Networking & Connectivity which contains (see <a href="#">Table 2-9</a> ): <ul style="list-style-type: none"><li>• Platform vPro NIC</li><li>• Wired LAN Configuration</li><li>• Wireless LAN Configuration</li></ul>

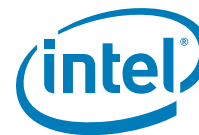


Table 2-1. - Initial Screen Layout (Sheet 7 of 9)

#	Label	Contents
16	Internal PCH Buses Tab	Internal PCH Buses which contains (see Table 2-10): <ul style="list-style-type: none"> <li>PCH Timer Configuration</li> <li>SMBus / SMLink Configuration</li> <li>DMI Configuration</li> <li>eSPI Configuration</li> </ul>
17	Power Tab	Power which contains (see Table 2-11): <ul style="list-style-type: none"> <li>Platform Power</li> <li>Deep Sx</li> <li>PCH Thermal Reporting</li> </ul>
18	Debug Tab	Debug which contains (see Table 2-12): <ul style="list-style-type: none"> <li>IDLM</li> <li>Delayed Authentication Mode Configuration</li> <li>Intel® Trace Hub Technology</li> <li>Intel® ME Firmware Debugging Overrides</li> <li>Direct Connection Interface Configuration</li> <li>eSPI Feature Overrides</li> </ul>

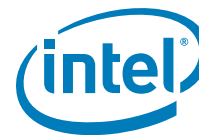


Table 2-1. - Initial Screen Layout (Sheet 8 of 9)

#	Label	Contents
19	CPU Straps Tab	CPU Straps which contain a detailed list of parameters (see <a href="#">Table 2-13</a> ) <ul style="list-style-type: none"> <li>CPU Straps</li> </ul>
20	Flex I/O Tab	Flex I/O which contains (see <a href="#">Table 2-14</a> ): <ul style="list-style-type: none"> <li>Intel® RST for PCIe Configuration</li> <li>PCIe Lane Reversal Configuration</li> <li>PCIe Port Configuration</li> <li>SATA / PCIe Combo Port Configuration</li> <li>USB3 Port Configuration</li> <li>PCIe gen3 PLL Clock Control</li> </ul>
21	GPIO Tab	GPIO which contains (see <a href="#">Table 2-15</a> ): <ul style="list-style-type: none"> <li>LAN / GPIO Select</li> <li>WLAN / GPIO Select</li> <li>Platform Power / GPIO</li> <li>ME Feature Pins</li> <li>Touch Controller Pins</li> <li>SMLink1 Pins</li> </ul>
22	Intel® Precise Touch and Stylus	Intel® Precise Touch and Stylus which contains (see <a href="#">Table 2-16</a> ): <ul style="list-style-type: none"> <li>Integrated Touch Configuration</li> <li>Intel® Integrated Touch and Stylus Configuration</li> </ul>

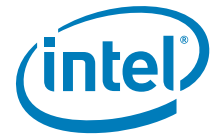


Table 2-1. - Initial Screen Layout (Sheet 9 of 9)

#	Label	Contents
23	FW Update Image Build	FW Update Image Build which contains (see <a href="#">Table 2-17</a> ): <ul style="list-style-type: none"><li>• ME Image</li><li>• PMC Image</li><li>• OEM KM Image</li><li>• PCHC Image</li></ul>
	Console Window Area	Displays opening messages, log file entries, and build activity messages

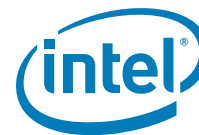


Table 2-2. - Build Settings (Sheet 1 of 2)

Click on Build Button in the top menu bar > Build Settings window pop up is displayed:			
▼ Image Build Settings			
Parameter	Value		Help Text
Output Path	\$DestDir\outimage.bin	1	-
FWUpdate Output Path	\$DestDir\FWUpdate.bin	2	-
Build FWUpdate With Full Image	No	3	-
Generate Intermediate Files	Yes	4	-
Enable Boot Guard warning message at build time	Yes	5	-
Enable Intel (R) Platform Trust Technology warning ...	Yes	6	-
Region Order	53241	7	1=BIOS, 2=ME/IFWI, 3=GbE, 4=PDR, 5=EC
IfwiBuildVersion	0x0	8	32-bit value to use as the IFWI build version number
Intel(R) Manifest Extension Utility Path		9	-
Signing Tool Path		10	-
Signing Tool	OpenSSL	11	-
▼ Environment Variables			
Parameter	Value		Help Text
\$WorkingDir	.		Path for environment variable \$WorkingDir
\$SourceDir	.		Path for environment variable \$SourceDir
\$DestDir	.		Path for environment variable \$DestDir
\$UserVar1	.		Path for environment variable \$UserVar1
\$UserVar2	.		Path for environment variable \$UserVar2
\$UserVar3	.		Path for environment variable \$UserVar3
#	Parameter	CRB	Values
1	Output Path		Double click to the right of outimage.bin and click to get browse button to specify path and name of file to create for the build - default is outimage.bin in the same folder as Intel® FIT tool
2	FWUpdate Output Path		Double click to the right of FWUpdate.bin and click to get browse button to specify path and name of file to create for the build.
3	Build FWUpdate With Full Image	No	Yes/No - No is default
4	Generate Intermediate Files	Yes	Yes/No - Yes is default
5	Enable Boot Guard warning message at build time	Yes	Yes/No - Yes is default
6	Enable Intel (R) Platform Trust Technology warning message at build time	Yes	Yes/No - Yes is default



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:			
7	Region Order	Yes	53241 - is default
8	IFWI Build Version	Yes	32-bit value to use as the IFWI build version number.
9	Intel® Manifest Extension Utility Path	Yes	
10	Signing Tool	Yes	
11	Signing Tool Path	Yes	
12	Environment Variables		\$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

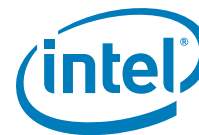


Table 2-3. - Flash Layout (Sheet 1 of 5)

Click on Flash Layout in the left tabs menu> Descriptor Region is expanded by default:															
<div> <div>▼ Descriptor Region</div> <div>1</div> <table> <tr> <th>Parameter</th><th>Value</th><th colspan="2"></th></tr> <tr> <td>OEM Section Binary</td><td></td><td colspan="2">This loads the OEM Sec</td></tr> </table> </div>				Parameter	Value			OEM Section Binary		This loads the OEM Sec					
Parameter	Value														
OEM Section Binary		This loads the OEM Sec													
#	Parameter	Platform	Settings												
1	Descriptor Region														
	<b>OEM Section Binary</b> This loads the OEM Section binary that will be merged into the output image generated by the Intel® FIT tool.	CML-V	OEM Binary (optional)												
Click on Flash Layout in the left tabs menu> BIOS Region is expanded by default:															
<div> <div>▼ BIOS Region</div> <div>2</div> <table> <tr> <th>Parameter</th><th>Value</th><th colspan="2">Help Text</th></tr> <tr> <td>Length</td><td>0</td><td colspan="2">-</td></tr> <tr> <td>BIOS Binary File</td><td></td><td colspan="2">This loads the BIOS binary that will be merged</td></tr> </table> </div>				Parameter	Value	Help Text		Length	0	-		BIOS Binary File		This loads the BIOS binary that will be merged	
Parameter	Value	Help Text													
Length	0	-													
BIOS Binary File		This loads the BIOS binary that will be merged													
#	Parameter	Platform	Settings												
2	BIOS Region														
	<b>Length</b> <b>Note:</b> This value will be automatically populated by Intel® FIT during image build.														
	<b>BIOS Binary File</b> 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-V	biosimage.bin												
Click on Flash Layout in the left tabs menu> Intel® CSME Region is expanded by default:															



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

▼ Ifwi: Intel(R) Me and Pmc Region <span style="background-color: red; color: white; border-radius: 50%; padding: 2px 5px;">3</span>			
Parameter	Value	Help Text	
Intel(R) ME Binary File		This loads the Intel(R) ME binary that will be merged in	
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 load	
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		-	

#	Parameter	Platform	Settings
<span style="background-color: red; color: white; border-radius: 50%; padding: 2px 5px;">3</span>	IFWI: Intel® ME and PMC Region		
	<b>Intel® ME Binary File</b> Navigate to your <b>Source Directory</b> (as specified in <a href="#">Table 2-2</a> ) 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. <b>Note:</b> You may choose to build the Intel® CSME Region only. To do so, the <b>Number of Flash Components in Flash Settings&gt; Flash Components</b> must be set to 0. <b>Note:</b> If loading meimage.bin file, check that the ME region is enabled in tool before building image.	CML-V	meimage.bin
	<b>Major Version</b> - This displays Major revision number of the currently loaded Intel® ME binary.		
	<b>Minor Version</b> - This displays Minor revision number of the currently loaded Intel® ME binary.		
	<b>Hotfix Version</b> - This displays Hot-Fix revision number of the currently loaded Intel® ME binary.		
	<b>Build Version</b> - This displays Build version number of the currently loaded Intel® ME binary.		
	<b>Chipset Initialization Version</b> - This displays the current Chipset Initialization version contained in the currently loaded Intel® ME binary.		



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

	<b>Chipset Initialization Binary</b> - 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.  <b>Note:</b> 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-V	Chipset.bin (Optional)
	<b>Chipset Init Override Version</b> - This displays the version of the Chipset Initialization Binary override if specified.		
	<b>PMC Binary File</b> - This loads the PMC binary that will be merged into the output image generated by the Intel® FIT tool.	CML-V	PMC.bin
	<b>Version</b> - This displays the version of PMC		
Click on Flash Layout in the left tabs menu> Ec Region is expanded by default:			
▼ EC Region <span style="background-color: red; color: white; border-radius: 50%; padding: 2px 5px;">4</span>			
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
<span style="background-color: red; color: white; border-radius: 50%; padding: 2px 5px;">4</span>	EC Region		
	<b>Length</b> <b>Note:</b> This value will be automatically populated by Intel® FIT during image build.		
	<b>EC Binary File</b> 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-V	EC Binary
	<b>EC Region Enable</b> <b>Values: Enabled/Disabled</b> This option allows the user to enable or disable the Embedded Controller data region.	CML-V	Enabled
	<b>EC Region Pointer File</b> This loads a binary file containing the 16 byte Embedded Controller pointer value at the start of the flash descriptor	CML-V	Pointer Binary
Click on Flash Layout in the left tabs menu> Gbe Region is expanded by default:			

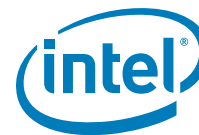


Table 2-3. - Flash Layout (Sheet 4 of 5)

▼ GbE Region <span>5</span>			
Parameter	Value	Help Text	
Length	0	-	
GbE Binary File		This loads the Intel(R) Integrated LAN binary that will be	
GbE Region Enable	Enabled	This option allows the user to enable or disable the Giga	
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
<span>5</span>	GbE Region		
	Length Note: This value will be automatically populated by Intel® FIT during image build.		
	GbE Binary File Navigate to your <b>Source Directory</b> (as specified in <a href="#">Table 2-2</a> ) and switch to the GbE subdirectory. Choose the appropriate Intel GbE LAN Firmware binary image. <b>If not using Intel LAN then load the GbE image before disabling the region along with changing additional settings below.</b> 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-V	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 <b>does not include the GbE LAN</b> 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-V	Enabled
Click on Flash Layout in the left tabs menu> PDR Region is expanded by default:			
▼ PDR Region <span>6</span>			
Parameter	Value	Help Text	
Length	0	-	
PDR Binary File		This loads the Platform Data region binary the	
PDR Region Enable	Disabled	This option allows the user to enable or disab	
#	Parameter	Platform	Settings



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

<b>6</b>	<b>PDR Region</b> Region is disabled by default. Displays Region size information when <b>Binary input file</b> is specified.		
	<b>Length</b> <b>Note:</b> This value will be automatically populated by Intel® FIT during image build.		
	<b>PDR Binary File</b> Navigate to path to load pdrimage.bin file if required and available. This loads the Platform Data region binary that will be merged into the output image generated by the Intel® FIT tool.	CML-V	PDR.bin (Optional)
	<b>PDR Region Enable</b> <b>Values: Enabled/Disabled</b> - This option allows the user to enable or disable the Platform Data Region. <b>Note:</b> If loading PDR.bin file, check that the PDR region is enabled in tool before building image.	CML-V	Disabled

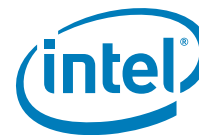


Table 2-4. - Flash Settings (Sheet 1 of 9)

Click on Flash Settings in the left tabs menu> Flash Components is expanded by default:			
<div> <div>▼ Flash Components</div> <div>1</div> </div>			
Parameter	Value		
Number of Flash Components	1	Specifies the number of Flash components	
Flash component 1 Size	16MB	This field identifies the size of the 1st Flash component	
Flash component 2 Size	8MB	This field identifies the size of the 2nd Flash component	
SPI Global Protected Range	0x0	Sets the default value of the Global Protected Range register in the SPI Flash Controller.	
SPI Idle to Deep Power Down Timeout Default	0x5	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.	
SPI Out of Order operation Enabled	Yes	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.	
SPI Resume Hold-off Delay	4us	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.	
SPI Max write / erase Resume to Suspend intervals	No Ceiling	This setting specifies the maximum value for the write and erase Resume to Suspend intervals.	
SPI Suspend / Resume Enabled	Yes	When this setting is enabled writes and erases will be allowed while the device is in suspend.	
SPI Software Binding Enabled	No	When enabled this settings will allow for SPI software binding.	
#	Parameter	Platform	Settings
1	Flash Components		
	<b>Number of Components</b> Values: 0, 1, 2 - This setting configures the total number of flash components for the platform. <b>Note:</b> Choosing a selection of '0' part will cause the Intel® FIT tool to build an output image containing only the Intel® CSME region.	CML-V	1
	<b>Flash component 1 Size</b> Values: 512KB, 1MB, 2MB, 4MB, 8MB, 16MB, 32MB, 64MB - This setting determines the size of Flash component 1 for the platform image.	CML-V	16MB 16MB
	<b>Flash component 2 Size</b> Values: 512KB, 1MB, 2MB, 4MB, 8MB, 16MB, 32MB, 64MB - This setting determines the size of Flash component 2 for the platform image. <b>Note:</b> This setting is only applicable when the Number of Flash Components option is set to '2'.	CML-V	Greyed Out
	<b>SPI Global Protected Range</b> - This sets the default value of the Global Protected Range register in the SPI Flash Controller.	CML-V	0x0
	<b>SPI Idle to Deep Power Down Timeout</b> - 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-V	0x5
	<b>SPI Out of Order operation Enabled</b> - 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-V	Yes
	<b>SPI Resume Hold-off Delay</b> - 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-V	4us
	<b>SPI Max write / erase Resume to Suspend intervals</b> - This setting specifies the maximum value for the write and erase Resume to Suspend intervals.	CML-V	No Ceiling

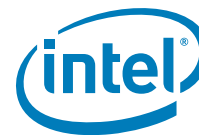


Table 2-4. - Flash Settings (Sheet 2 of 9)

	<b>SPI Suspend / Resume Enabled</b> - 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-V	Yes
	<b>SPI Software Binding Enabled</b> - When enabled this settings will allow for SPI re-binding to a new PCH during re-manufacturing flows.	CML-V	No
Click on Flash Layout in the left tabs menu> BIOS Region is expanded by default:			
<div> <div>▼ Host CPU / BIOS Master Access</div> <div>2</div> </div>			
Parameter		Value	
Host CPU / BIOS Write Access Intel Recommended		0xFFFF	This setting determines write access control for the BIOS region.
Host CPU / BIOS Write Access Custom		0x0000	This setting determines write access control for the BIOS region.
Host CPU / BIOS Read Access Intel Recommended		0xFFFF	This setting determines read access control for the BIOS region.
Host CPU / BIOS Read Access Custom		0x0000	This setting determines read access control for the BIOS region.
#	Parameter	Platform	Settings
2	Host CPU / BIOS Master Access		
	<b>Host CPU / BIOS Write Access Intel Recommended</b> <b>Values:</b> 0xFFFF, 0x000A, 0x001A, 0x010A, 0x011A - This setting determines write access control for the BIOS region. <b>0xFFFF</b> = Debug/Manufacturing <b>0x000A</b> = Production <b>0x001A</b> = Production with access to PDR (should ONLY be used if PDR region is implemented). <b>0x010A</b> = Production with access to EC <b>0x011A</b> = Production with access to EC and PDR <b>Custom</b> = User custom Host / BIOS Write Access values  For further details on Region Access Control see Comet Lake LP SPI Programming guide further details.	CML-V	0xFFFF
	<b>Host CPU / BIOS Write Access Custom</b> - This setting allows free form user customized Host CPU / BIOS Write Access regions permissions  <b>Note:</b> This setting is grayed out unless Custom is selected under the Host CPU / BIOS Write Access Intel Recommended drop down menu.  <b>Warning:</b> Setting region access permission values outside of Intel recommendation could result in compromised platform security	CML-V	Hex Input
	<b>Host CPU / BIOS Read Access</b> <b>Values:</b> 0xFFFF, 0x000F, 0x001F, 0x010F, 0x011F - This setting determines read access control for the BIOS region. <b>0xFFFF</b> = Debug/Manufacturing <b>0x000F</b> = Production <b>0x001F</b> = Production with access to PDR (should ONLY be used if PDR region is implemented). <b>0x010F</b> = Production with access to EC <b>0x011F</b> = Production with access to EC and PDR <b>Custom</b> = User custom Host / BIOS Read Access values  For further details on Region Access Control see Comet Lake LP SPI Programming guide.	CML-V	0xFFFF

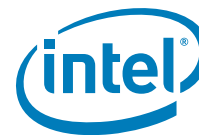


Table 2-4. - Flash Settings (Sheet 3 of 9)

	<b>Host CPU / BIOS Read Access Custom</b> - This setting allows free form user customized Host CPU / BIOS Read Access regions permissions  <b>Note:</b> This setting is grayed out unless Custom is selected under the Host CPU / BIOS Read Access Intel Recommended drop down menu.  <b>Warning:</b> Setting region access permission values outside of Intel recommendation could result in compromised platform security	CML-V	Hex Input
Click on Flash Settings in the left tabs menu> Intel® CSME Master Access is expanded by default:			
<b>Intel(R) ME Master Access</b> <span style="background-color: red; color: white; border-radius: 50%; padding: 2px 5px;">3</span>			
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
<span style="background-color: red; color: white; border-radius: 50%; padding: 2px 5px;">3</span>	Intel® ME Master Access		
	<b>Intel® ME Write Access Intel Recommended</b> <b>Values: 0xFFFF, 0x0004</b> - This setting determines write access control for the Intel® CSME region. <b>0xFFFF</b> = Debug/Manufacturing <b>0x0004</b> = Production <b>0x000C</b> = Production <b>Custom</b> = User custom Intel® ME Write Access values  For further details on Region Access Control see Comet Lake LP SPI Programming guide further details.	CML-V	0xFFFF
	<b>Intel® ME Write Access Custom</b> - This setting allows free form user customized Intel® ME Write Access regions permissions  <b>Note:</b> This setting is grayed out unless Custom is selected under the Intel® ME Write Access Intel Recommended drop down menu.  <b>Warning:</b> Setting region access permission values outside of Intel recommendation could result in compromised platform security	CML-V	Hex Input
	<b>Intel® ME Read Access Intel Recommended</b> <b>Values: 0xFFFF, 0x000D</b> - This setting determines read access control for the Intel® CSME region. <b>0xFFFF</b> = Debug/Manufacturing <b>0x000D</b> = Production <b>Custom</b> = User custom Intel® ME Read Access values  For further details on Region Access Control see Comet Lake LP SPI Programming guide further details.	CML-V	0xFFFF

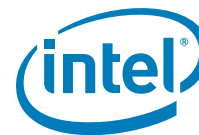


Table 2-4. - Flash Settings (Sheet 4 of 9)

	<b>Intel® ME Read Access Custom</b> - This setting allows free form user customized Intel® ME Read Access regions permissions  <b>Note:</b> This setting is grayed out unless Custom is selected under the Intel® ME Read Access Intel Recommended drop down menu.  <b>Warning:</b> Setting region access permission values outside of Intel recommendation could result in compromised platform security	CML-V	Hex Input
Click on Flash Settings in the left tabs menu> GbE Master Access is expanded by default:			
<b>▼ GbE Master Access</b> <div>4</div>			
Parameter	Value	Help To	
GbE Write Access Intel Recommended	0xFFFF	This setting determines write access control for the GbE region	
GbE Write Access Custom	0x0000	This setting determines read access control for the GbE region	
GbE Read Access Intel Recommended	0xFFFF	This setting determines read access control for the GbE region	
GbE Read Access Custom	0x0000	This setting determines read access control for the GbE region	
#	Parameter	Platform	Settings
4	GbE Master Access		
	<b>GbE Write Access Intel Recommended</b> <b>Values: 0xFFFF, 0x0008</b> - This setting determines write access control for the Gigabit Ethernet Region. <b>0xFFFF</b> = Debug/Manufacturing <b>0x0008</b> = Production <b>Custom</b> = User custom GbE Write Access values  For further details on Region Access Control see Comet Lake LP SPI Programming guide further details.	CML-V	0xFFFF
	<b>GbE Write Access Custom</b> - This setting allows free form user customized GbE Write Access regions permissions  <b>Note:</b> This setting is grayed out unless Custom is selected under the GbE Write Access Intel Recommended drop down menu.  <b>Warning:</b> Setting region access permission values outside of Intel recommendation could result in compromised platform security	CML-V	Hex Input
	<b>GbE Read Access Intel Recommended</b> <b>Values: 0xFFFF, 0x0009</b> - This setting determines read access control for the Gigabit Ethernet Region. <b>0xFFFF</b> = Debug/Manufacturing <b>0x0009</b> = Production <b>Custom</b> = User custom GbE Read Access values  For further details on Region Access Control see Comet Lake LP SPI Programming guide further details.	CML-V	0xFFFF



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

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



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

	<b>EC Read Access Custom</b> - This setting allows free form user customized EC Read Access regions permissions  <b>Note:</b> This setting is grayed out unless Custom is selected under the EC Read Access Intel Recommended drop down menu.  <b>Warning:</b> Setting region access permission values outside of Intel recommendation could result in compromised platform security	CML-V	Hex Input
Click on Flash Layout in the left tabs menu> IUnit Sub-Partition is expanded by default:			
<div> <div>Flash Configuration</div> <div>6</div> </div>			
Parameter	Value	Help Text	
Dual I/O Read Enable	No	This soft-strap only has effect if Dual I/O Read is discovered as supported	
Dual Output Read Enable	No	This soft-strap only has effect if Dual Output Read is discovered as supported	
Fast Read Clock Frequency	48MHz	This setting allows customers to configure the flash component clock frequency	
Fast Read Supported	Yes	This setting allows customers to enable support for Fast Read capabilities	
Invalid Instruction 0	0x21	This setting allows customers to configure invalid instruction to protect	
Invalid Instruction 1	0x42	This setting allows customers to configure invalid instruction to protect	
Invalid Instruction 2	0x60	This setting allows customers to configure invalid instruction to protect	
Invalid Instruction 3	0xAD	This setting allows customers to configure invalid instruction to protect	
Invalid Instruction 4	0xB7	This setting allows customers to configure invalid instruction to protect	
Invalid Instruction 5	0xB9	This setting allows customers to configure invalid instruction to protect	
Invalid Instruction 6	0xC4	This setting allows customers to configure invalid instruction to protect	
Invalid Instruction 7	0xC7	This setting allows customers to configure invalid instruction to protect	
Quad I/O Read Enable	No	This soft-strap only has effect if Quad I/O Read is discovered as supported	
Quad Output Read Enable	No	This soft-strap only has effect if Quad Output Read is discovered as supported	
Read ID and Read Status Clock Frequency	48MHz	This setting allows customers to configure the flash component clock frequency	
Write and Erase Clock Frequency	48MHz	This setting allows customers to configure the flash component clock frequency	
#	Parameter	Platform	Settings
6	Flash Configuration		
	<b>Dual I/O Read Enabled</b> <b>Values: Yes/No</b> - This setting allows the customer to enable support for Dual I/O Read capabilities for flash components. See Comet Lake V SPI Programming guide for further details.	CML-V	Yes
	<b>Dual Output Read Enabled</b> <b>Values: Yes/No</b> - This setting allows the customer to enable support for Dual Output Read capabilities for flash components. See Comet Lake V SPI Programming guide for further details.	CML-V	Yes
	<b>Fast Read Clock Frequency</b> <b>Values: 17MHz, 30MHz, 48MHz</b> - This setting allows the customer to configure the flash component clock frequency setting for Fast Read. See Comet Lake V SPI Programming guide for further details.	CML-V	48MHz

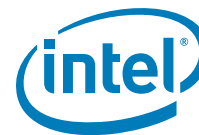


Table 2-4. - Flash Settings (Sheet 7 of 9)

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



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

Legacy VSCC Table

7

VSCC Entries

8

W25Q128BV

9

Add VSCC Entry

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

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

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

Bios Configuration

10

Parameter	Value	Help Text
Top Swap Block Size	64KB	This configures the Top Swap Block size for the platform.

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



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

10	BIOS Configuration														
	<b>Top Swap Block Size</b> Values: 64KB, 128KB, 256KB, 512KB, 1MB - This configures the Top Swap Block size for the platform. For further details see Comet Lake V Platform Controller Hub EDS.	CML-V	128KB												
Click on Flash Settings in the left tabs menu > OEM and Platform IDs															
▼ OEM and Platform IDs 11															
<table border="1"> <thead> <tr> <th>Parameter</th><th>Value</th><th colspan="2">Help Text</th></tr> </thead> <tbody> <tr> <td>OEM Vendor ID</td><td>0x0</td><td colspan="2">This setting allows OEMs to configure their Unique</td></tr> <tr> <td>OEM Platform ID</td><td>0x0</td><td colspan="2">This setting allows OEMs to configure a Unique Pla</td></tr> </tbody> </table>				Parameter	Value	Help Text		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	Value	Help Text													
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													
11	<b>OEM Vendor ID</b> - This is a free form 32bit field that allows the OEM to configure their unique Vendor identifier in the firmware image.	CML-V	0x0												
	<b>OEM Platform ID</b> - This is a free form 32bit field that allows the OEM to configure their unique platform identifier in the firmware image.	CML-V	0x0												
Click on Flash Settings in the left tabs menu> BIOS Configuration is expanded by default:															
▼ FPF Configuration 12															
<table border="1"> <thead> <tr> <th>Parameter</th><th>Value</th><th colspan="2">Help Text</th></tr> </thead> <tbody> <tr> <td>FPF Hardware Binding Enabled</td><td>Disabled</td><td colspan="2">This setting configures the FPF Hardware bi</td></tr> </tbody> </table>				Parameter	Value	Help Text		FPF Hardware Binding Enabled	Disabled	This setting configures the FPF Hardware bi					
Parameter	Value	Help Text													
FPF Hardware Binding Enabled	Disabled	This setting configures the FPF Hardware bi													
12	FPF Configuration														
	<b>FPF Hardware Binding Enabled</b> 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.  <b>Note:</b> For Revenue parts this setting will be ignored and FPF Hardware binding will take place when close manufacturing flow is executed.	CML-V	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:			
<div> <div>▼ Processor</div> <div>1</div> </div>			
Parameter		Value	Help Text
Processor Emulation		No Emulation	-
Missing Processor Detection Alert		No	-
#	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-V	No Emulation No Emulation
	Missing Processor Detection Alert Values: Yes / No This setting determines if missing processor detection is enabled on Desktop / Workstation platforms. <b>Note:</b> This feature will only work if appropriate glue logic is present.	CML-V	No
Click on Intel® ME Kernel in the left tabs menu> Intel® CSME Firmware Update is expanded by default:			
<div> <div>▼ Intel (R) ME Firmware Update</div> <div>2</div> </div>			
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® CSME Firmware Update		
	<b>Firmware Update OEM ID</b> - 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-V	0 string



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

	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-V	No								
	Intel® ME Region Flash Protection Override Values: Yes/No - This setting enables descriptor unlock of the Intel® CSME Region when the HMRFP0 message is sent to firmware prior to BIOS End of POST.	CML-V	Yes								
Click on Intel® ME Kernel in the left tabs menu> Image Identification is expanded by default:											
<div> <div>▼ Image Identification</div> <div>3</div> </div>											
<table> <tr> <th>Parameter</th><th>Value</th><th colspan="2">Help Text</th></tr> <tr> <td>OEM Tag</td><td>0x00000000</td><td colspan="2">-</td></tr> </table>				Parameter	Value	Help Text		OEM Tag	0x00000000	-	
Parameter	Value	Help Text									
OEM Tag	0x00000000	-									
#	Parameter	Platform	Settings								
3	Image Identification										
	OEM Tag - This is a free form 32bit field that allows the OEM to configure their own unique identifier in the firmware image.	CML-V	0x00000000								
Click on Intel® CSME Kernel in the left tabs menu> Firmware Diagnostics is expanded by default:											
<div> <div>▼ Firmware Diagnostics</div> <div>4</div> </div>											
<table> <tr> <th>Parameter</th><th>Value</th><th colspan="2">Help Text</th></tr> <tr> <td>Automatic Built in Self Test</td><td>Disabled</td><td colspan="2">-</td></tr> </table>				Parameter	Value	Help Text		Automatic Built in Self Test	Disabled	-	
Parameter	Value	Help Text									
Automatic Built in Self Test	Disabled	-									
#	Parameter	Platform	Settings								
4	Firmware Diagnostics										
	Automatic Built in Self Test Values: Enabled/Disabled This setting enables the firmware Automatic Built in Self Test which is executed during first platform boot after initial image flashing.	CML-V	Disabled								
Click on Intel® CSME Kernel in the left tabs menu> Post Manufacturing Lock is expanded by default:											
<div> <div>▼ Post Manufacturing Lock</div> <div>5</div> </div>											
<table> <tr> <th>Parameter</th><th>Value</th><th colspan="2">Help Text</th></tr> <tr> <td>Post Manufacturing NVAR Configuration Enabled</td><td>Yes</td><td colspan="2">This setting determines if modifications to Cust</td></tr> </table>				Parameter	Value	Help Text		Post Manufacturing NVAR Configuration Enabled	Yes	This setting determines if modifications to Cust	
Parameter	Value	Help Text									
Post Manufacturing NVAR Configuration Enabled	Yes	This setting determines if modifications to Cust									
#	Parameter	Platform	Settings								
5	Post Manufacturing Lock										

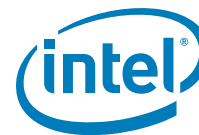


Table 2-5. - Intel® ME Kernel (Sheet 3 of 4)

	Post Manufacturing NVAR Configuration Enabled - This setting determines if modifications to Customer configurable NVARs is to be allowed after close of manufacturing.	CML-V	Yes
Click on Intel® CSME Kernel in the left tabs menu> MCTP Configuration is expanded by default:			
<div> <div>▼ MCTP Configuration</div> <div>6</div> </div>			
Parameter	Value	Help Text	
MCTP Stack Configuration	0x920030	Defines the ME's 8-bits MCTP Endpoint IDs for each SMBus physical interface (SMBus, ...	
MctpDevicePortEc	0x02	-	
MctpDevicePortSio	0x00	-	
MctpDevicePortIsh	0x00	-	
MctpDevicePortBmc	0x00	-	
#	Parameter	Platform	Settings
6	MCTP Configuration		
	<b>MCTP Stack Configuration</b> Defines the Intel® CSME'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-V	0x920030
	MctpDevicePortEc	CML-V	0x02
	MctpDevicePortSio	CML-V	0x00
	MctpDevicePortIsh	CML-V	0x00
	MctpDevicePortBmc	CML-V	0x00
Click on Intel® ME Kernel in the left tabs menu> Intel® ME Boot Configuration is expanded by default:			
<div> <div>▼ Intel (R) ME Boot Configuration</div> <div>7</div> </div>			
Parameter	Value	Help Text	
Persistent PRTC Backup Power	Exists	FPF that indicates if the device is designed such	
#	Parameter	Platform	Settings
7	Intel® ME Boot Configuration		
	<b>Persistent PRTC Backup Power</b> <b>Values: None / Exists</b> 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-V	Exists
Click on Intel® CSME Kernel in the left tabs menu> Reserved is expanded by default:			



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

▼ Reserved <span>8</span>			
Parameter	Value	Help Text	
Reserved	No	-	

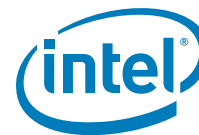


Table 2-6. - Intel® AMT (Sheet 1 of 7)

Click on Intel® AMT in the left tabs menu> Intel® AMT is expanded by default:			
<div> <div>Intel(R) AMT Configuration</div> <div>1</div> </div>			
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 permanently 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		
	<b>Intel® AMT Supported</b> <b>Values: Yes/No</b> - This setting allows customers to disable Intel® AMT on the platform and force the platform into Standard Manageability mode. <b>Note:</b> 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-V	No No
	<b>Intel® CSME Network Services Supported</b> <b>Values: Yes/No</b> - This setting allows customers to enable / disable Intel® CSME Network Services on the platform. <b>Note:</b> 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-V	No No
	<b>Intel® Manageability Application Supported</b> <b>Values: Yes/No</b> - This setting allows customers to force Intel® AMT enabled platforms to operate in Standard Manageability mode. <b>Note:</b> This setting only applies to Desktop and Workstation platforms.	CML-V	No No
	<b>Manageability Application initial power-up state</b> <b>Values: Enabled/Disabled</b> This setting allows customers to determine the power up state for Intel® AMT or Standard Manageability. <b>Note:</b> If this setting is disabled Intel® AMT or Standard Manageability can still be re-enabled through the Intel® CSMEBx interface.	CML-V	Disabled Disabled
	<b>Intel® AMT Idle Timeout</b> <b>Values: 0xFFFF</b> - This setting configures the idle timeout value before Intel® AMT enters into an off state.	CML-V	0xFFFF
	<b>Intel® AMT Watchdog Automatic Reset Enabled</b> <b>Values: Yes/No</b> - This setting allows customers to enable the Intel® CSME firmware to trigger an automatic platform reset if either the MEI or Agent Presence are in a hung state. <b>Note:</b> 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-V	No No
Click on Intel® AMT in the left tabs menu> KVM Configuration is expanded by default:			
<div> <div>KVM Configuration</div> <div>2</div> </div>			
Parameter	Value	Help Text	
Firmware KVM Screen Blanking	No	-	
KVM Redirection Supported	Yes	-	

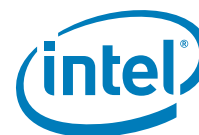


Table 2-6. - Intel® AMT (Sheet 2 of 7)

#	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-V													
	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-V													
Click on Intel® AMT in the left tabs menu> Provisioning Configuration is expanded by default:															
▼ Provisioning Configuration 3															
<table><tr><th>Parameter</th><th>Value</th><th>Help Text</th></tr><tr><td>Embedded Host Based Config...</td><td>No</td><td>-</td></tr><tr><td>PKI Domain Name Suffix</td><td></td><td>-</td></tr></table>				Parameter	Value	Help Text	Embedded Host Based Config...	No	-	PKI Domain Name Suffix		-			
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-V	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-V	-												
Click on Intel® AMT in the left tabs menu> OEM Customizable Certificate 1 is expanded by default:															
▼ OEM Customizable Certificate 1 4															
<table><tr><th>Parameter</th><th>Value</th><th>Help Text</th></tr><tr><td>Certificate Enabled</td><td>No</td><td>This setting allows customers to enable PKI provisioning Custo...</td></tr><tr><td>Certificate Friendly Name</td><td></td><td>This setting allows customers to assign a user friendly name for...</td></tr><tr><td>Certificate Stream</td><td></td><td>This setting allows customers to input hash stream for PKI provi...</td></tr></table>				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	Value	Help Text													
Certificate Enabled	No	This setting allows customers to enable PKI provisioning Custo...													
Certificate Friendly Name		This setting allows customers to assign a user friendly name for...													
Certificate Stream		This setting allows customers to input hash stream for PKI provi...													
#	Parameter	Platform	Settings												
4	OEM Customizable Certificate 1														
	Certificate Enabled Values: Yes/No - This setting allows customers to enable PKI provisioning Custom Certificate 1.	CML-V	No												



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

	<b>Certificate Friendly Name</b> - This setting allows customers to assign a user friendly name for PKI provisioning Custom Certificate 1. Maximum of 32 characters.	CML-V	-
	<b>Certificate Stream</b> - 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. <b>Note:</b> If the platform is un-configured the Custom Certificate Hash will be deleted.	CML-V	-

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

▼ OEM Customizable Certificate 25

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

#	Parameter	Platform	Settings
5	OEM Customizable Certificate 2		
	<b>Certificate Enabled</b> <b>Values: Yes/No</b> - This setting allows customers to enable PKI provisioning Custom Certificate 2.	CML-V	No
	<b>Certificate Friendly Name</b> - This setting allows customers to assign a user friendly name for PKI provisioning Custom Certificate 2. Maximum of 32 characters.	CML-V	-
	<b>Certificate Stream</b> - 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. <b>Note:</b> If the platform is un-configured the Custom Certificate Hash will be deleted.	CML-V	-

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

▼ OEM Customizable Certificate 36

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

#	Parameter	Platform	Settings
6	OEM Customizable Certificate 3		
	<b>Certificate Enabled</b> <b>Values: Yes/No</b> - This setting allows customers to enable PKI provisioning Custom Certificate 3.	CML-V	No
	<b>Certificate Friendly Name</b> - This setting allows customers to assign a user friendly name for PKI provisioning Custom Certificate 3. Maximum 32 characters.	CML-V	-
	<b>Certificate Stream</b> - 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. <b>Note:</b> If the platform is un-configured the Custom Certificate Hash will be deleted.	CML-V	-

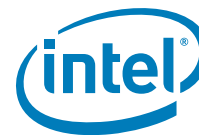


Table 2-6. - Intel® AMT (Sheet 4 of 7)

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

▼ OEM Default Certificate 1

7

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

#	Parameter	Platform	Settings
7	OEM Default Certificate 1		
	<b>Certificate Enabled</b> <b>Values: Yes/No</b> - This setting allows customers to enable PKI provisioning Default certificate 1.	CML-V	No
	<b>Certificate Friendly Name</b> - This setting allows customers to assign a user friendly name for PKI provisioning Default Certificate 1. Maximum 32 characters.	CML-V	-
	<b>Certificate Stream</b> - This setting allows customers to input hash stream for PKI provisioning custom certificate 1. <b>Note:</b> 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-V	-

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		
	<b>Certificate Enabled</b> <b>Values: Yes/No</b> - This setting allows customers to enable PKI provisioning Default certificate 2.	CML-V	No
	<b>Certificate Friendly Name</b> - This setting allows customers to assign a user friendly name for PKI provisioning Default Certificate 2. Maximum 32 characters.	CML-V	-
	<b>Certificate Stream</b> - This setting allows customers to input hash stream for PKI provisioning custom certificate 2. <b>Note:</b> 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-V	-

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



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

▼ OEM Default Certificate 3 <span>9</span>			
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
<span>9</span>	OEM Default Certificate 3		
	<b>Certificate Enabled</b> <b>Values: Yes/No</b> - This setting allows customers to enable PKI provisioning Default certificate 3.	CML-V	No
	<b>Certificate Friendly Name</b> - This setting allows customers to assign a user friendly name for PKI provisioning Default Certificate 3. Maximum 32 characters.	CML-V	-
	<b>Certificate Stream</b> - This setting allows customers to input hash stream for PKI provisioning custom certificate 3. <b>Note:</b> 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-V	-
Click on Intel® AMT in the left tabs menu> OEM Default Certificate 4 is expanded by default:			
▼ OEM Default Certificate 4 <span>10</span>			
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
<span>10</span>	OEM Default Certificate 4		
	<b>Certificate Enabled</b> <b>Values: Yes/No</b> - This setting allows customers to enable PKI provisioning Default certificate 4.	CML-V	No
	<b>Certificate Friendly Name</b> - This setting allows customers to assign a user friendly name for PKI provisioning Default Certificate 4.	CML-V	-
	<b>Certificate Stream</b> - This setting allows customers to input hash stream for PKI provisioning custom certificate 4. <b>Note:</b> 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-V	-
Click on Intel® AMT in the left tabs menu> OEM Default Certificate 5 is expanded by default:			

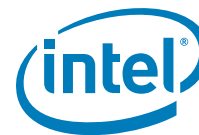


Table 2-6. - Intel® AMT (Sheet 6 of 7)

▼ OEM Default Certificate 5 <span>11</span>			
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
<span>11</span>	OEM Default Certificate 5		
	<b>Certificate Enabled</b> Values: Yes/No - This setting allows customers to enable PKI provisioning Default certificate 5.	CML-V	No
	<b>Certificate Friendly Name</b> - This setting allows customers to assign a user friendly name for PKI provisioning Default Certificate 5.	CML-V	-
	<b>Certificate Stream</b> - This setting allows customers to input hash stream for PKI provisioning custom certificate 5. <b>Note:</b> 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-V	-
Click on Intel® AMT in the left tabs menu> Redirection Configuration is expanded by default:			
▼ Redirection Configuration <span>12</span>			
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
<span>12</span>	Redirection Configuration		
	<b>Redirection Localized Language</b> - 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-V	English
	<b>Redirection Privacy / Security Level</b> - This setting allows customers to configure the Privacy and Security level for redirection operations. <b>Default</b> enables all redirection ports (User consent is configurable). <b>Enhanced</b> - Enables all redirection ports. (User consent is required and cannot be disabled). <b>Extreme</b> - Disables Redirection and Remote Configuration / Client Control Mode. <b>Note:</b> 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-V	Default
Click on Intel® AMT in the left tabs menu> TLS Configuration is expanded by default:			

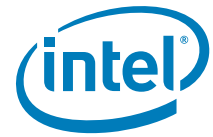


Table 2-6. - Intel® AMT (Sheet 7 of 7)

▼ TLS Configuration <span>13</span>			
Parameter	Value	Help Text	
Transport Layer Security Supp...	Yes	This setting allows customers to enable / disable firmware Trans...	

#	Parameter	Platform	Settings
13	TLS Configuration		
	<b>Transport Layer Security Supported</b> <b>Values: Yes/No</b> - This setting allows customers to enable / disable firmware Transport Layer Security support. <b>Note:</b> 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-V	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:																							
<div> <div>▼ Content Protection</div> <div>1</div> </div>																							
<table> <tr> <th>Parameter</th><th>Value</th><th colspan="2">Help 1</th></tr> <tr> <td>PAVP Supported</td><td>Yes</td><td colspan="2">This setting determines if the Protec</td></tr> <tr> <td>LSPCON Internal Display Port 1 - LSPCON / 4K</td><td>None</td><td colspan="2">This setting determines which port f</td></tr> <tr> <td>HDCP Internal Display Port 1 - 5K</td><td>None</td><td colspan="2">This setting determines which port</td></tr> <tr> <td>HDCP Internal Display Port 2 - 5K</td><td>None</td><td colspan="2">This setting determines which port</td></tr> </table>				Parameter	Value	Help 1		PAVP Supported	Yes	This setting determines if the Protec		LSPCON Internal Display Port 1 - LSPCON / 4K	None	This setting determines which port f		HDCP Internal Display Port 1 - 5K	None	This setting determines which port		HDCP Internal Display Port 2 - 5K	None	This setting determines which port	
Parameter	Value	Help 1																					
PAVP Supported	Yes	This setting determines if the Protec																					
LSPCON Internal Display Port 1 - LSPCON / 4K	None	This setting determines which port f																					
HDCP Internal Display Port 1 - 5K	None	This setting determines which port																					
HDCP Internal Display Port 2 - 5K	None	This setting determines which port																					
#	Parameter	Platform	Settings																				
1	Content Protection																						
	<b>PAVP Supported</b> <b>Values: Yes/No</b> This setting determines if the Protected Audio Video Path (PAVP) feature will be permanently disabled in the FW image.	CML-V	Yes																				
	<b>LSPCON Internal Display Port 1 - LSPCON / 4K</b> <b>Values: None, Port B, Port C, Port D</b> This setting determines which port for LSPCON will be connected to HDCP 2.2 Bridge adapter Display 1.	CML-V	None																				
	<b>HDCP Internal Display Port 1 - 5K</b> <b>Values: None, Port A, Port B, Port C, Port D</b> This setting determines which port is connected for 5K output on the Internal Display 1. <b>Note:</b> Both Display Port 1 & 2 need to be configured for proper operation.	CML-V	PortA																				
	<b>HDCP Internal Display Port 2 - 5K</b> <b>Values: None, Port A, Port B, Port C, Port D</b> This setting determines which port is connected for 5K output on the Internal Display 2. <b>Note:</b> Both Display Port 1 & 2 need to be configured for proper operation.	CML-V	None																				
Click on Platform Protection in the left tabs menu> Graphics uController is expanded by default:																							
<div> <div>▼ Graphics uController</div> <div>2</div> </div>																							
<table> <tr> <th>Parameter</th><th>Value</th><th colspan="2">Help 1</th></tr> <tr> <td>GuC Encryption Key</td><td>00 00 00 00 00 00 00 00 00 00 ...</td><td colspan="2">This option is for entering the raw ha:</td></tr> </table>				Parameter	Value	Help 1		GuC Encryption Key	00 00 00 00 00 00 00 00 00 00 ...	This option is for entering the raw ha:													
Parameter	Value	Help 1																					
GuC Encryption Key	00 00 00 00 00 00 00 00 00 00 ...	This option is for entering the raw ha:																					
#	Parameter	Platform	Settings																				
2	Graphics UController																						
	<b>GuC Encryption Key</b> <b>Values:</b> This option is for entering the raw hash 256 bit string or certificate file for the Graphics uController.	CML-V	0x00000000																				

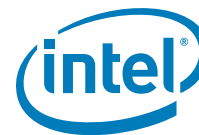


Table 2-7. - Platform Protection (Sheet 2 of 8)

Click on Platform Protection in the left tabs menu> Hash Key Configuration for Bootguard / ISH is expanded by default:			
<div> <div>▼ Hash Key Configuration for Bootguard / ISH</div> <div>3</div> </div>			
Parameter	Value	Help Text	
OEM Public Key Hash	00 00 00 00 00 00 00 00 00 00 ...	Raw hash string for the SHA-256 hash of the OEM pub	
OEM Key Manifest Binary		Signed manifest file containing hashes of keys used fo	
#	Parameter	Platform	
3	Hash Key Configuration for Bootguard / ISH		
	<b>OEM Public Key Hash</b> <b>Values:</b> 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-V	0x00000000
	<b>OEM Key Manifest Binary</b> 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-V	
Click on Platform Protection in the left tabs menu> Exclusion Ranges is expanded by default:			



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

<div> <div>▼</div> <div>Exclusion Ranges</div> <div>4</div> </div>			
Parameter	Value	Help	
Range 1 offset	0x800	Range 1 offset covers manifest, cannot be changed	
Range 1 size	0x400	Range 1 size covers manifest, cannot be changed	
Range 2 offset	0x80	Range 2 offset covers OEM defined unprotected range	
Range 2 size	0x20	Range 2 size covers OEM defined unprotected range length	
Range 3 offset	0x0	Range 3 offset covers OEM defined unprotected range start	
Range 3 size	0x0	Range 3 size covers OEM defined unprotected range length	
Range 4 offset	0x0	Range 4 offset covers OEM defined unprotected range start	
Range 4 size	0x0	Range 4 size covers OEM defined unprotected range length	
Range 5 offset	0x0	Range 5 offset covers OEM defined unprotected range start	
Range 5 size	0x0	Range 5 size covers OEM defined unprotected range length	
Range 6 offset	0x0	Range 6 offset covers OEM defined unprotected range start	
Range 6 size	0x0	Range 6 size covers OEM defined unprotected range length	
Range 7 offset	0x0	Range 7 offset covers OEM defined unprotected range start	
Range 7 size	0x0	Range 7 size covers OEM defined unprotected range length	
Range 8 offset	0x0	Range 8 offset covers OEM defined unprotected range start	
Range 8 size	0x0	Range 8 size covers OEM defined unprotected range length	

#	Parameter	Platform	
4	<b>Exclusion Ranges</b> 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-V	0x800
	Range 1 size	CML-V	0x400
	Range 2 offset	CML-V	0x80
	Range 2 size	CML-V	0x20
	Range 3 offset Values: This offset covers Range 3 OEM defined unprotected range start	CML-V	0x0
	Range 3 size Values: This offset covers Range 3 OEM defined unprotected range length	CML-V	0x0
	Range 4 offset Values: This offset covers Range 4 OEM defined unprotected range start	CML-V	0x0
	Range 4 size Values: This offset covers Range 4 OEM defined unprotected range length	CML-V	0x0
	Range 5 offset Values: This offset covers Range 5 OEM defined unprotected range start	CML-V	0x0

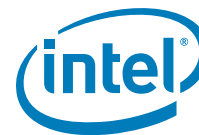


Table 2-7. - Platform Protection (Sheet 4 of 8)

	<b>Range 5 size</b> Values: This offset covers Range 5 OEM defined unprotected range length	CML-V	0x0
	<b>Range 6 offset</b> Values: This offset covers Range 6 OEM defined unprotected range start	CML-V	0x0
	<b>Range 6 size</b> Values: This offset covers Range 6 OEM defined unprotected range length	CML-V	0x0
	<b>Range 7 offset</b> Values: This offset covers Range 7 OEM defined unprotected range start	CML-V	0x0
	<b>Range 7 size</b> Values: This offset covers Range 7 OEM defined unprotected range length	CML-V	0x0
	<b>Range 8 offset</b> Values: This offset covers Range 8 OEM defined unprotected range start	CML-V	0x0
	<b>Range 8 size</b> Values: This offset covers Range 8 OEM defined unprotected range length	CML-V	0x0
Click on Platform Protection in the left tabs menu> Descriptor Configuration is expanded by default:			
<div> <div>▼ Descriptor Configuration</div> <div>5</div> </div>			
	<b>Parameter</b>	<b>Value</b>	<b>Help</b>
	Flash Descriptor Verification En...	No	-
	Descriptor Signing Key		This is the path to the private key used to sign th
	exclude master access in the si...	Yes	include/exclude master access in the signature.
#	Parameter	Platform	
5	Descriptor Configuration		
	<b>Flash Descriptor Verification Enabled</b> Value: Yes/No This settings enables / disables Flash Descriptor verification.	CML-V	No
	<b>Descriptor Signing Key</b> 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-V	None
	<b>exclude master access in the signature</b> Value: Yes/No This setting excludes the region master access values in the descriptor signature.	CML-V	Yes
Click on Platform Protection in the left tabs menu> Boot Guard Configuration is expanded by default:			

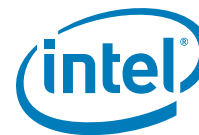


Table 2-7. - Platform Protection (Sheet 5 of 8)

▼ Boot Guard Configuration <b>6</b>			
Parameter	Value		
Key Manifest ID	0	ODM identifier used during the Key mani	
Boot Guard Profile Configuration	Boot Guard Profile 0 - No_FVME	Boot Guard Profile 0 - Legacy is for platf	
CPU Debugging	Enabled	This setting determines if CPU debug mc	
BSP Initialization	Enabled	This setting determines BSP behavior wh	
S3 Optimization	Enabled	This setting overrides Boot Guard S3 opt	

#	Parameter	Platform	Settings
<b>6</b>	Boot Guard Configuration		
	<b>Key Manifest ID</b> <b>Values:</b> This option is for entering the hash of another public key, used by the ACM to verify the Boot Policy Manifest.	CML-V	0x0
	<b>Boot Guard Profile Configuration</b> <b>Values:</b> 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-V	Boot Guard Profile 0 - No_FVME
	<b>CPU Debugging</b> <b>Values:</b> Enabled/Disabled This setting determines if CPU debug modes will be displayed. When set to 'Enabled' CPU debugging is enabled.	CML-V	Enabled
	<b>BSP Initialization</b> <b>Values:</b> 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-V	Enabled
	<b>S3 Optimization</b> <b>Values:</b> Enabled/Disabled This setting overrides Boot Guard S3 optimization.  <b>Note:</b> Used for testing only.	CML-V	Enabled

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

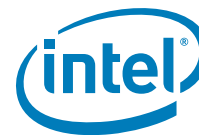


Table 2-7. - Platform Protection (Sheet 6 of 8)

▼ Intel(R) PTT Configuration <b>7</b>			
Parameter		Value	
Intel(R) PTT Supported		Yes	This setting permanently disables
Intel(R) PTT initial power-up state		Enabled	-
Intel(R) PTT Supported [FPF]		Yes	This setting will permanently disa
Intel(R) PTT RPMC Supported		No	This setting determines if RPMC is
Intel(R) PTT RPMC Rebinding Enabled		No	This setting determines if Rebindi
#	Parameter	Platform	Settings
<b>7</b>	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-V	Yes
	Intel® PTT Supported Values: Yes/No - This setting permanently disables Intel® PTT in the firmware image.	CML-V	Enabled
	Intel® PTT Supported [FPF] Values: Yes/No - This setting will permanently disable Intel® PTT through platform FPFs. <b>Caution:</b> Using this option will permanently disable Intel® PTT on the platform hardware.	CML-V	Yes
	Intel® PTT RPMC Supported Values: Yes/No - This setting determines if RPMC is enabled for Intel® PTT.  <b>Note:</b> The SPI parts being used need to support RPMC in order to use this feature.	CML-V	No
	Intel® PTT RPMC Rebinding Enabled Values: Yes/No - This setting determines if Rebinding of RPMC enabled SPI parts is supported.	CML-V	No
Click on Platform Protection in the left tabs menu> TPM Over SPI Bus Configuration is expanded by default:			
▼ TPM Over SPI Bus Configuration <b>8</b>			
Parameter		Value	
TPM Clock Frequency		17MHz	This setting determines the clock frequency setting to be used fo...
TPM Over SPI Bus Enabled		No	This setting determines if TPM over SPI bus is enabled on the pl...
#	Parameter	Platform	Settings
<b>8</b>	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-V	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-V	Yes
Click on Platform Protection in the left tabs menu> BIOS Guard Configuration is expanded by default:			
▼ BIOS Guard Configuration 9			
Parameter		Value	
BIOS Guard Protection Override Enabled		No	This setting allows BIOS G
#	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-V	Yes
Click on Platform Protection in the left tabs menu> TXT Configuration is expanded by default:			
▼ TXT Configuration 10			
Parameter		Value	Help Text
TXT Supported		No	This setting determines is enabled for the platform.
#	Parameter	Platform	Settings
10	TXT Configuration		
	TXT Supported This setting determines if enabled for the platform.	CML-V	No
Click on Platform Protection in the left tabs menu> TXT Configuration is expanded by default:			
▼ Crypto Hardware Support 11			
Parameter		Value	
Crypto HW Support		Yes	This setting can be used to disable crypto
#	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.	CML-V	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 <span>12</span>			
Parameter		Value	Help
Enable TDS Capabilities		No	This setting enables Intel(R) Trusted Device Setup
#	Parameter	Platform	Settings
<span>12</span>	Platform Trusted Device Setup Support		
	Enable TDS Capabilities Values: Yes / No This setting enables Intel® Trusted Device Setup on the platform	CML-V	No
Click on Platform Protection in the left tabs menu> Intel FPF Anti-Rollback Configuration is expanded by default:			
▼ Intel FPF Anti-Rollback Configuration <span>13</span>			
Parameter		Value	Help
FPF SVN Enabled		Disabled	This option enables usage of Intel FPF for Antiroll
RBE SVN Enabled		Disabled	This option enables usage of Intel FPF for Antiroll
IDLM SVN Enabled		Disabled	This option enables usage of Intel FPF for Antiroll
#	Parameter	Platform	Settings
<span>13</span>	Intel FPF Anti-Rollback Configuration		
	<b>FPF SVN Enabled</b> This option enables the Intel FPF Anti-Rollback mechanism for all firmware components.	CML-V	Enabled Enabled
	<b>RBE SVN Enabled</b> This option enables the Intel FPF Anti-Rollback mechanism for selected firmware components.	CML-V	Enabled Enabled
	<b>IDLM SVN Enabled</b> This option enables the Intel FPF Anti-Rollback mechanism for selected firmware components.	CML-V	Enabled Enabled

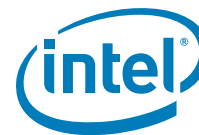


Table 2-8. - Integrated Clock Controller (Sheet 1 of 11)

Click on Integrated Clock Controller in the left tabs menu> Integrated Clock Controller Policies are expanded by default:			
<div> <div>▼ Integrated Clock Controller Policies</div> <div>1</div> </div>			
Parameter	Value	Help Text	
Boot Profile	Profile 0	Profile applied during each boot.	
Failsafe Boot Profile	Profile 0	Boot profile used when system instability is detected.	
Profile Changeable	true	Allows user to change boot profile via BIOS menu or 3rd party appli...	
#	Parameter	Platform	Settings
1	Integrated Clock Controller - Integrated Clock Controller Policies		
	<b>Boot Profile</b>  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-V	Profile 0
	<b>Failsafe Profile</b>  This parameter specifies the profile index of the fail-safe profile. On boot failure detection or CMOS clear the Intel® CSME 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-V	Profile 0
	<b>Profile Changeable</b>  Possible configuration: True/False.  This parameter controls if BIOS or 3rd party application can select boot profile or not. When set to true, it allows user to change boot profile via BIOS or 3rd party application. When set to false, Runtime change to boot profile is not allowed and boot profile selected by "Integrated Clock Controller   Integrated Clock Controller Policies - Boot Profile" parameter will be used to boot platform.  Double click on value column of this parameter to choose from available options.	CML-V	True
Click on Integrated Clock Controller in the left tabs menu> Profiles are expanded by default:			

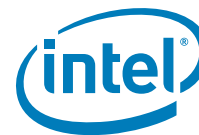


Table 2-8. - Integrated Clock Controller (Sheet 2 of 11)

▼ Profiles			
<div> <div>Profile 0</div> <div>3</div> <div>+ Add Profile</div> </div>			
▼ Profile 2			
Parameter			Value
Profile Name			Profile 0
Profile Type			Standard
			Help Text
			Editable text string.
			Specifies the profile. Intel (R) ME image has to be loaded to enable other ICC profile settings.
#	Parameter	Platform	Settings
2	<b>Integrated Clock Controller - Profiles - Profile 0</b> <b>Note:</b> Intel® CSME image has to be loaded to enable other ICC profile settings.  <b>For CML-V, Intel® FIT provides 2 pre- defined ICC profiles to choose from.</b> <b>•Standard:</b> 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. <b>•Adaptive:</b> 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.  <b>For CML-V, Intel® FIT provides 2 pre-defined ICC profiles to choose from.</b>  <b>•Standard</b> <b>•Adaptive</b>  <b>Note:</b> 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-V	Standard
	<b>Profile Name</b>  This parameter allows user to customize profile name for easy identification. By default it uses pre-defined profile name like Profile 0.	CML-V	Profile 0
	<b>Profile Type</b>  Available ICC profiles for CML-V 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-V	Standard
3	<b>+ Add Profile Button</b>  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-V	
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 11)

▼ BCLK Clock Configurations <span style="color: red; font-weight: bold;">4</span>			
Parameter	Value	Help Text	
BCLK Clock Configuration Enabled	Disabled	Enables/disables BCLK Clock configuration va	
BCLK Clock Frequency	100.000 MHz	Displays the nominal frequency for the select	
BCLK Spread setting	0.45 %	Displays the percentage of Spread setting fo	
#	Parameter	Platform	Settings
<span style="color: red; font-weight: bold;">4</span>	Integrated Clock Controller - Profiles - Profile BCLK Clock Configuration		
	<b>BCLK Clock Configuration Enabled</b> - This setting enables BCLK Clock configuration values for adaptive/overclocking profiles.	CMP-V	Disabled
	<b>BCLK Clock Frequency</b> - 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. <b>Standard Setting Profile Type</b> - Option is grayed out. <b>Adaptive Setting Profile Type</b> - Option is able to be edited.	CML-V	
	<b>BCLK Spread Setting</b> - 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. <b>BCLK Clock Frequency</b> <b>Standard Setting Profile Type</b> - Option is grayed out. <b>Adaptive Setting Profile Type</b> - Option is able to be edited.	CML-V	
Click on Integrated Clock Controller in the left tabs menu> Profiles >Profile> Clock Range Definition Record is expanded by default:			
▼ ClockRangeDefinitionRecord <span style="color: red; font-weight: bold;">5</span>			
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
<span style="color: red; font-weight: bold;">5</span>	Integrated Clock Controller - Profiles - Profile ClockRangeDefinitionRecord		
	<b>BCLK PLL Clock Source Maximum Frequency</b> - 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. <b>Standard Setting Profile Type</b> - Option is grayed out. <b>Adaptive Setting Profile Type</b> - Option is able to be edited.	CML-V	

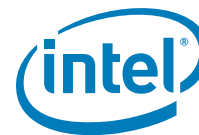


Table 2-8. - Integrated Clock Controller (Sheet 4 of 11)

	<b>BCLK PLL Clock Source Minimum Frequency</b> - 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. <b>Standard Setting Profile Type</b> - Option is grayed out. <b>Adaptive Setting Profile Type</b> - Option is able to be edited.	CML-V	
	<b>BCLK SSC Halt Allowed</b> - 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. <b>Standard Setting Profile Type</b> - Option is grayed out. <b>Adaptive Setting Profile Type</b> - Option is able to be edited.	CML-V	
	<b>BCLK SSC Percentage</b> - 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%) <b>Standard Setting Profile Type</b> - Option is grayed out. <b>Adaptive Setting Profile Type</b> - Option is able to be edited.	CML-V	
Click on Integrated Clock Controller in the left tabs menu> Profiles > Profile> Clock Output Configuration is expanded by default:			
<div> <div>▼ Clock Output Configuration</div> <div>6</div> </div>			
Parameter	Value		
ITPXD	Enabled	Enable/Disable the CLKOUT_ITPXD differ	
SRC0	Enabled	Enable/Disable the CLKOUT_SRC0 differ	
SRC1	Enabled	Enable/Disable the CLKOUT_SRC1 differ	
SRC2	Enabled	Enable/Disable the CLKOUT_SRC2 differ	
SRC3	Enabled	Enable/Disable the CLKOUT_SRC3 differ	
SRC4	Enabled	Enable/Disable the CLKOUT_SRC4 differ	
SRC5	Enabled	Enable/Disable the CLKOUT_SRC5 differ	
SRC6	Enabled	Enable/Disable the CLKOUT_SRC6 differ	
SRC7	Enabled	Enable/Disable the CLKOUT_SRC7 differ	
SRC8	Enabled	Enable/Disable the CLKOUT_SRC8 differ	
SRC9	Enabled	Enable/Disable the CLKOUT_SRC9 differ	
SRC10	Enabled	Enable/Disable the CLKOUT_SRC10 differ	
SRC11	Enabled	Enable/Disable the CLKOUT_SRC11 differ	
SRC12	Enabled	Enable/Disable the CLKOUT_SRC12 differ	
SRC13	Enabled	Enable/Disable the CLKOUT_SRC13 differ	
SRC14	Enabled	Enable/Disable the CLKOUT_SRC14 differ	
SRC15	Enabled	Enable/Disable the CLKOUT_SRC15 differ	
#	Parameter	Platform	Settings

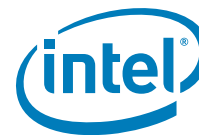


Table 2-8. - Integrated Clock Controller (Sheet 5 of 11)

6	Integrated Clock Controller - Profiles - Profile Clock Output Configuration		
	<b>ITPXD, SRC[0:5]</b> <b>Values: Enabled/Disabled</b> 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-V	Enabled
	<b>SRC0[6:15]</b> <b>Values: Enabled/Disabled</b> 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-V	Enabled
	<b>SRC1</b> <b>Values: Enabled/Disabled</b> Enables or Disables the CLKOUT_SRC1 differential output buffer.	CML-V	Enabled
	<b>SRC2</b> <b>Values: Enabled/Disabled</b> Enables or Disables the CLKOUT_SRC2 differential output buffer.	CML-V	Enabled
	<b>SRC3</b> <b>Values: Enabled/Disabled</b> Enables or Disables the CLKOUT_SRC3 differential output buffer.	CML-V	Enabled
	<b>SRC4</b> <b>Values: Enabled/Disabled</b> Enables or Disables the CLKOUT_SRC4 differential output buffer.	CML-V	Enabled
	<b>SRC5</b> <b>Values: Enabled/Disabled</b> Enables or Disables the CLKOUT_SRC5 differential output buffer.	CML-V	Enabled
	<b>SRC6</b> <b>Values: Enabled/Disabled</b> Enables or Disables the CLKOUT_SRC5 differential output buffer.	CML-V	Enabled
	<b>SRC7</b> <b>Values: Enabled/Disabled</b> Enables or Disables the CLKOUT_SRC5 differential output buffer.	CML-V	Enabled
	<b>SRC8</b> <b>Values: Enabled/Disabled</b> Enables or Disables the CLKOUT_SRC5 differential output buffer.	CML-V	Enabled
	<b>SRC9</b> <b>Values: Enabled/Disabled</b> Enables or Disables the CLKOUT_SRC5 differential output buffer.	CML-V	Enabled



Table 2-8. - Integrated Clock Controller (Sheet 6 of 11)

	<b>SRC10</b> <b>Values: Enabled/Disabled</b> Enables or Disables the CLKOUT_SRC5 differential output buffer.	CML-V	Enabled
	<b>SRC11</b> <b>Values: Enabled/Disabled</b> Enables or Disables the CLKOUT_SRC5 differential output buffer.	CML-V	Enabled
	<b>SRC12</b> <b>Values: Enabled/Disabled</b> Enables or Disables the CLKOUT_SRC5 differential output buffer.	CML-V	Enabled
	<b>SRC13</b> <b>Values: Enabled/Disabled</b> Enables or Disables the CLKOUT_SRC5 differential output buffer.	CML-V	Enabled
	<b>SRC14</b> <b>Values: Enabled/Disabled</b> Enables or Disables the CLKOUT_SRC5 differential output buffer.	CML-V	Enabled
	<b>SRC15</b> <b>Values: Enabled/Disabled</b> Enables or Disables the CLKOUT_SRC5 differential output buffer.	CML-V	Enabled
Click on Integrated Clock Controller in the left tabs menu> Profiles >Profile> Power Management Configuration is expanded by default:			



Table 2-8. - Integrated Clock Controller (Sheet 7 of 11)

Power Management Configuration <span style="color: red; font-weight: bold;">7</span>		
Parameter	Value	
SRC0 CLKREQ# Mapping	GPP_B5	Assign the CLKREQ# signal associated with CLKOUT_SRC0. Please note that remapping of any SRC
SRC1 CLKREQ# Mapping	GPP_B6	Assign the CLKREQ# signal associated with CLKOUT_SRC1. Please note that remapping of any SRC
SRC2 CLKREQ# Mapping	GPP_B7	Assign the CLKREQ# signal associated with CLKOUT_SRC2. Please note that remapping of any SRC
SRC3 CLKREQ# Mapping	GPP_B8	Assign the CLKREQ# signal associated with CLKOUT_SRC3. Please note that remapping of any SRC
SRC4 CLKREQ# Mapping	GPP_B9	Assign the CLKREQ# signal associated with CLKOUT_SRC4. Please note that remapping of any SRC
SRC5 CLKREQ# Mapping	GPP_B10	Assign the CLKREQ# signal associated with CLKOUT_SRC5. Please note that remapping of any SRC
SRC6 CLKREQ# Mapping	GPP_H0	Assign the CLKREQ# signal associated with CLKOUT_SRC6. Please note that remapping of any SRC
SRC7 CLKREQ# Mapping	GPP_H1	Assign the CLKREQ# signal associated with CLKOUT_SRC7. Please note that remapping of any SRC
SRC8 CLKREQ# Mapping	GPP_H2	Assign the CLKREQ# signal associated with CLKOUT_SRC8. Please note that remapping of any SRC
SRC9 CLKREQ# Mapping	GPP_H3	Assign the CLKREQ# signal associated with CLKOUT_SRC9. Please note that remapping of any SRC
SRC10 CLKREQ# Mapping	GPP_H4	Assign the CLKREQ# signal associated with CLKOUT_SRC10. Please note that remapping of any SRC
SRC11 CLKREQ# Mapping	GPP_H5	Assign the CLKREQ# signal associated with CLKOUT_SRC11. Please note that remapping of any SRC
SRC12 CLKREQ# Mapping	GPP_H6	Assign the CLKREQ# signal associated with CLKOUT_SRC12. Please note that remapping of any SRC
SRC13 CLKREQ# Mapping	GPP_H7	Assign the CLKREQ# signal associated with CLKOUT_SRC13. Please note that remapping of any SRC
SRC14 CLKREQ# Mapping	GPP_H8	Assign the CLKREQ# signal associated with CLKOUT_SRC14. Please note that remapping of any SRC
SRC15 CLKREQ# Mapping	GPP_H9	Assign the CLKREQ# signal associated with CLKOUT_SRC15. Please note that remapping of any SRC
CLKREQ SRC0 Enable	Enabled	Enable/Disable the dynamic clock request control by the assigned CLKREQ# for CLKOUT_SRC0.
CLKREQ SRC1 Enable	Enabled	Enable/Disable the dynamic clock request control by the assigned CLKREQ# for CLKOUT_SRC1.
CLKREQ SRC2 Enable	Enabled	Enable/Disable the dynamic clock request control by the assigned CLKREQ# for CLKOUT_SRC2.
CLKREQ SRC3 Enable	Enabled	Enable/Disable the dynamic clock request control by the assigned CLKREQ# for CLKOUT_SRC3.
CLKREQ SRC4 Enable	Enabled	Enable/Disable the dynamic clock request control by the assigned CLKREQ# for CLKOUT_SRC4.
CLKREQ SRC5 Enable	Enabled	Enable/Disable the dynamic clock request control by the assigned CLKREQ# for CLKOUT_SRC5.
CLKREQ SRC6 Enable	Enabled	Enable/Disable the dynamic clock request control by the assigned CLKREQ# for CLKOUT_SRC6.
CLKREQ SRC7 Enable	Enabled	Enable/Disable the dynamic clock request control by the assigned CLKREQ# for CLKOUT_SRC7.
CLKREQ SRC8 Enable	Enabled	Enable/Disable the dynamic clock request control by the assigned CLKREQ# for CLKOUT_SRC8.
CLKREQ SRC9 Enable	Enabled	Enable/Disable the dynamic clock request control by the assigned CLKREQ# for CLKOUT_SRC9.
CLKREQ SRC10 Enable	Enabled	Enable/Disable the dynamic clock request control by the assigned CLKREQ# for CLKOUT_SRC10.
CLKREQ SRC11 Enable	Enabled	Enable/Disable the dynamic clock request control by the assigned CLKREQ# for CLKOUT_SRC11.
CLKREQ SRC12 Enable	Enabled	Enable/Disable the dynamic clock request control by the assigned CLKREQ# for CLKOUT_SRC12.
CLKREQ SRC13 Enable	Enabled	Enable/Disable the dynamic clock request control by the assigned CLKREQ# for CLKOUT_SRC13.
CLKREQ SRC14 Enable	Enabled	Enable/Disable the dynamic clock request control by the assigned CLKREQ# for CLKOUT_SRC14.
CLKREQ SRC15 Enable	Enabled	Enable/Disable the dynamic clock request control by the assigned CLKREQ# for CLKOUT_SRC15.
CLKRUN LPC0 Enable	Enabled	Enable/Disable the CLKRUN protocol on LPC0 output clock.
CLKRUN LPC1 Enable	Enabled	Enable/Disable the CLKRUN protocol on LPC1 output clock.
Clock Gating of Core 24Mhz Crystal Disable	Enabled	Enable/Disable dynamic clock gating of Core 24Mhz Crystal Oscillator clock. When enabled , Core 24M
Clock Gating of CLKOUT_ITPxDP Disable	Enabled	Enable/Disable dynamic control of CLKOUT_ITPxDP. When enabled by this register bit, CLKOUT_ITPxD
Clock Gating of CLKOUT_CPUBCLK Disable	Enabled	Enable/Disable dynamic control of CLKOUT_CPUBCLK. When enabled by this register bit, CLKOUT_CPL
Clock Gating of CLKOUT_CPUPCIBCLK Disable	Enabled	Enable/Disable dynamic control of CLKOUT_CPUPCIBCLK. When enabled by this register bit, CLKOUT
Clock Gating of CLKOUT_CPUNSSC Disable	Enabled	Enable/Disable dynamic control of CLKOUT_CPUNSSC. When enabled by this register bit, CLKOUT_C
Clock Gating of CLKOUT_CPUNSSC[P/N] Disable	Enabled	Enable/Disable dynamic control of CLKOUT_CPUNSSC[P/N]. Controls the parked state of True (P) an
Clock Gating of icc_osc_fast_clk Disable	Enabled	Enable/Disable dynamic clock gate on icc_osc_fast_clk.
Clock Gating of icc_osc_side_clk Disable	Enabled	Enable/Disable dynamic clock gate on icc_osc_side_clk.
USB3Gen2PCIe PLL OFF Wait	16us	Set G2PLLOFFWAIT timer value. Once timer expires and there are no wake events, the USB3Gen2PC
USB3Gen2PCIe PLL PG Wait	16us	Set G2PLLPWAIT timer value. Once timer expires and there are no wake events, the USB3Gen2PCI
Run-time S0 SUS PG Wait	16us	Set SUSPGWAIT timer value. Once timer expires and there are no wake events, the USB3Gen2PCIe
Crystal Oscillator Fast Restart Mode	00b	Configure Crystal Oscillator Fast Restart Mode. In all below listed fast start modes, ISCLK kickstarts
BCLK PLL Shutdown Wait Interval	16us	Enable Dynamic power management of BCLK PLL. Upon the event that all conditions (other than this
24Mhz Crystal Shutdown Wait Interval	16us	Enable Dynamic power management of Crystal. Upon the event that all conditions (other than this w



Table 2-8. - Integrated Clock Controller (Sheet 8 of 11)

#	Parameter	Platform	Settings
<b>7</b>	<b>Integrated Clock Controller - Profiles - Profile PwrManagementConfiguration</b>  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.  <b>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.</b>		
	<b>SRC0[5:0] CLKREQ# Mapping</b> 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.	CML-V	GPP_B5 GPP_B5
	<b>SRC1 CLKREQ# Mapping</b> Assign the CLKREQ# signal associated with CLKOUT_SRC1.	CML-V	GPP_B6 GPP_B6
	<b>SRC2 CLKREQ# Mapping</b> Assign the CLKREQ# signal associated with CLKOUT_SRC2.	CML-V	GPP_B7 GPP_B7
	<b>SRC3 CLKREQ# Mapping</b> Assign the CLKREQ# signal associated with CLKOUT_SRC3.	CML-V	GPP_B8 GPP_B8
	<b>SRC4 CLKREQ# Mapping</b> Assign the CLKREQ# signal associated with CLKOUT_SRC4.	CML-V	GPP_B9 GPP_B9
	<b>SRC5 CLKREQ# Mapping</b> Assign the CLKREQ# signal associated with CLKOUT_SRC5.	CML-V	GPP_B10 GPP_B10
	<b>SRC6 CLKREQ# Mapping</b> Assign the CLKREQ# signal associated with CLKOUT_SRC5.	CML-V	GPP_H0 GPP_H0
	<b>SRC7 CLKREQ# Mapping</b> Assign the CLKREQ# signal associated with CLKOUT_SRC5.	CML-V	GPP_H1 GPP_H1
	<b>SRC8 CLKREQ# Mapping</b> Assign the CLKREQ# signal associated with CLKOUT_SRC5.	CML-V	GPP_H2 GPP_H2
	<b>SRC9 CLKREQ# Mapping</b> Assign the CLKREQ# signal associated with CLKOUT_SRC5.	CML-V	GPP_H3 GPP_H3
	<b>SRC10 CLKREQ# Mapping</b> Assign the CLKREQ# signal associated with CLKOUT_SRC5.	CML-V	GPP_H4 GPP_H4
	<b>SRC11 CLKREQ# Mapping</b> Assign the CLKREQ# signal associated with CLKOUT_SRC5.	CML-V	GPP_H5 GPP_H5
	<b>SRC12 CLKREQ# Mapping</b> Assign the CLKREQ# signal associated with CLKOUT_SRC5.	CML-V	GPP_H6 GPP_H6
	<b>SRC13 CLKREQ# Mapping</b> Assign the CLKREQ# signal associated with CLKOUT_SRC5.	CML-V	GPP_H7 GPP_H7
	<b>SRC14 CLKREQ# Mapping</b> Assign the CLKREQ# signal associated with CLKOUT_SRC5.	CML-V	GPP_H8 GPP_H8
	<b>SRC15 CLKREQ# Mapping</b> Assign the CLKREQ# signal associated with CLKOUT_SRC5.	CML-V	GPP_H9 GPP_H9
	<b>CLKREQ SRC0 Enable</b> <b>Values: Enabled/Disabled</b> This parameter allows user to Enable/Disable the dynamic clock request control by the assigned CLKREQ# for CLKOUT_SRC1.	CML-V	Enabled
	<b>CLKREQ SRC1 Enable</b> <b>Values: Enabled/Disabled</b> This parameter allows user to Enable/Disable the dynamic clock request control by the assigned CLKREQ# for CLKOUT_SRC1.	CML-V	Enabled

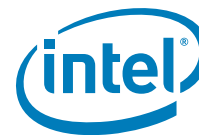


Table 2-8. - Integrated Clock Controller (Sheet 9 of 11)

	<b>CLKREQ SRC2 Enable</b> <b>Values: Enabled/Disabled</b> This parameter allows user to Enable/Disable the dynamic clock request control by the assigned CLKREQ# for CLKOUT_SRC2.	CML-V	Enabled
	<b>CLKREQ SRC3 Enable</b> <b>Values: Enabled/Disabled</b> This parameter allows user to Enable/Disable the dynamic clock request control by the assigned CLKREQ# for CLKOUT_SRC3.	CML-V	Enabled
	<b>CLKREQ SRC4 Enable</b> <b>Values: Enabled/Disabled</b> This parameter allows user to Enable/Disable the dynamic clock request control by the assigned CLKREQ# for CLKOUT_SRC4.	CML-V	Enabled
	<b>CLKREQ SRC5 Enable</b> <b>Values: Enabled/Disabled</b> This parameter allows user to Enable/Disable the dynamic clock request control by the assigned CLKREQ# for CLKOUT_SRC5.	CML-V	Enabled
	<b>CLKREQ SRC6 Enable</b> <b>Values: Enabled/Disabled</b> This parameter allows user to Enable/Disable the dynamic clock request control by the assigned CLKREQ# for CLKOUT_SRC6.	CML-V	Enabled
	<b>CLKREQ SRC7 Enable</b> <b>Values: Enabled/Disabled</b> This parameter allows user to Enable/Disable the dynamic clock request control by the assigned CLKREQ# for CLKOUT_SRC7.	CML-V	Enabled
	<b>CLKREQ SRC8 Enable</b> <b>Values: Enabled/Disabled</b> This parameter allows user to Enable/Disable the dynamic clock request control by the assigned CLKREQ# for CLKOUT_SRC8.	CML-V	Enabled
	<b>CLKREQ SRC9 Enable</b> <b>Values: Enabled/Disabled</b> This parameter allows user to Enable/Disable the dynamic clock request control by the assigned CLKREQ# for CLKOUT_SRC9.	CML-V	Enabled
	<b>CLKREQ SRC10 Enable</b> <b>Values: Enabled/Disabled</b> This parameter allows user to Enable/Disable the dynamic clock request control by the assigned CLKREQ# for CLKOUT_SRC10.	CML-V	Enabled
	<b>CLKREQ SRC11 Enable</b> <b>Values: Enabled/Disabled</b> This parameter allows user to Enable/Disable the dynamic clock request control by the assigned CLKREQ# for CLKOUT_SRC11.	CML-V	Enabled
	<b>CLKREQ SRC12 Enable</b> <b>Values: Enabled/Disabled</b> This parameter allows user to Enable/Disable the dynamic clock request control by the assigned CLKREQ# for CLKOUT_SRC12.	CML-V	Enabled
	<b>CLKREQ SRC13 Enable</b> <b>Values: Enabled/Disabled</b> This parameter allows user to Enable/Disable the dynamic clock request control by the assigned CLKREQ# for CLKOUT_SRC13.	CML-V	Enabled
	<b>CLKREQ SRC14 Enable</b> <b>Values: Enabled/Disabled</b> This parameter allows user to Enable/Disable the dynamic clock request control by the assigned CLKREQ# for CLKOUT_SRC14.	CML-V	Enabled
	<b>CLKREQ SRC15 Enable</b> <b>Values: Enabled/Disabled</b> This parameter allows user to Enable/Disable the dynamic clock request control by the assigned CLKREQ# for CLKOUT_SRC15.	CML-V	Enabled

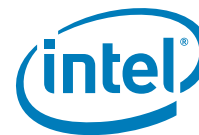


Table 2-8. - Integrated Clock Controller (Sheet 10 of 11)

	<b>CLKRUN LPC0 Enable</b> <b>Values: Enabled/Disabled</b> This parameter allows user to Enable/Disable CLKRUN protocol on LPC1 output clock.	CML-V	Enabled
	<b>CLKRUN LPC1 Enable</b> <b>Values: Enabled/Disabled</b> This parameter allows user to Enable/Disable CLKRUN protocol on LPC1 output clock.	CML-V	Enabled
	<b>Clock Gating of Core 24MHz Crystal Disable</b> <b>Values: Enabled/Disabled</b> This parameter decides if Crystal is forced to be on or is subjected to dynamic shutdown. Crystal Oscillator can dynamically shut down upon iSCLK detecting idle condition on all clock consumers of crystal clock. <b>Note:</b> Recommendation is to leave setting at default value.	CML-V	Enabled
	<b>Clock Gating of CLKOUT_ITPxDP Disable</b> <b>Values: Enabled/Disabled</b> This parameter allows user to Enable/Disable dynamic control of CLKOUT_ITPxDP. When enabled, CLKOUT_ITPxDP is subject to gating/ungating control by CPUBCLKREQ <b>Note:</b> Recommendation is to leave setting at default value.	CML-V	Enabled
	<b>Clock Gating of CLKOUT_CPUBCLK Disable</b> <b>Values: Enabled/Disabled</b> This parameter allows user to Enable/Disable dynamic control of CLKOUT_CPUBCLK. When enabled, CLKOUT_CPUBCLK is subject to gating/ungating control by CPUBCLKREQ These settings should match with platform hardware design. <b>Note:</b> Recommendation is to leave setting at default value.	CML-V	Enabled
	<b>Clock Gating of CLKOUT_CPUPCIBCLK Disable</b> <b>Values: Enabled/Disabled</b> This parameter allows user to Enable/Disable dynamic control of CLKOUT_CPUPCIBCLK. When enabled, CLKOUT_CPUPCIBCLK is subject to gating/ungating control by CPUPCIBCLKREQ <b>Note:</b> Recommendation is to leave setting at default value.	CML-V	Enabled
	<b>Clock Gating of CLKOUT_CPUNSSC Disable</b> <b>Values: Enabled/Disabled</b> This parameter allows user to Enable/Disable dynamic control of CLKOUT_CPUNSSC. When enabled, CLKOUT_CPUNSSC is subject to gating/ungating control by CPUNSSCLKREQ <b>Note:</b> Recommendation is to leave setting at default value.  <b>Note:</b> For HEDT platform, when SKX-X processor is paired, by design, Intel® ME FW disables clock gating of CLKOUT_CPUNSSC by default. In this case Intel® FIT default setting is overwritten using Intel® ME FW.	CML-V	Enabled
	<b>Clock Gating of CLKOUT_CPUNSSC[P/N] Disable</b> <b>Values: Enabled/Disabled</b> This parameter allows user to Enable/Disable dynamic control of CLKOUT_CPUNSSC[P/N]. Controls the parked state of True (P) and Complementary (N) copies of the differential pair when CLKOUT_CPUNSSC[P/N] is dynamically gated under S0 idle state. <b>Note:</b> Recommendation is to leave setting at default value.	CML-V	Enabled
	<b>Clock Gating of icc_rosc_fast_clk Disable</b> <b>Values: Enabled/Disabled</b> This parameter allows user to Enable/Disable dynamic clock gate on icc_rosc_fast_clk <b>Note:</b> Recommendation is to leave setting at default value.	CML-V	Enabled

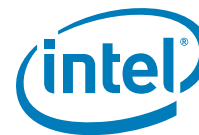


Table 2-8. - Integrated Clock Controller (Sheet 11 of 11)

	<b>Clock Gating of icc_rosc_side_clk Disable</b> <b>Values: Enabled/Disabled</b> This parameter allows user to Enable/Disable dynamic clock gate on icc_rosc_side_clk <b>Note:</b> Recommendation is to leave setting at default value.	CML-V	Enabled
	<b>USB3Gen2PCIe PLL OFF Wait</b> This parameter allows user to set G2PLLOFFWAIT timer value. Once timer expires and there are no wake events, the USB3Gen2PCIe PLL can be shutdown <b>Note:</b> Recommendation is to leave setting at default value.	CML-V	8us
	<b>USB3Gen2PCIe PLL PG Wait</b> This parameter allows user to set G2PLLPWAIT timer value. Once timer expires and there are no wake events, the USB3Gen2PCIe PLL can be shutdown <b>Note:</b> Recommendation is to leave setting at default value.	CML-V	8us
	<b>Run-time S0 SUS PG Wait</b> This parameter allows user to set SUSPGWAIT timer value. Once timer expires and there are no wake events, the USB3Gen2PCIe PLL can be shutdown <b>Note:</b> Recommendation is to leave setting at default value.	CML-V	8us
	<b>Crystal Oscillator Fast Restart Mode</b> This parameter allows user to configure Crystal Oscillator Fast Restart Mode. In all below listed fast start modes, iSCLK kickstarts crystal XIN/XOUT by injecting a 24Mhz kickstart reference clock onto these pins.  <b>Note:</b> Configuration of this parameter co-relates to configuration of <b>Clock Gating of Core 24MHz Crystal Disable</b> parameter.  If Clock Gating of Core 24MHz Crystal Disable is set to ' <b>Disable</b> ', Crystal Oscillator Fast Restart Mode parameter has <b>no impact</b> .  If Clock Gating of Core 24MHz Crystal Disable is set to ' <b>Enabled</b> ', Crystal Oscillator Fast Restart Mode parameter <b>must be set to '01b'</b> . Other value like '00b' can cause wake latency conflict which can cause platform functional issue.	CML-V	01b
	<b>BCLK PLL Shutdown Wait Interval</b> This parameter allows user to enable Dynamic power management of BCLK PLL. Upon the event that all conditions (other than this wait timer itself) are satisfied for iSCLK dynamic PLL shutdown, a timer is started. Once it expires and there are no wake events, this PLL will shutdown. <b>Note:</b> Recommendation is to leave setting at default value.	CML-V	8us
	<b>24MHz Crystal Shutdown Wait Interval</b> 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. <b>Note:</b> Recommendation is to leave setting at default value.	CML-V	8us



Table 2-9. - Networking &amp; 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	Help Text
Platform Discrete vPro NIC Enabled	No	YES = Discrete NIC enabled in platform NO = Intel Integrated vPro NIC
Platform Discrete vPro NIC SMBUS slave address	0x49	Platform discrete NIC slave address Note: Input

#	Parameter	Platform	Settings
1	Platform vPro NIC		
	<b>Platform Discrete vPro NIC Enabled</b> This setting enables Intel® vPro with discrete NIC on the platform.	CML-V	No
	<b>Platform Discrete vPro NIC SMBus slave address</b> This setting configures the discrete NIC SMBus slave address.	CML-V	0x49

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

▼ Wired LAN Configuration

2

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
2	Wired LAN Configuration		
	<b>LAN Power Well</b> 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-V	SLP_LAN#
	<b>LAN PHY Power Up Time</b> Values: 50ms, 100ms	CML-V	100ms

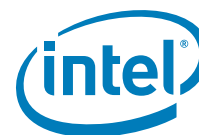


Table 2-9. - Networking &amp; Connectivity (Sheet 2 of 3)

	<b>Intel® Integrated Wired LAN Enable</b> <b>Values:</b> Enabled/Disabled - This setting enables or disables the Intel® Integrated LAN.	CML-V	Yes
	<b>GbE PCIe Port Select</b> <b>Values:</b> PORT4, PORT5, PORT9, PORT12, PORT13 - This setting allows customers to configure the PCIe Port that will Intel® Integrated LAN will operate on.	CML-V	Port4
	<b>GbE PHY SMBus Address</b> This setting configures Intel® Integrated Wired LAN SMBus address to accept SMBus cycles from the MAC. <b>Note:</b> Recommended setting is 64h.	CML-V	0x64
	<b>GbE SMBus Address Enabled</b> <b>Values:</b> Yes/No - This enables the Intel® Integrated Wired LAN MAC SMBus address. <b>Note:</b> This setting must be enabled if using Intel® Integrated LAN.	CML-V	Yes
	<b>GbE MAC SMBus Address</b>	CML-V	0x70
	<b>PHY Connection</b> <b>Values:</b> No PHY connected, PHY on SMLink0	CML-V	PHY on SMLink0
	<b>LAN PHY Power Control GPD11 Signal Configuration</b> <b>Values:</b> GPD11, LANPHYPC - This setting allows the customer to assign the LAN PHY Power Control signal to GbE or as GDP11.	CML-V	LANPHYPC
Click on Networking & Connectivity in the left tabs menu> Wireless LAN Configuration is expanded by default:			
<div> <div>▼ Wireless LAN Configuration</div> <div>3</div> </div>			
Parameter	Value	Help Text	
Intel(R) ME CLINK Signal Enabled	No	This setting allows customers to enable / disable th	
SLP_WLAN# / GDP9 Signal Configuration	Enable as SLP_WLAN#	This setting allows user the to assign the WLAN Poi	
WLAN Microcode	0x9DF0 PULSAR	This setting allows OEMs to configure which Intel(R)	
WLAN Power Well	SLP_WLAN#	-	
#	Parameter	Platform	Settings
3	Wireless LAN Configuration		
	<b>Intel® ME CLINK Signal Enabled</b> <b>Values:</b> Yes/No - This setting allows customers to enable / disable the Wireless LAN CLINK signal through Intel® CSME firmware. <b>Note:</b> For using Intel® vPro™ Wireless solutions this should be set to "Yes".	CML-V	No
	<b>SLP_WLAN# / GDP9 Signal Configuration</b> <b>Values:</b> SLP_WLAN#, GDP9 - This setting allows the customer to assign the WLAN Power Control signal to WLAN or as GDP9. <b>Note:</b> If using Intel® Wireless LAN this setting should be set to "Enable as SLP_WLAN#".	CML-V	Enable as SLP_WLAN#
	<b>WLAN Microcode</b> - This setting allow OEMs to configure which Intel® Wireless LAN card microcode to load into the firmware image.	CML-V	0x9DF0

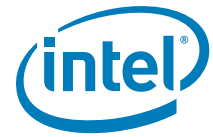


Table 2-9. - Networking &amp; Connectivity (Sheet 3 of 3)

	<b>WLAN Power Well</b> <b>Values:</b> 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) <b>Note:</b> Recommended setting is SLP_WLAN#.	CML-V	SLP_WLAN#

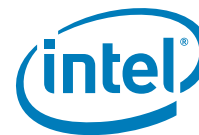


Table 2-10. - Internal PCH Buses (Sheet 1 of 5)

Click on Internal PCH Buses in the left tabs menu> PCH Timer Configuration is expanded by default:			
<b>▼ PCH Timer Configuration</b> <b>1</b>			
Parameter	Value	Help Text	
APWROK Timing	2 ms	This soft strap determines the time between the SLP_A# pin de-...	
PCH clock output stable to PRO...	1 ms	This setting configures the minimum timing from XCK_PLL locke...	
PCIe Power Stable Timer (tPCH...	Disabled	This setting configures the enables / disables the tPCH33 timer. ...	
PROCPWRGD and SYS_PWROK ...	1 ms	This setting configures the minimum timing from CPUPWRGD as...	
Time Stamp Counter Clear on ...	No	When set to 'Yes' causes the PCH to clear the Time Stamp Coun...	
#	Parameter	Platform	Settings
<b>1</b>	Internal PCH Buses - PCH Timer Configuration		
	<b>APWROK Timing</b> <b>Values: 2ms, 4ms, 8ms, 16ms</b> - This soft strap determines the time between the SLP_A# pin de-asserting and the APWROK timer expiration. For further details see Comet Lake V Platform Controller Hub EDS.	CML-V	2ms
	<b>PCH clock output stable to PROCPWRGD high (tPCH45)</b> <b>Values: 100ms, 50ms, 5ms, 1ms</b> - This setting configures the minimum timing from XCK_PLL locked to CPUPWRGD high. For further details see Comet Lake V Platform Controller Hub EDS.	CML-V	1ms
	<b>PCIe Power Stable Timer (tPCH33)</b> <b>Values: Enabled/Disabled</b> - This setting configures the enables / disables the t36 timer. When enabled PCH will count 99ms from PWROK assertion before PLTRST# is de-asserted. <b>Note:</b> The recommended setting is "Disabled".	CML-V	Disabled
	<b>PROCPWRGD and SYS_PWROK high to SUS_STAT# de-assertion (tPCH46)</b> <b>Values: 1ms, 2ms, 5ms</b> - This setting configures the minimum timing from CPUPWRGD assertion to SUS_STAT#. For further details see Comet Lake V Platform Controller Hub EDS.	CML-V	1ms
	<b>Time Stamp Counter Clear on Warm Reset</b> <b>Values: Yes/No</b> - When set to 'Yes' causes PCH to clear the Time Stamp Counter when a Warm Reset is performed.	CML-V	No
Click on Internal PCH Buses in the left tabs menu> SMBus / SMLink Configuration is expanded by default:			

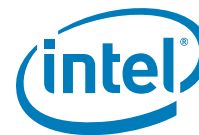


Table 2-10. - Internal PCH Buses (Sheet 2 of 5)

▼ SMBus / SMLink Configuration <span style="background-color: red; color: white; border-radius: 50%; padding: 2px 5px;">2</span>			
Parameter	Value		
Intel(R) SMBus ASD Address	0x0	This setting configures the Intel(R) SMBus Alert Sending Device Address	
Intel(R) SMBus ASD Address En...	No	This setting enables / disables the Intel(R) SMBus Alert Sending Device	
Intel(R) SMBus Subsystem Ven...	0x0	This setting configures the Intel(R) SMBus Subsystem Vendor and Devi	
Intel(R) SMBus I2C Address	0x0	This setting configures the Intel(R) SMBus I2C Address. Note: This sett	
Intel(R) SMBus I2C Address En...	No	This setting enables / disables the Intel(R) SMBus I2C Address. Note: T	
SMBus / SMLink TCO Slave Con...	Intel(R) SMBus	This setting configures the TCO Slave connection to ether the Intel(R) S	
SMLink0 Enabled	Yes	This setting enables / disables SMLink0 interface. For further details se	
SMLink0 Frequency	1 MHz	This setting determines the frequency at which the SMLink0 will operat	
SMLink1 I2C Target Address	0x0	This setting configures SMLink1 I2C Target Address. For further details	
SMLink1 I2C Target Address En...	No	This setting configures SMLink1 I2C Target Address. For further details	
SMLink1 GP Target Address	0x0	This setting configures SMLink1 GP Target Address. For further details	
SMLink1 GP Target Address En...	No	This setting enables / disables SMLink1 GP Target Address interface. Fi	
SMLink1 Enabled	No	This setting enables / disables SMLink1 interface. For further details se	
SMLink1 Frequency	100 KHz	This setting determines the frequency at which the SMLink1 will operat	
Intel(R) SMBus ASD Mode Confi...	Enable as GPP_C2	This setting determines the native mode of operation for the Intel(R) SI	
Intel(R) SMBus MCTP Address	0x0	This setting configures the Intel(R) SMBus MCTP Address. Note: This s	
Intel(R) SMBus MCTP Address ...	No	This setting enables / disables the Intel(R) SMBus MCTP Address. Note	
SMLink1 MCTP Address	0x0	This setting configures the Intel(R) SMBus MCTP Address. Note: This s	
SMLink1 MCTP Address Enabled	No	This setting enables / disables the Intel(R) SMBus MCTP Address. Note	
#	Parameter	Platform	Settings
<span style="background-color: red; color: white; border-radius: 50%; padding: 2px 5px;">2</span>	Internal PCH Buses - SMBus / SMLink Configuration		
	<b>Intel® SMBus ASD Address</b> - This setting configures the Intel® SMBus Alert Sending Device Address. For details see Comet Lake V SPI Programming guide for further details.	CML-V	0x00000000
	<b>Intel® SMBus ASD Address Enable</b> <b>Values: Yes/No</b> - This setting enables / disables the Intel® SMBus Alert Sending Device. For details see Comet Lake V SPI Programming guide for further details.	CML-V	No
	<b>Intel® SMBus Subsystem Vendor &amp; Device ID for ASF</b> - This setting configures the Intel® SMBus Subsystem Vendor & Device ID for ASF. For details see Comet Lake V SPI Programming guide further details.	CML-V	0x00000000
	<b>Intel® SMBus I2C Address</b> - This setting configures the Intel® SMBus I2C Address. <b>Note:</b> This setting is only used for testing purposes. The recommended setting is "0000000".	CML-V	0x00000000

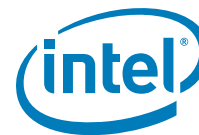


Table 2-10. - Internal PCH Buses (Sheet 3 of 5)

	<b>Intel® SMBus I2C Address Enabled</b> <b>Values:</b> Yes/No - This setting enables / disables the Intel® SMBus I2C Address. <b>Note:</b> This setting is only used for testing purposes. The recommended setting is "No".	CML-V	No
	<b>SMBus / SMLink TCO Slave Connection</b> <b>Values:</b> Intel® SMBus, SMLink0 - This setting configures the TCO Slave connection to either the Intel® SMBus or SMLink0. For further details see Comet Lake V Platform Controller Hub EDS.	CML-V	Intel® SMBus
	<b>SMLink0 Enabled</b> <b>Values:</b> Yes/No - This setting enables / disables SMLink0 interface. For further details see Comet Lake V Platform Controller Hub EDS.	CML-V	Yes
	<b>SMLink0 Frequency</b> <b>Values:</b> 100KHz, 400KHz, 1 MHz - This setting determines the frequency at which the SMLink0 will operate. <b>Note:</b> The recommended setting is "1MHz".	CML-V	1 MHz
	<b>SMLink1 I2C Target Address</b> - This setting configures SMLink1 I2C Target Address. For further details see Comet Lake V Platform Controller Hub EDS.	CML-V	0x00000000
	<b>SMLink1 I2C Target Address Enabled</b> <b>Values:</b> Yes/No - This setting configures SMLink1 I2C Target Address. For further details see Comet Lake V Platform Controller Hub EDS.	CML-V	No
	<b>SMLink1 GP Target Address</b> - This setting configures SMLink1 GP Target Address. For further details see Comet Lake V Platform Controller Hub EDS.	CML-V	0x00000000
	<b>SMLink1 GP Target Address Enabled</b> <b>Values:</b> Yes/No - This setting enables / disables SMLink1 GP Target Address interface. For further details see Comet Lake V Platform Controller Hub EDS. <b>Note:</b> This setting must be set to "Yes" if using PCH / MCP Thermal reporting.	CML-V	No
	<b>SMLink1 Enabled</b> <b>Values:</b> Yes/No - This setting enables / disables SMLink1 interface. For further details see Comet Lake V Platform Controller Hub EDS. <b>Note:</b> This setting must be set to "Yes" if using PCH / MCP Thermal reporting.	CML-V	No
	<b>SMLink1 Frequency</b> <b>Values:</b> 100KHz, 400KHz, 1 MHz - This setting determines the frequency at which the SMLink1 will operate. <b>Note:</b> The recommended setting is "100KHz".	CML-V	100 KHz
	<b>Intel® SMBus ASD Mode Configuration</b> This setting determines the native mode of operation for the Intel® SMBus ASD signal.	CML-V	Enable as GPP_C2
	<b>Intel® SMBus MCTP Address Enabled</b> <b>Values:</b> Yes/No - This setting enables / disables the Intel® SMBus MCTP Address. <b>Note:</b> This setting is only used for testing purposes. The recommended setting is "No".	CML-V	0x00000000
	<b>Intel® SMBus MTCP Address</b> - This setting configures the Intel® SMBus MCTP Address. <b>Note:</b> This setting is only used for testing purposes. The default setting is "00000000".	CML-V	No
	<b>SMLink1 MTCP Address</b> - This setting configures the SMLink1 MCTP Address. <b>Note:</b> This setting is only used for testing purposes. The default setting is "00000000".	CML-V	0x00000000
	<b>SMLink1 MCTP Address Enabled</b> <b>Values:</b> Yes/No - This setting enables / disables the SMLink1 MCTP Address. <b>Note:</b> This setting is only used for testing purposes. The recommended setting is "No".	CML-V	No
Click on Internal PCH Buses in the left tabs menu> DMI Configuration is expanded by default:			

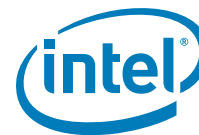


Table 2-10. - Internal PCH Buses (Sheet 4 of 5)

▼ DMI Configuration 3			
Parameter	Value	Help	
DMI Lane Reversal	No	This setting allow the DMI Lane signals to be	
DMI Port Staggering Enabled	Yes	This setting configures DMI for Port Staggerin	
DMI AC Coupling Select	No	This setting determines if DMI is operating in	
DMI Lane Width	DMI x4	This setting determines the number of DMI la	
#	Parameter	Platform	Settings
3	Internal PCH Buses - DMI Configuration		
	DMI Lane Reversal Values: Yes/No - This setting allows the DMI Lane signals to be reversed. For further details see Comet Lake V Platform Controller Hub EDS.	CML-V	No
	DMI Port Staggering Values: Yes/No - This setting configures DMI for Port Staggering. For further details see Comet Lake V Platform Controller Hub EDS.	CML-V	Yes
	DMI AC Coupling Values: Yes/No - This determines if DMI is operating in AC or DC coupled mode	CML-V	No
	DMI Lane Width Values: Disabled, x1, x2, x4 - This setting determines the number of DMI lanes available	CML-V	DMI x4
Click on Internal PCH Buses in the left tabs menu> eSPI Configuration is expanded by default:			
▼ eSPI Configuration 4			
Parameter	Value		
eSPI / EC Bus Frequency	60MHz	This setting determines the maximum frequer	
eSPI / EC Maximum I/O Mode	Single, Dual and Quad	This setting determines the maximum IO Mod	
eSPI / EC CRC Check Enabled	Yes	This setting enables CRC checking on eSPI Sla	
eSPI / EC Max Outstanding Request for Master Attached Flash Channel	2	This setting determines the Maximum outstan	
eSPI / EC Slave Attached Flash Multiple Outstanding Requests Enable	Single Outstanding Request	This setting enabled multiple outstanding requ	
eSPI / EC Slave Attached Flash Channel OOO Enable	In-Order SAF Requests	This setting enables Out or Order requests on	
eSPI / EC Slave 1 Device CRC Check Enable	Yes	This setting determines if CRC checking is ena	
eSPI / EC Slave Device Maximum I/O Mode	Single, Dual and Quad	This setting configures the maximum I/O mod	
eSPI / EC Slave Device Bus Frequency	60MHz	This setting configures the maximum operatin	
eSPI / EC Slave Device Enabled	No	This setting enables the Slave device on the e	
#	Parameter	Platform	Settings
4	Internal PCH Buses - eSPI Configuration		



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

	eSPI / EC Bus Frequency 20MHz, 24MHz, 30MHz, 40MHz, 60MHz	CML-V	60MHz
	eSPI / EC Maximum I/O Mode Values: Single, Single and Dual, Single and Quad, Single Dual and Quad	CML-V	Single, Dual and Quad
	eSPI / EC CRC Check Enabled Values: Yes/No	CML-V	Yes
	eSPI / EC Max Outstanding Request for Master Attached Flash Channel	CML-V	2
	eSPI / EC Slave Attached Flash Multiple Outstanding Requests Enable	CML-V	Single Outstanding Request
	eSPI / EC Slave Attached Flash Channel OOO Enable	CML-V	In-Order SAF Requests
	eSPI / EC Slave 1 Device CRC Check Enabled Values: Yes/No	CML-V	Yes
	eSPI / EC Slave Device Maximum I/O Mode	CML-V	Single, Dual and Quad
	eSPI / EC Slave Device Bus Frequency	CML-V	60MHz
	eSPI / EC Slave Device Enabled	CML-V	No



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

Click on Power in the left tabs menu> Platform Power is expanded by default:			
<div> <div>▼ Platform Power</div> <div>1</div> </div>			
Parameter	Value	Help	
SLP_S5# / GPD10 Signal Configuration	Enable as SLP_S5#	This setting allows the user to assign the SLP_S5	
SLP_S3# / GPD4 Signal Configuration	Enable as SLP_S3#	This setting allows the user to assign the SLP_S3	
SLP_S4# / GPD5 Signal Configuration	Enable as SLP_S4#	This setting allows the user to assign the SLP_S4	
SLP_A# / GPD6 Signal Configuration	Enable as SLP_A#	This setting allows the user to assign the SLP_A#	
SLP_S0# Tunnel	Disabled	This setting Enables / Disables the tunneling of th	
#	Parameter	Platform	Settings
1	Power - Platform Power		
	<b>SLP_S5# / GPD10 Signal Configuration</b> <b>Values:</b> 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 V Platform Controller Hub EDS.	CML-V	SLP_S5#
	<b>SLP_S3# / GPD4 Signal Configuration</b> <b>Values:</b> 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 V Platform Controller Hub EDS.	CML-V	SLP_S3#
	<b>SLP_S4# / GPD5 Signal Configuration</b> <b>Values:</b> 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 V Platform Controller Hub EDS.	CML-V	SLP_S4#
	<b>SLP_A# / GPD6 Signal Configuration</b> <b>Values:</b> 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 V Platform Controller Hub EDS.	CML-V	SLP_A#
	<b>SLP_S0# Tunnel</b> <b>Values:</b> Enabled, Disabled This setting Enables / Disables the tunneling of the SLP_S0# pin over eSPI to the EC when in eSPI mode.  <b>Warning:</b> This setting needs to be set to disabled when the platform is running in eSPI mode.	CML-V	Disabled
Click on Power in the left tabs menu> Deep Sx is expanded by default:			
<div> <div>▼ Deep Sx</div> <div>2</div> </div>			
Parameter	Value	Help Text	
Deep Sx Enabled	Yes	This requires the target platform to support Deep SX state	
#	Parameter	Platform	Settings

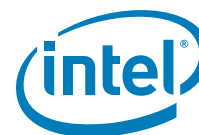


Table 2-11. - Power (Sheet 2 of 2)

2	Power - Deep Sx		
	Deep Sx Enabled Values: Yes/ No - This setting enables / disables support for Deep Sx operation. For further details see Comet Lake V Platform Controller Hub EDS. Note: Support for Deep Sx is board design dependent.	CML-V	Yes

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

PCH Thermal Reporting

3

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

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

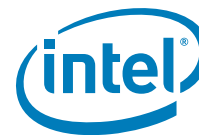


Table 2-12. - Debug (Sheet 1 of 4)

Click on Debug in the left tabs menu> IDLM is expanded by default:			
<div> <div>▼ IDLM</div> <div>1</div> </div>			
Parameter		Value	
IDLM Binary			This allows an IDLM binary to be merged in
#	Parameter	Platform	Settings
1	IDLM		
	IDLM Binary This allows an IDLM binary to be merged into output image built by Intel® FIT.	CML-V	
Click on Debug in the left tabs menu> Delayed Authentication Mode Configuration is expanded by default:			
<div> <div>▼ Delayed Authentication Mode Configuration</div> <div>2</div> </div>			
Parameter		Value	
Delayed Authentication Mode Enabled		No	This setting enables Delayed Authentica
2	Delayed Authentication Mode Configuration		
	Delayed Authentication Mode Enabled Values: Yes/No - This setting enables Delayed Authentication Mode on the platform.	CML-V	No
Click on Debug in the left tabs menu> Intel® Trace Hub Technology is expanded by default:			
<div> <div>▼ Intel(R) Trace Hub Technology</div> <div>3</div> </div>			
Parameter		Value	
Intel(R) Trace Hub Binary		C:\Users\jlwhismo\Desktop\CM...	This loads the Intel(R) Trace Hub binary that will be m
Intel(R) Trace Hub Emergency Mode Enabled		No	When enabled, Intel(R) ME programs Intel(R) Trace h
Intel(R) Trace Hub Debug Messages Enabled		No	Intel(R) Trace Hub Debug Messages Enabled - When s
Unlock Token		C:\Users\jlwhismo\Desktop\CM...	This allows the OEM to input an Unlock Token binary f
Intel(R) Trace Hub Soft Enable		No	When set to Yes, enables Intel(R) ME FW trace messa
#	Parameter	Platform	Settings
3	Intel® Trace Hub Technology		



Table 2-12. - Debug (Sheet 2 of 4)

	<b>Intel® Trace Hub Binary</b> - This loads the Intel® Trace Hub binary that will be merged into the output image generated by the Intel® FIT tool.	CML-V	Trace Hub Binary
	<b>Intel® Trace Hub Emergency Mode Enabled</b> <b>Values: Yes/No</b> - This setting enable / disables Intel® Trace Hub in the firmware base image.	CML-V	No
	<b>Intel® Trace Hub Debug Message Enabled</b> <b>Values: Yes/No</b> - This setting enables/disables the Intel® Trace Hub debug messages. <b>Note:</b> When enabling this setting you also need to enable Intel® Trace Hub Soft Enable setting for proper operation.	CML-V	Yes
	<b>Unlock Token</b> This allows the OEM to input an Unlock Token binary file for closed chassis debug.	CML-V	
	<b>Intel® Trace Hub Soft Enable</b> <b>Values: Yes/No</b> - This setting configures the Intel® Trace Hub soft enable. <b>Note:</b> When enabling this setting you also need to enable Intel® Trace Hub Debug Messages setting for proper operation.	CML-V	No
Click on Debug in the left tabs menu> Intel® ME Debugging Overrides is expanded by default:			
<div> <div>▼ Intel(R) ME Firmware Debugging Overrides</div> <div>4</div> </div>			
Parameter	Value		
Debug Override Pre-Production Silicon	0x00000008	Allows the OEM to control FW features to assist with	
Debug Override Production Silicon	0x00000000	Allows the OEM to control FW features to assist with	
Intel(R) ME Reset Behavior	Intel(R) ME Alternate image boot	This setting determines Intel(R) ME behavior when b	
Enable Intel(R) ME Reset Capture on CLR_RST#	No	This setting configures Intel(R) ME behavior when it	
Firmware ROM Bypass	No	This setting enables / disables firmware ROM bypass	
AFS Idle Flash Reclaim Enabled	Yes	This controls enabling / disabling of Intel(R) ME AFS	
#	Parameter	Platform	Settings
4	Intel® CSME Firmware Debugging Overrides		
	<b>Debug Override Pre-Production Silicon</b> - Allows the OEM to control FW features to assist with pre-production platform debugging. This control has no effect if used on production silicon. <b>Bit 0:</b> Disable DRAM_INIT_DONE (default timeout 60 seconds) <b>Bit 1:</b> Disable Host Reset Timer <b>Bit 2:</b> Disable CPU_RESET_DONE timeout <b>Bit 3:</b> Reserved <b>Bit 4:</b> Disable Intel® CSME Power Gating <b>Bit 5:</b> Reserved <b>Bit 6:</b> Secure Boot debug hook. Used to shorten wait time before ENF shutdown. <b>Bit 7:</b> Force real FPFs on preproduction (default is to use flash) <b>Bit 8:</b> Secure Boot debug hook. Used to reduce S3 or FFS optimization tries. <b>Bit 9:</b> Reserved <b>Bit 10:</b> Override power package to always enter M3. <b>Note:</b> Certain options do not work when the descriptor is locked.	CML-V	0x00000000

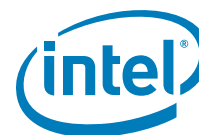


Table 2-12. - Debug (Sheet 3 of 4)

	<b>Debug Override Production Silicon</b> - Allows the OEM to control FW features to assist with production platform debugging. <b>Bit 0:</b> Extend DRAM_INIT_DONE timeout to 30 minutes (default timeout 15 seconds) <b>Bit 1:</b> Disable Host Reset Timer <b>Bit 2:</b> Disable CPU_RESET_DONE timeout <b>Note:</b> Certain options do not work when the descriptor is locked.	CML-V	0x00000000
	<b>Intel® CSME Reset Behavior</b> This setting determines Intel® CSME 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-V	Intel® ME will Halt
	<b>Enable Intel® ME Reset Capture on CLR_RST#</b> <b>Values: Yes/No</b> - This setting configures Intel® ME behavior when it resets during CLR_RST#1. <b>Note:</b> The recommended default for this setting is "No".	CMP-V	No
	<b>Firmware ROM Bypass</b> <b>Values: Yes/No</b> - This setting enables / disables firmware ROM bypass. <b>Note:</b> This setting only has affect when the firmware being used has ROM Bypass code present.	CML-V	No
	<b>ASF Idle Flash Reclaim Enabled</b> <b>Values: Yes / No</b> This controls enabling / disable the Intel® AFS Idle flash reclaim capabilities.  <b>Note:</b> This setting should be used for debug purposes only.	CML-V	Yes

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

▼ Direct Connect Interface Configuration

5

Parameter	Value	Help Text
Direct Connect Interface (DCI) ...	Yes	This setting enables / disables the DCI interface used for Intel(R) Tr...

#	Parameter	Platform	Settings
5	Debug - Direct Connection Interface Configuration		
	Direct Connect Interface (DCI) Enabled <b>Values: Yes/No</b> - This setting enables / disables the DCI interface used for Intel® Trace Hub debugging.	CML-V	No

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

▼ eSPI Feature Overrides

6

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

#	Parameter	Platform	Settings
6	eSPI Feature Overrides		



Table 2-12. - Debug (Sheet 4 of 4)

	<b>eSPI / EC Low Frequency Debug Override</b> When enabled this setting will divide eSPI clock frequency by 8.  <b>Note:</b> This setting should only be used for debugging purposes. Leaving this setting enable will impact eSPI performance.	CML-V	No No



Table 2-13. - CPU Straps (Sheet 1 of 3)

Click on CPU Straps in the left tabs menu> CPU Straps are expanded by default:			
<div> <div>▼ CPU Straps</div> <div>1</div> </div>			
Parameter	Value		
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.	
GT_US VR Type	SVID	This setting determines the GT Unslice domain VR ty	
Ring VR Type	SVID	This setting determines the Ring domain VR type. Se	
IA Power Plane VR	SVID	This setting determines the IA core domain VR type.	
SA VR Type	SVID	This setting determines the SA core domain VR type.	
SE Key Mode	0x0	Note: This strap should be left at the recommended i	
JTAG Power Disable	No JTAG Power on C10 and Lo...	This setting determines if JTAG power will be mainta	
Processor Boot Max Frequency	Yes	This setting determines if the processor will operate	
Flex Ratio	0x0	This setting controls the maximum processor non-tur	
BIST Initialization	No	This setting determines if BIST will be run at platform	
Number of Active Cores	All Cores Active	This setting controls the number of active processor	
Disable Hyperthreading	No	This setting control enabling / disabling of Hyper thre	
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 I	
IA SVID Address	0x0	This setting determines the IA SVID address. See Prt	
SA SVID Address	0x2	This setting determines the SA SVID address. See Pr	
#	Parameter	Platform	Settings
1	CPU Straps - CPU Straps		

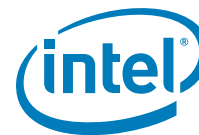


Table 2-13. - CPU Straps (Sheet 2 of 3)

	<b>SVID Presence</b> <b>Value: SVID is Present/SVID is not Present</b> This setting determines if SVID rails are present on the platform. See Processor EDS for details.	CML-V	SVID is Present
	<b>Platform IMON</b> This strap should be left at the recommended default setting.	CML-V	Enabled
	<b>GT_S VR Type</b> <b>Value: SVID/Fixed VR</b> This setting determines the GT slice domain VR type. See Processor EDS for details.	CML-V	SVID
	<b>GT_US VR Type</b> <b>Value: SVID/Fixed VR</b> This setting determines the GT Unslice domain VR type. See Processor EDS for details.	CML-V	SVID
	<b>Ring VR Type</b> <b>Value: SVID/Fixed VR</b> This setting determines the Ring domain VR type. See Processor EDS for details.	CML-V	SVID
	<b>IA Power Plane VR</b> <b>Value: SVID/Fixed VR</b> This setting determines the IA core domain VR type. See Processor EDS for details.	CML-V	SVID
	<b>SA VR Type</b> <b>Value: SVID/Fixed VR</b> This setting determines the SA core domain VR type. See Processor EDS for details.	CML-V	Fixed VR
	<b>SE Key Mode</b> <b>Note:</b> This strap should be left at the recommended default setting.	CML-V	0x0
	<b>JTAG Power Disable</b> <b>Values: Yes - JTAG Power on C10 and Lower/No - No Power on C10 and Lower</b> This setting determines if JTAG power will be maintained on C10 or lower power states. <b>Note:</b> This strap is intended for debugging purposes only.	CML-V	No
	<b>Processor Boot Max Frequency</b> <b>Values: Yes/No</b> This setting determines if the processor will operate at maximum frequency at power-on and boot. <b>Note:</b> This strap is intended for debugging purposes only.	CML-V	Yes
	<b>Flex Ratio</b> This setting controls the maximum processor non-turbo ratio. <b>Note:</b> This strap is intended for debugging purposes only. See BIOS Spec for more details on maximum processor non-turbo ratio configuration.	CML-V	0x0
	<b>BIST Initialization</b> <b>Values: Yes/No</b> This setting determines if BIST will be run at platform reset after BIOS requested actions. <b>Note:</b> This strap is intended for debugging purposes only.	CML-V	No
	<b>Number of Active Cores</b> <b>Values: All, 1, 2, 3, 4, 5, 6, 7, 8</b> This setting controls the number of active processor cores. <b>Note:</b> This strap is intended for debugging purposes only. See BIOS Spec for more details on enabling or disabling processor cores.	CML-V	All
	<b>Disable Hyperthreading</b> <b>Values: Yes/No</b> This setting controls enabling or disabling of Hyper threading. <b>Note:</b> This strap is intended for debugging purposes only. See BIOS Spec for more details on enabling / disabling Hyperthreading.	CML-V	No
	<b>Six Core CPU Configuration</b> <b>Value: Not Six Core/Six Core</b> This setting determines if the board supports six core processor configuration.	CML-V	Not Six Core
	<b>IA VR Offset VID</b> <b>Value: Above 1.52v Not Allowed/Above 1.52v Allowed</b> This setting determines if output voltage higher than 1.52v is allowed for 8 or higher core count processors.	CML-V	Above 1.52v Not Allowed

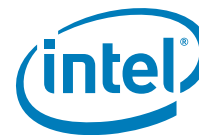


Table 2-13. - CPU Straps (Sheet 3 of 3)

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

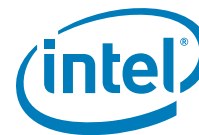


Table 2-14. - Flex I/O Straps (Sheet 1 of 7)

Click on Flex I/O in the left tabs menu> Intel® RST for PCIe Configuration is expanded by default:			
▼ Intel(R) RST for PCIe Configuration 1			
Parameter	Value		
PCIe Controller 3 Port 1 SRIS Enabled	No	This is used to configure SRIS Port 1 for Intel(R) RST for PCI	
PCIe Controller 3 Port 2 SRIS Enabled	No	This is used to configure SRIS Port 2 for Intel(R) RST for PCI	
PCIe Controller 3 Port 3 SRIS Enabled	No	This is used to configure SRIS Port 1 for Intel(R) RST for PCI	
PCIe Controller 3 Port 4 SRIS Enabled	No	This is used to configure SRIS Port 4 for Intel(R) RST for PCI	
PCIe Controller 5 Port 1 SRIS Enabled	No	This is used to configure SRIS Port 1 for Intel(R) RST for PCI	
PCIe Controller 5 Port 2 SRIS Enabled	No	This is used to configure SRIS Port 2 for Intel(R) RST for PCI	
PCIe Controller 5 Port 3 SRIS Enabled	No	This is used to configure SRIS Port 3 for Intel(R) RST for PCI	
PCIe Controller 5 Port 4 SRIS Enabled	No	This is used to configure SRIS Port 4 for Intel(R) RST for PCI	
PCIe Controller 6 Port 1 SRIS Enabled	No	This is used to configure SRIS Port 1 for Intel(R) RST for PCI	
PCIe Controller 6 Port 2 SRIS Enabled	No	This is used to configure SRIS Port 2 for Intel(R) RST for PCI	
PCIe Controller 6 Port 3 SRIS Enabled	No	This is used to configure SRIS Port 3 for Intel(R) RST for PCI	
PCIe Controller 6 Port 4 SRIS Enabled	No	This is used to configure SRIS Port 4 for Intel(R) RST for PCI	
Intel(R) RST for PCIe-C1 Select x2 or x4	x4	This is used to configure NAND Cycle routers for the Intel(R)	
Intel(R) RST for PCIe-C2 Select x2 or x4	x4	This is used to configure NAND Cycle routers for the Intel(R)	
Intel(R) RST for PCIe-C3 Select x2 or x4	x4	This is used to configure NAND Cycle routers for the Intel(R)	
Intel® RST for PCIe Controller 1	1x4	This is used to configure PCIe Controller 1 for Intel(R) RST f	
Intel® RST for PCIe Controller 2	1x4	This is used to configure PCIe Controller 2 for Intel(R) RST f	
Intel® RST for PCIe Controller 3	2x2	This is used to configure PCIe Controller 3 for Intel(R) RST f	
#	Parameter	Platform	Settings
1	Flex I/O - Intel® RST for PCIe Configuration		
	<b>PCIe Controller 3 Port 1 SRIS Enabled</b> <b>Values: Yes/ No</b> - This is used to configure SRIS Port 1 for Intel® RST for PCIe on PCIe Controller 3. <b>Note:</b> Configuration of this setting is only required if the NVM device will be connected external SATA Express cable.	CML-V	No
	<b>PCIe Controller 3 Port 2 SRIS Enabled</b> <b>Values: Yes/ No</b> - This is used to configure SRIS Port 2 for Intel® RST for PCIe on PCIe Controller 3. <b>Note:</b> Configuration of this setting is only required if the NVM device will be connected external SATA Express cable.	CML-V	No
	<b>PCIe Controller 3 Port 3 SRIS Enabled</b> <b>Values: Yes/ No</b> - This is used to configure SRIS Port 3 for Intel® RST for PCIe on PCIe Controller 3. <b>Note:</b> Configuration of this setting is only required if the NVM device will be connected external SATA Express cable.	CML-V	No

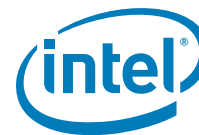


Table 2-14. - Flex I/O Straps (Sheet 2 of 7)

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

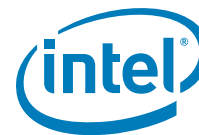


Table 2-14. - Flex I/O Straps (Sheet 3 of 7)

Intel® RST for PCIe Controller 3 Values: 1x4, 2x2 - This is used to configure PCIe Controller 3 for Intel® RST for PCIe interface as either x2 or x4 lane operation on PCIe Controller 3.		CML-V	1x4
Click on Flex I/O in the left tabs menu> PCIe Lane Reversal Configuration is expanded by default:			
▼ PCIe Lane Reversal Configuration <b>2</b>			
Parameter	Value		
PCIe Controller 1 Lane Reversal Enabled	No	This setting allows the PCIe lanes on Controller 1	
PCIe Controller 2 Lane Reversal Enabled	No	This setting allows the PCIe lanes on Controller 2	
PCIe Controller 3 Lane Reversal Enabled	No	This setting allows the PCIe lanes on Controller 3	
PCIe Controller 4 Lane Reversal Enabled	No	This setting allows the PCIe lanes on Controller 4	
PCIe Controller 5 Lane Reversal Enabled	No	This setting allows the PCIe lanes on Controller 5	
PCIe Controller 6 Lane Reversal Enabled	No	This setting allows the PCIe lanes on Controller 6	
#	Parameter	Platform	Settings
<b>2</b>	Flex I/O - PCIe Lane Reversal Configuration		
	PCIe Controller 1 Lane Reversal Enabled Values: Yes/ No - This setting allows the PCIe lanes on Controller 1 to be reversed. Note: Refer to EDS for PCIe supported port configurations.	CML-V	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-V	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-V	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-V	No
	PCIe Controller 5 Lane Reversal Enabled Values: Yes/ No - This setting allows the PCIe lanes on Controller 5 to be reversed. Note: Refer to EDS for PCIe supported port configurations.	CML-V	No
	PCIe Controller 6 Lane Reversal Enabled Values: Yes/ No - This setting allows the PCIe lanes on Controller 6 to be reversed. Note: Refer to EDS for PCIe supported port configurations.	CML-V	No
Click on Flex I/O in the left tabs menu> PCIe Port Configuration is expanded by default:			

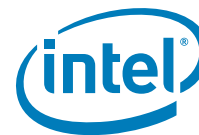


Table 2-14. - Flex I/O Straps (Sheet 4 of 7)

▼ PCIe Port Configuration <b>3</b>			
Parameter	Value		
PCIe Controller 1 (Port 1-4)	4x1	This setting controls PCIe Port configurations for PCIe Controller 1.	
PCIe Controller 2 (Port 5-8)	1x4	This setting controls PCIe Port configurations for PCIe Controller 2.	
PCIe Controller 3 (Port 9-12)	1x4	This setting controls PCIe Port configurations for PCIe Controller 3.	
PCIe Controller 4 (Port 13-16)	4x1	This setting controls PCIe Port configurations for PCIe Controller 4.	
PCIe Controller 5 (Port 17-20)	4x1	Setting of this field depend on what PCIe ports 17-20 configurator	
PCIe Controller 2 (Port 21-24)	4x1	This setting controls PCIe Port configurations for PCIe Controller 6.	
#	Parameter	Platform	Settings
<b>3</b>	Flex I/O - PCIe Port Configuration		
	<b>PCIe Controller 1 (Port 1-4)</b> <b>Values: 4x1, (1x2, 2x1), 2x2, 1x4</b> - This setting controls PCIe Port configurations for PCIe Controller 1. For further details see Comet Lake V Platform Controller Hub EDS.	CML-V	4x1
	<b>PCIe Controller 2 (Port 5-8)</b> <b>Values: 4x1, (1x2, 2x1), 2x2, 1x4</b> - This setting controls PCIe Port configurations for PCIe Controller 2. For further details see Comet Lake V Platform Controller Hub EDS.	CML-V	1x4
	<b>PCIe Controller 3 (Port 9-12)</b> <b>Values: 4x1, (1x2, 2x1), 2x2, 1x4</b> - This setting controls PCIe Port configurations for PCIe Controller 3. For further details see Comet Lake V Platform Controller Hub EDS.	CML-V	1x4
	<b>PCIe Controller 4 (Port 13-16)</b> <b>Values: 4x1, (1x2, 2x1), 2x2, 1x4</b> - This setting controls PCIe Port configurations for PCIe Controller 4. For further details see Comet Lake V Platform Controller Hub EDS.	CML-V	4x1
	<b>PCIe Controller 5 (Port 17-20)</b> <b>Values: 4x1, (1x2, 2x1), 2x2, 1x4</b> - This setting controls PCIe Port configurations for PCIe Controller 5. For further details see Comet Lake V Platform Controller Hub EDS.	CML-V	1x4
	<b>PCIe Controller 6 (Port 21-24)</b> <b>Values: 4x1, (1x2, 2x1), 2x2, 1x4</b> - This setting controls PCIe Port configurations for PCIe Controller 6. For further details see Comet Lake V Platform Controller Hub EDS.	CML-V	1x4
Click on Flex I/O in the left tabs menu> SATA / PCIe Combo Port Configuration is expanded by default:			



Table 2-14. - Flex I/O Straps (Sheet 5 of 7)

▼ SATA / PCIe Combo Port Configuration <span style="color: red; font-weight: bold; border: 1px solid red; border-radius: 50%; padding: 2px 5px;">4</span>			
Parameter	Value		
SATA / PCIe Combo Port 0 and 2 Mode Select	PCIe CLKREQ#	The corresponding CLKREQ# GPIO can only function as DEVSLP# if S	
SATA / PCIe Combo Port 1 and 3 Mode Select	PCIe CLKREQ#	The corresponding CLKREQ# GPIO can only function as DEVSLP# if S	
SATA / PCIe Combo Port 0	PCIe	This setting configures the PCIe port to operate as either PCIe Port 9	
SATA / PCIe Combo Port 1	PCIe	This setting configures the PCIe port to operate as either PCIe Port 1	
SATA / PCIe Combo Port 2	SATA	This setting configures the PCIe port to operate as either PCIe Port 1	
SATA / PCIe Combo Port 3	SATA	This setting configures the PCIe port to operate as either PCIe Port 1	
SATA / PCIe Combo Port 4	GPIO Polarity SATA	This setting configures the PCIe port to operate as either PCIe Port 1	
SATA / PCIe Combo Port 5	GPIO Polarity SATA	This setting configures the PCIe port to operate as either PCIe Port 1	
SATA / PCIe Combo Port 6	GPIO Polarity SATA	This setting configures the PCIe port to operate as either PCIe Port 1	
SATA / PCIe Combo Port 7	PCIe	This setting configures the PCIe port to operate as either PCIe Port 1	
SATA / PCIe Combo Port 8	PCIe	This setting configures the PCIe port to operate as either PCIe Port 1	
SATA / PCIe Combo Port 9	PCIe	This setting configures the PCIe port to operate as either PCIe Port 2	
#	Parameter	Platform	Settings
<span style="color: red; font-weight: bold; border: 1px solid red; border-radius: 50%; padding: 2px 5px;">4</span>	Flex I/O - SATA / PCIe Combo Port Configuration		
	<b>SATA / PCIe Combo Port 0 and 2 Mode Select</b> <i>Note:</i> Leave this setting at default value	CML-V	PCIe CLKREQ#
	<b>SATA / PCIe Combo Port 1 and 3 Mode Select</b> <i>Note:</i> Leave this setting at default value	CML-V	PCIe CLKREQ#
	<b>SATA / PCIe Combo Port 0</b> <b>Values:</b> SATA, PCIe (or GbE), GPIO - This setting configures the PCIe port to operate as either: PCIe Port 9 or SATA Port 0a For further details on Flex I/O see Comet Lake V Platform Controller Hub EDS.	CML-V	PCIe
	<b>SATA / PCIe Combo Port 1</b> <b>Values:</b> SATA, PCIe, GPIO Polarity PCIe, GPIO Polarity SATA - This setting configures the PCIe port to operate as either: PCIe Port 10 or SATA Port 1a For further details on Flex I/O see Comet Lake V Platform Controller Hub EDS.	CML-V	PCIe
	<b>SATA / PCIe Combo Port 2</b> <b>Values:</b> SATA, PCIe, GPIO Polarity PCIe, GPIO Polarity SATA - This setting configures the PCIe port to operate as either: PCIe Port 13 or SATA Port 0b For further details on Flex I/O see Comet Lake V Platform Controller Hub EDS.	CML-V	PCIe

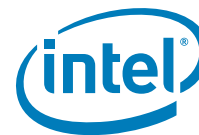


Table 2-14. - Flex I/O Straps (Sheet 6 of 7)

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



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

5	Flex I/O - USB3 Port Configuration										
	<b>USB3 / PCIe Combo Port 0</b> <b>Values: USB3, PCIe</b> 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 V Platform Controller Hub EDS.	CML-V	USB3								
	<b>USB3 / PCIe Combo Port 1</b> <b>Values: USB3, PCIe</b> 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 V Platform Controller Hub EDS.	CML-V	USB3								
	<b>USB3 / PCIe Combo Port 2</b> <b>Values: USB3, PCIe</b> 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 V Platform Controller Hub EDS.	CML-V	PCIe								
	<b>USB3 / PCIe Combo Port 3</b> <b>Values: USB3, PCIe</b> 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 V Platform Controller Hub EDS.	CML-V	PCIe								
Click on Flex I/O in the left tabs menu> PCIe gen3 PLL Clock Control is expanded by default:											
<div> <div>▼ PCIe gen3 PLL Clock Control</div> <div>6</div> </div>											
<table border="1"> <thead> <tr> <th>Parameter</th><th>Value</th><th colspan="2"></th></tr> </thead> <tbody> <tr> <td>Secondary Gen3 PLL Enabled</td><td>No</td><td colspan="2">This setting determines which Gen3 PLL so</td></tr> </tbody> </table>				Parameter	Value			Secondary Gen3 PLL Enabled	No	This setting determines which Gen3 PLL so	
Parameter	Value										
Secondary Gen3 PLL Enabled	No	This setting determines which Gen3 PLL so									
#	Parameter	Platform	Settings								
6	Flex I/O - PCIe gen3 PLL Clock Control										
	<b>Secondary Gen3 PLL Enabled</b> <b>Values: Yes, No</b> This setting determines which Gen3 PLL source clock PCIe Controller 6 (Port 21-24) will use.  <b>Note:</b> When the Secondary Gen3 PLL option is disabled PCIe Controller 6 (Port 21-24) will use Primary Gen3 PLL as the source clock.	CML-V	Yes								

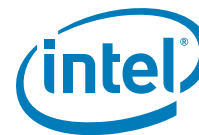


Table 2-15. - GPIO (Sheet 1 of 3)

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

▼ LAN / GPIO Select

1

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

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

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

▼ WLAN / GPIO Select

2

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

#	Parameter	Platform	Settings
2	GPIO - WLAN / GPIO Select		
	SLP_WLAN# / GDP9 Signal Configuration	CML-V	SLP_WLAN#

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

▼ Platform Power / GPIO

3

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

#	Parameter	Platform	Settings
3	GPIO - Platform Power / GPIO		
	SLP_A# / GPD6 Signal Configuration	CML-V	SLP_A#

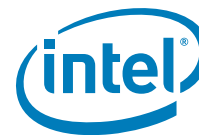


Table 2-15. - GPIO (Sheet 2 of 3)

	SLP_S3# / GPD4 Signal Configuration	CML-V	SLP_S3#
	SLP_S4# / GPD5 Signal Configuration	CML-V	SLP_S4#
	SLP_S5# / GPD10 Signal Configuration	CML-V	SLP_S5#
Click on GPIO in the left tabs menu> ME Feature Pins is expanded by default:			
<div> <div>ME Feature Pins</div> <div>4</div> </div>			
Parameter		Value	
Intel(R) Precise Touch and Stylus Reset GPIO Select		None	Configure Intel(R) Precise
Intel(R) Precise Touch and Stylus Interrupt GPIO Select		None	Configure Intel(R) Precise
#	Parameter	Platform	Settings
4	GPIO - ME Feature Pins		
	Intel® Precise Touch and Stylus Reset GPIO Select Configure Intel® Precise Touch and Stylus Reset GPIO.	CML-V	None
	Intel® Precise Touch and Stylus Interrupt GPIO Select Configure Intel® Precise Touch and Stylus Interrupt GPIO.	CML-V	None
Click on GPIO in the left tabs menu> Touch Controller Pins is expanded by default:			
<div> <div>Touch Controller Pins</div> <div>5</div> </div>			
Parameter		Value	
GPP_E_1		GPIO	-
GPP_E_2		GPIO	-
GPP_E_10		GPIO	-
GPP_E_11		GPIO	-
GPP_E_12		GPIO	-
GPP_E_13		GPIO	-
#	Parameter	Platform	Settings
5	GPIO - Touch Controller Pins		
	GPP_E_1	CML-V	GPIO
	GPP_E_2	CML-V	GPIO
	GPP_E_10	CML-V	GPIO
	GPP_E_11	CML-V	GPIO
	GPP_E_12	CML-V	GPIO
	GPP_E_13	CML-V	GPIO
Click on GPIO in the left tabs menu> SMLink1 Pins is expanded by default:			

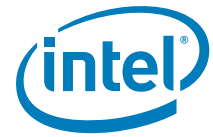


Table 2-15. - GPIO (Sheet 3 of 3)

▼ SMLink1 Pins 6			
Parameter		Value	Help
GPP_C_6		GPIO	-
GPP_C_7		GPIO	-
#	Parameter	Platform	Settings
6	SMLink1 Pins		
	GPP_C_6	CML-V	GPIOGPIO
	GPP_C_7	CML-V	GPIOGPIO



Table 2-16. - Intel® Precise Touch and Stylus

Click on Intel® Precise Touch and Stylus in the left tabs menu> Integrated Touch Configuration is expanded by default:			
▼ IntegratedTouchConfiguration <b>1</b>			
Parameter		Value	
Intel(R) Precise Touch and Stylus Enabled		No	-
#	Parameter	Platform	Settings
<b>1</b>	Integrated Touch Configuration		
	Intel® Precise Touch and Stylus Enabled	CML-V	No
Click on Intel® Precise Touch and Stylus in the left tabs menu> Integrated Touch And Stylus Configuration is expanded by default:			
▼ Intel Precise Touch And Stylus Configuration <b>2</b>			
Parameter		Value	
Intel(R) Precise Touch and Stylus Controller 1 Maximum Frequency		30 MHz	This setting all
Touch Spread Spectrum Clock Enabled		Yes	This setting er
<b>2</b>	Intel PerciseTouch and Stylus Configuration		
	Intel® Precise Touch and Stylus Controller 1 Maximum Frequency	CML-V	30MHz
	Touch Spread Spectrum Clock Enabled Values: Yes/No This setting enabled the use of the spread spectrum clock when generating the SPI_CLK for touch.	CML-V	Yes



Table 2-17. - FW Update Image Build

Click on FW Update Image Build in the left tabs menu> ME Image is expanded by default:															
<div> <div>▼ ME Image</div> <div>1</div> </div>															
<table> <tr> <th>Parameter</th><th>Value</th><th colspan="2"></th></tr> <tr> <td>ME Binary File</td><td></td><td colspan="2">This loads the Embedded Controller binary</td></tr> </table>				Parameter	Value			ME Binary File		This loads the Embedded Controller binary					
Parameter	Value														
ME Binary File		This loads the Embedded Controller binary													
#	Parameter	Platform	Settings												
	<p>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:</p> <p>Intel® ME, PMC, OEM KM, ISH, iUnit</p>														
1	ME Image														
	<p>ME Binary Image</p> <p>Values: Binary File</p> <p>This loads the Embedded Controller binary that will be merged into the FWUpdate image generated by the Intel® FIT tool.</p>	CML-V	ME Binary												
Click on FW Update Image Build in the left tabs menu> PMC Image is expanded by default:															
<div> <div>▼ PMC Image</div> <div>2</div> </div>															
<table> <tr> <th>Parameter</th><th>Value</th><th colspan="2"></th></tr> <tr> <td>PMC Max Length</td><td>0x20000</td><td colspan="2">-</td></tr> <tr> <td>PMC Binary File</td><td></td><td colspan="2">This loads the PMC binary that will be mer</td></tr> </table>				Parameter	Value			PMC Max Length	0x20000	-		PMC Binary File		This loads the PMC binary that will be mer	
Parameter	Value														
PMC Max Length	0x20000	-													
PMC Binary File		This loads the PMC binary that will be mer													
#	Parameter	Platform	Settings												
2	PMC Image														
	<p>PMC Max Length</p> <p>Note: This value will be automatically populated by Intel® FIT during image build.</p>														
	<p>PMC Binary Image</p> <p>Values: Binary File</p> <p>This loads the PMC binary that will be merged into the FWUpdate image generated by the Intel® FIT tool.</p>	CML-V	PMC Binary												
Click on FW Update Image Build in the left tabs menu> OEM KM Image is expanded by default:															



Table 2-17. - FW Update Image Build

▼ OEM KM Image <span style="color: red; font-weight: bold; border: 1px solid red; border-radius: 50%; padding: 2px 5px;">3</span>			
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
<span style="color: red; font-weight: bold; border: 1px solid red; border-radius: 50%; padding: 2px 5px;">3</span>	OEM KM Image		
	OEM KM Enable Values: Enabled/Disabled This setting Enables / Disables OEM KM in the FWUpdate image.	CML-V	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-V	OEM KM Binary
Click on FW Update Image Build in the left tabs menu> I SH Image is expanded by default:			
▼ PCH Configuration Sub-Partition <span style="color: red; font-weight: bold; border: 1px solid red; border-radius: 50%; padding: 2px 5px;">4</span>			
Parameter	Value		
Length	0x1000	-	
PCH Configuration File		This loads the PCH Configuration binary that will be merged into the output im	
#	Parameter	Platform	Settings
<span style="color: red; font-weight: bold; border: 1px solid red; border-radius: 50%; padding: 2px 5px;">4</span>	PCH Configuration Sub-Partition This loads the PCH Configuration binary that will be merged in the output image generated by the Intel® FIT tool.		
	Length - This displays the length of the PCH Configuration Sub-Partition. Note: This value will be automatically populated by Intel® FIT during image build.		
	PCH Configuration File Navigate to path to load PCHC.bin file. This loads the PCH Configuration binary.	CML-V	PCHC.bin

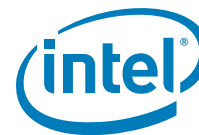


Table 2-18. - Intel® FIT - Build Image

1

2

3

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

▼ Cryptor Region

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

▼ BIOS Region

▼ Ifwi: Intel(R) Me and Pmc Region

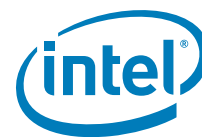
Parameter	Value	Help Text
Intel(R) ME Binary File		This loads the Intel(R) ME binary that will be merged into the output image generated by the Int...
Major Version	0	This displays Major revision number of the currently loaded Intel(R) ME binary.
Minor Version	0	This displays Minor revision number of the currently loaded Intel(R) ME binary.
Hotfix Version	0	This displays Hot-Fix revision number of the currently loaded Intel(R) ME binary.

01/24/2019 12:21:36  
Using vsccommn.bin with timestamp 18:12:31 12/11/2018 GMT

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

Log file written to fit.log

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

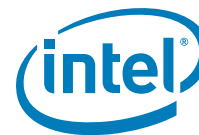
Mobile CRBs have the SPI Flash devices soldered down. As a result, to program the SPI Flash for mobile CRBs, follow these steps:

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.

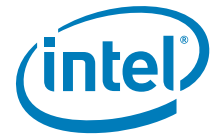
```
FPT Operation Passed
```

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.

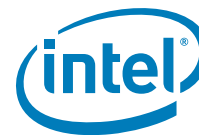
4. Use fptw.exe -greset to perform a G3 power cycle. Next go to [Section 3.3](#) to check the Intel® ME Firmware status.

### 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: 14.5.0.xxxx

Copyright(C) 2005 - 2019, 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, <ol style="list-style-type: none"> <li>1. Enter BIOS menu, then go to the 'Boot' screen</li> <li>2. Change 'Boot Option #1' to be your USB key (ensure USB key is formatted to be DOS bootable)</li> <li>3. Press 'F4' to save settings and reboot</li> </ol>
Hear 3 beeps when platform powers on	Possible device is disconnected or device not found, check <ul style="list-style-type: none"> <li>• platform power and MCP fan power connectors</li> <li>• DIMM memory modules (if applicable for memory down modules)</li> <li>• USB devices (keyboard, mouse, USB key) may be plugged into inactive USB port</li> <li>• missing/incorrect jumpers</li> <li>• missing or poorly socketed MCP</li> </ul>
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: <ul style="list-style-type: none"> <li>• wrong FW selected during Flash image build process</li> <li>• wrong Flash size selected</li> </ul> Re-build image with correct settings and re-flash using Flash burner.

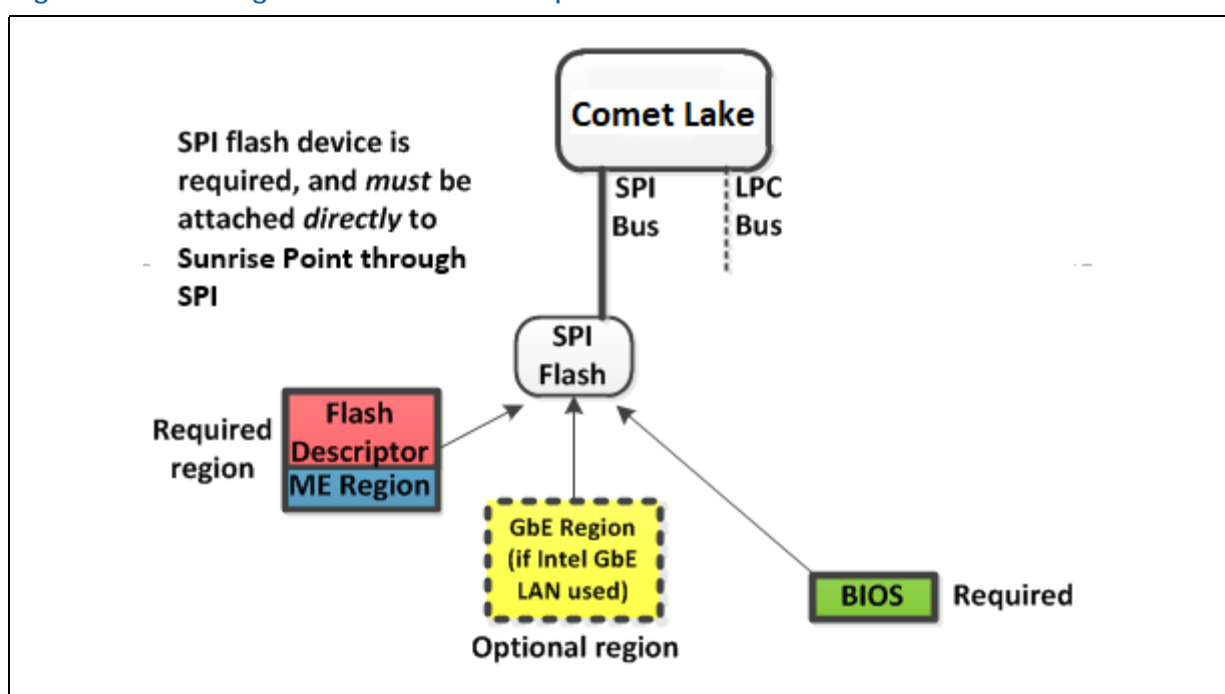
§ §



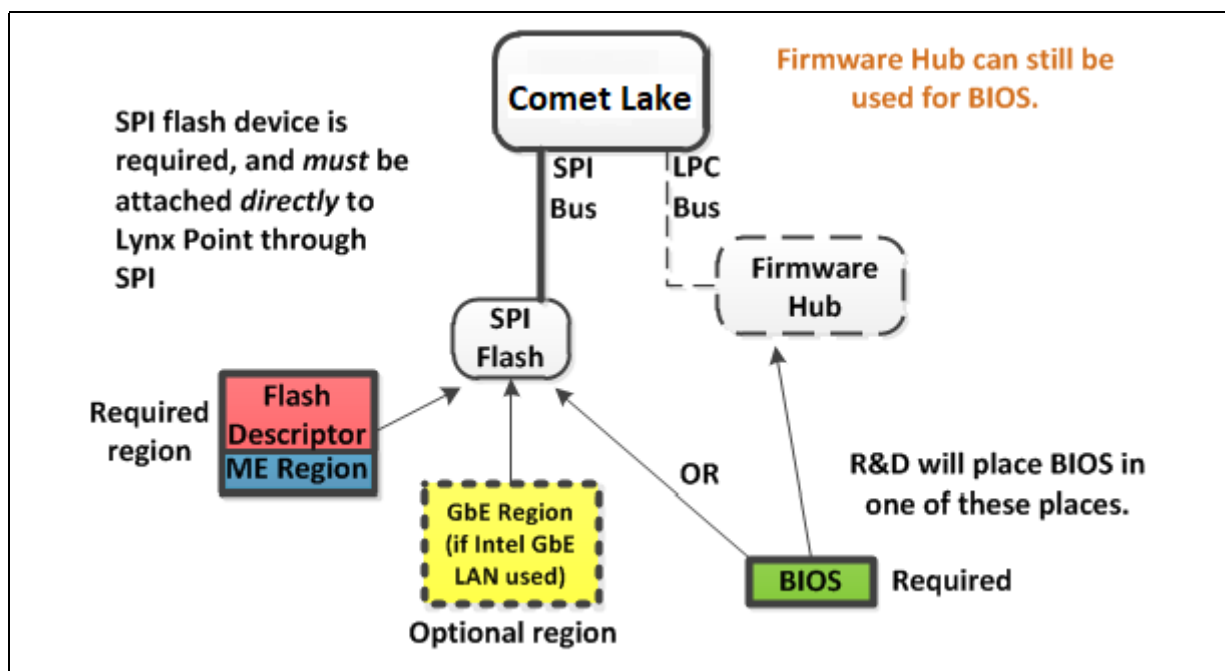
# A Appendix — Flash Configurations

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

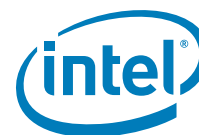
Figure A-1. Configuration “A” — Desktop



### Figure A-2. Configuration “C” — Desktop



§ 2



# 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-V SKUs.

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

In below tables,

Min = Clock Div Max (minimum allowed frequency)

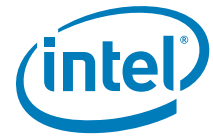
Max = Clock Div Min (maximum allowed frequency)

## B.1 Intel® ICCS SKU Matrix - CNP-H

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

**Table B-1. Intel® ICCS SKU Matrix - CMP-V**

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



## B.2 How to configure CLKREQ# parameters

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

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

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



# C Appendix — Boot Guard Configuration

## C.1 Boot Guard Profiles

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

Table C-1. Profile Description

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

## C.2 Enforcement Policies

Table C-2. Enforcement Policy Description

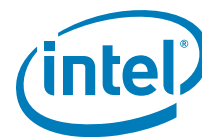
Error Enforcement Policy (ENF)	Enforcement Mode Name	Description
0	Unrestricted Mode	Infinite time before shutdown – don't shutdown the platform, let everything run normally.
1	Remediation Mode	<b>30 minutes</b> before shutdown – enough time to remediate the system, e.g. update BIOS or other data on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



## C.3 OEM Profile Parameters

Table C-3. Profile Parameters Description

Parameter	Description	Settings
<b>Force Boot Guard ACM Enabled (F)</b>	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.	<b>false</b> - Allow the CPU to jump to the legacy reset vector if the Boot Guard Module cannot be successfully loaded. (default)  <b>true</b> - Force the Boot Guard ACM to execute.
<b>Verified Boot Enabled (V)</b>	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.	<b>false</b> - Platform does not perform verified boot (default)  <b>true</b> - Platform performs verified boot
<b>Measured Boot Enabled (M)</b>	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 Skylake implementation of Boot Guard will support measurements into TPM or Intel's Platform Trust Technology.	<b>false</b> - Platform does not perform measured boot (default)  <b>true</b> - Platform performs measured boot
<b>Protect Bios Environment Enabled (PBE)</b>	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.	<b>false</b> - Take no actions to control the environment during execution of the BIOS components (default)  <b>true</b> - Takes actions to control the environment during the execution of the BIOS components.
<b>Error Enforcement Policy (ENF)</b>	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, <ul style="list-style-type: none"> <li>• Allowing platform to continue to boot</li> <li>• Immediate Shutdown</li> <li>• Shutdown with Timeout intervals</li> </ul> When the ENF logic is invoked, PTT or TPM also disconnects.	See <a href="#">Section C-2</a> for details.



# D Appendix — Intel® Platform Trust Technology

## D.1 Intel® Platform Trust Technology

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

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

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



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

The following table describes the configuration matrix required for ISH configuration for the Intel® FIT tool. Please see System Tools User Guide within ME kit, Manufacturing Test with Intel® Converged Security and Management Engine (Intel® ME) Firmware 14 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.

