Cisco UCS Server BIOS Tokens in Intersight Managed Mode

First Published: 2022-06-08

Last Modified: 2024-02-26

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

CONTENTS

Communications, Services, Bias-free Language, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you’re looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Documentation Feedback

To provide feedback about Cisco technical documentation, use the feedback form available in the right pane of every online document.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.

Bias-Free Language

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

CHAPTER 1

Introduction to Intersight Managed Mode Server Bios Tokens

Introduction to Intersight Managed Mode Server BIOS Tokens

Intersight Managed Mode provides two methods for making global modifications to the BIOS settings on servers in Cisco UCS domain. You can create one or more BIOS policies that include a specific grouping of BIOS settings that match the needs of a server or set of servers, or you can use the default BIOS settings for a specific server platform.

Both the BIOS policy and the default BIOS settings for a server platform enables you to fine tune the BIOS settings for a server managed by IMM.

Depending upon the needs of the data center, you can configure BIOS policies for some service profiles and use the BIOS defaults in other service profiles in the same Cisco UCS domain, or you can use only one of them. You can also use IMM to view the actual BIOS settings on a server and determine whether they are meeting current needs.

Cisco Intersight Managed Mode supports the following M5, M6, and M7 servers:

- Cisco UCS X210c M7 Compute Node
- Cisco UCS X410c M7 Compute Node
- Cisco UCS X210c M6 Compute Node
- Cisco UCS C220 M7
- Cisco UCS C240 M7
- Cisco UCS C220 M6
- Cisco UCS C225 M6
- Cisco UCS C240 M6
- Cisco UCS C245 M6
- Cisco UCS C220 M5
- Cisco UCS C240 M5

- Cisco UCS C480 M5
- Cisco UCS B200 M6
- Cisco UCS B200 M5
- Cisco UCS B480 M5

Note The **Version** column in the table denotes the minimum firmware version where the token is supported and its consecutive version support.

Note For tokens having long value description, the **Values** column can be seen blank. In this case, you can scroll down the column to see their values.

Note All tokens also include a 'Platform default' option. The Platform default is identified by the setting in bold font. The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.

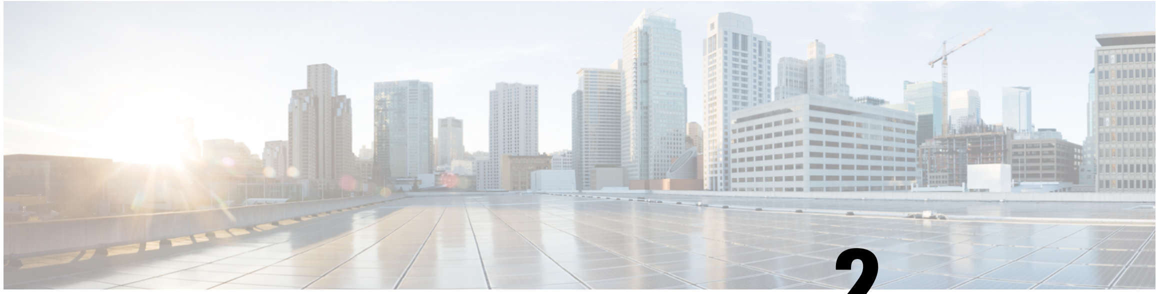
What's New

Note This document includes BIOS token information starting from 4.3(3a) and continue to cover all subsequent versions. It does not cover any versions prior to 4.3(3a).

Table 1: New/Changed BIOS Tokens for 4.3(3a)

BIOS Token	Platform	New/Changed
Trust Domain Extension (TDX)	X410c M7, X210c M7, C220 M7, C240 M7	New
TDX Secure Arbitration Mode (SEAM) Loader	X410c M7, X210c M7, C220 M7, C240 M7	New
SHA384 PCR Bank	X410c M7, X210c M7, C220 M7, C240 M7	New
QpiLinkSpeed	X410c M7, X210c M7, C220 M7, C240 M7	Changed
C1 Auto demotion	X410c M7, X210c M7, C220 M7, C240 M7	Changed
C1 Auto UnDemotion	X410c M7, X210c M7, C220 M7, C240 M7	Changed

For more information on BIOS tokens, see Cisco UCS Server BIOS Tokens in Intersight Managed Mode.



CHAPTER 2

Boot Options BIOS Settings

Boot Options BIOS Settings

The following table lists the boot options BIOS settings that you can configure through a BIOS policy or the default BIOS settings:

Name	Description	Supported Attributes			
		Version	Platform	Values	Dependencies
Number of Retries	Number of attempts to boot.	4.1(1)	B200 M5, B480 M5,C480 M5	Infinite. **13**, 5 • **Infinite**The system attempts all configured boot options and repeats until the system boots or is interrupted manually. • **5, 13**The system attempts all configured boot options and repeats the selected number of times until the system boots or is interrupted. If all attempts fail, the system prompts to continue. Value 13 is the default value for Cisco UCS B200 M5 and 5 is the default value for Cisco UCS B480 M5.	Applicable only when Boot Option Retry is Enabled.
Cool Down Time (sec)	The time to wait (in seconds) before the next boot attempt. This can be one of the following:	4.1(1)	B200 M5, B480 M5,C480 M5	15 sec, 45 sec, **90 sec** • **15, 45, 90**System waits for the selected time in seconds before the next boot attempt.	Applicable only when Boot Option Retry is Enabled.
Boot Option Retry	Whether the BIOS retries NON-EFI based boot options without waiting for user input.	4.1(1)	B200 M5, B480 M5,C480 M5	**Disabled**, Enabled • **Disabled**—Waits for user input before retrying NON-EFI based boot options. • **Enabled**—Continually retries NON-EFI based boot options without waiting for user input.	

Name	Description	Supported Attributes			
		Version	Platform	Values	Dependencies
IPV4 HTTP Support	Enables or disables IPv4 support for HTTP.	4.2(1)	C245 M6, C220 M7, C240 M7, X210c M7, X410c M7	Disabled, **Enabled** • **Disabled**—IPv4 HTTP support is not available. • **Enabled**—IPv4 HTTP support is made available.	The Network Stack token value should be Enabled.
IPV6 HTTP Support	Enables or disables IPv6 support for HTTP.	4.2(1)	C245 M6, C220 M7, C240 M7, X210c M7, X410c M7	Disabled, **Enabled** • **Disabled**—IPv46 HTTP support is not available. • **Enabled**—IPv6 HTTP support is made available.	The Network Stack token value should be Enabled.
IPV4 PXE Support	Enables or disables IPv4 support for PXE.	4.2(1)	C245 M6, C220 M7, C240 M7, X210c M7, X410c M7	Disabled, **Enabled** • **Disabled**—IPv44 PXE support is not available. • **Enabled**—IPv4 PXE support is made available.	
IPV6 PXE Support	Enables or disables IPv6 support for PXE.	4.2(1)	C245 M6, C220 M7, C240 M7, X210c M7, X410c M7	Disabled, **Enabled** • **Disabled**—IPv46 PXE support is not available. • **Enabled**—IPv6 PXE support is made available.	The Network Stack token value should be Enabled.

Name	Description	Supported Attributes			
		Version	Platform	Values	Dependencies
Network Stack	This option allows you to enable or disable the complete network style of the system.	4.1(1), 4.2(1)	C245 M6, B200 M5, B480 M5, C220 M5, C240 M5, C480 M5, C125 M5, C220 M7, C240 M7, X210c M7, X410c M7	Disabled,**Enabled** • **Disabled**—Network Stack support is not available. • **Enabled**—Network Stack support is available.	When disabled, the value set for IPV6 PXE, IPV4HTTP, and IPV6HTTP Support does not impact the system.
Power ON Password	This token requires that you set a BIOS password before using the F2 BIOS configuration. If enabled, password needs to be validated before you access BIOS functions such as IO configuration, BIOS set up, and booting to an operating system using BIOS.	4.1(1), 4.2(1)	C220 M5, C240 M5, C480 M5, C125 M5, C245 M6, C220 M7, C240 M7	**Disabled**, Enabled • **Disabled**—Power On Password is disabled. • **Enabled**—Power On Password is enabled.	
P-SATA Mode	This options allows you to select the P-SATA mode.	4.1(1)	B200 M5, B480 M5, C220 M5, C240 M5, C480 M5	Disabled, **LSI SW RAID** • Disabled—P-SATA mode is disabled • LSI SW RAID—Sets both SATA and sSATA controllers to RAID mode for LSI SW RAID.	

Name	Description	Supported Attributes			
		Version	Platform	Values	Dependencies
SATA Mode	This options allows you to select the SATA mode.	4.1(1)	B200 M5, B480 M5, C220 M5, C240 M5, C480 M5	AHCI, **LSISW RAID**, Disabled • Disabled—SATA mode is disabled • LSI SW RAID—Sets both SATA and sSATA controllers to RAID mode for LSI SW RAID • AHCI	
VMD Enablement	Whether NVMe SSDs that are connected to the PCIe bus can be hot swapped. It also standardizes the LED status light on these drives. LED status lights can be optionally programmed to display specific Failure indicator patterns.	4.1(1)	C220 M5, C240 M5, B200 M5, B480 M5, C220 M7, C240 M7, X210c M7, X410c M7	**Disabled**, Enabled • Disabled—Hot swap of NVMe SSDs that are connected to the PCIe bus is not allowed. • Enabled—Hot swap of NVMe SSDs that are connected to the PCIe bus is allowed.	

CHAPTER 3

Intel Directed IO

Intel Directed IO

The following table lists the Intel directed IO BIOS settings that you can configure through a BIOS policy or the default BIOS settings:

Name	Description	Supported Attributes			
		Versions	Platforms	Values	Dependencies
Intel VT for directed IO	Whether the processor uses Intel Virtualization Technology for Directed I/O (VT-d).	4.1(1), 5.0(1), 5.0(2)	B200 M5, B480 M5, C220 M5, C240 M5, C480 M5, B200 M6, C220 M6, C240 M6, X210c M6, C220 M7, C240 M7, X210c M7, X410c M7	**Enabled**, Disabled • **Disabled**—The processor does not use virtualization technology. • **Enabled**—The processor uses virtualization technology.	
Intel(R) VT-d Coherency Support	Whether the processor supports Intel VT-d Coherency.	4.1(1), 5.0(1), 5.0(2)	B200 M5, B480 M5, C220 M5, C240 M5, C480 M5, B200 M6, C220 M6, C240 M6, X210c M6, C220 M7, C240 M7, X210c M7, X410c M7	Enabled, **Disabled** • **Disabled**—The processor does not support coherency. • **Enabled**—The processor uses VT-d Coherency as required.	

Name	Description	Supported Attributes			
		Versions	Platforms	Values	Dependencies
Intel(R) VT-d Interrupt Remapping	Whether the processor supports Intel VT-d Interrupt Remapping.	4.1(1)	B200 M5, B480 M5, C220 M5, C240 M5, C480 M5	**Enabled**, Disabled • **Disabled**—The processor does not support remapping. • **Enabled**—The processor uses VT-d Interrupt Remapping as required.	
Intel(R) VT-d PassThrough DMA Support	Whether the processor supports Intel VT-d Pass-through DMA.	4.1(1)	B200 M5, B480 M5, C220 M5, C240 M5, C480 M5	Enabled, **Disabled** • **Disabled**—The processor does not support passthrough DMA. • **Enabled**—The processor uses VT-d Pass-through DMA as required.	
Intel VTD ATS Support	Whether the processor supports Intel VT-d Address Translation Services (ATS).	4.1(1)	B200 M5, B480 M5, C220 M5, C240 M5, C480 M5	Disabled, **Enabled** • **Disabled**—The processor does not support ATS. • **Enabled**—The processor uses VT-d ATS as required.	

CHAPTER 4

LOM and PCIe Slots

LOM and PCIe Slots

The following table lists the LOM and PCIe BIOS settings that you can configure through a BIOS policy or the default BIOS settings:

Name	Description	Supported Attributes			
		Versions	**Platforms**	**Values**	**Dependencies**
ACS Control GPU *n* where *n* varies from 1-14	Access Control Services (ACS) allow the processor to enable or disable peer-to-peer communication between multiple devices for GPUs. .	4.0(4), 4.1(1)	C480 M5	Enabled, **Disabled** • **Disabled** Disables peer-to-peer communication between multiple devices for GPUs. • **Enabled**Enables peer-to-peer communication between multiple devices for GPUs.	

Name	Description	Supported Attributes			
		Versions	Platforms	Values	Dependencies
CDN Support for LOM	Whether the Ethernet Networking Identifier naming convention is according to Consistent Device Naming (CDN) or the traditional way of naming conventions.	4.0(4), 4.1(1)	C480 M5, B200 M6, X210c M6, X210c M7, X410c M7	Enabled, **Disabled**, LOMs only • **Disabled**OS Ethernet Networking Identifier is named in a default convention as ETH0, ETH1 and so on. • **Enabled**OS Ethernet Network Identifier is named in a consistent device naming (CDN) convention according to the physical LAN on Motherboard (LOM) port numbering; LOM Port 0, LOM Port 1 and so on.	
External SSC Enable	This option allows you to Enable/Disable the Clock Spread Spectrum of the external clock generators.	4.1(2)	B480M5, B200M5, S3X60M5, C220 M7, C240 M7, X210c M6, X210c M7, X410c M7 servers.	Enabled, **Disabled**, 0P3_Percent, 0P5_Percent, Hardware, Off	
IIO eDPC Support	This option allows a downstream link to be disabled after an uncorrectable error, making recovery possible in a controlled and robust manner.	4.2(1), 5.0(1), 5.0(2)	C220 M6 and C240 M6, B200 M6, X210c M6, C220 M7, C240 M7	Disabled, On fatal error, **On fatal and non-fatal error**	

Name	Description	Supported Attributes			
		Versions	Platforms	Values	Dependencies
LOM Port *n* OptionROM, where *n* ranges from 0-3.	Whether Option ROM is available on the LOM port *n*	4.0(4), 4.1(1),	C220 M6 and C240 M6C220 M5, C240 M5, C480 M5	Disabled, **Enabled,** Legacy only, UEFI only • **Disabled**—The expansion slot is not available. • **Enabled**—The expansion slot is available. . • **UEFI only**—The expansion slot is available only for UEFI. • **Legacy only**—The expansion slot is available only for legacy.	
All Onboard LOM Ports	Whether all onboard LOM ports are enabled or disabled.	4.0(2), 4.0(4), 4.1(1),	C220 M5, C240 M5 C480 M5	Disabled, **Enabled** • **Disabled**—LOM Port 0 OptionROM and LOM Port 1 OptionROM are Disabled. • **Enabled**—LOM Port 0 OptionROM and LOM Port 1 OptionROM are enabled. .	If set as Disabled, then LOM Port 0 OptionROM and LOM Port 1 OptionROM are Disabled. If set as Enabled, then LOM Port 0 OptionROM and LOM Port 1 OptionROM are Enabled.

Name	Description	Supported Attributes			
		Versions	Platforms	Values	Dependencies
All PCIe Slots OptionROM	Whether all PCIe OptionROM ports are enabled or disabled.	4.0(2), 4.0(4), 4.1(1),	C220 M5, C240 M5, C480 M5,	Disabled, **Enabled**, Legacy only, UEFI only • **Disabled**—LOM Port 0 OptionROM and LOM Port 1 OptionROM are Disabled. • **Enabled**—LOM Port 0 OptionROM and LOM Port 1 OptionROM are enabled. . • **UEFI only**—The expansion slot is available only for UEFI. • **Legacy only**—The expansion slot is available only for legacy.	
PCI ROM CLP	Whether all PCI ROM CLP ports are enabled or disabled.	4.0(2), 4.0(4), 4.1(1),	C220 M5, C240 M5, C480 M5,	Disabled, Enabled • **Disabled**—The options are Disabled. • **Enabled**—The options are enabled. .	
PCIe ARI Support	Whether all ARI support ports are enabled or disabled.	4.2(1)	C225 M6 and C245 M6	Disabled, Enabled, **Auto** • **Disabled**—This option is Disabled. • **Enabled**—This options is enabled. • **Auto**—PCIe ARI Support is in auto mode. .	
PCIe PLL SSC Percent	Whether all PCIe PLL SSC ports are enabled or disabled.	4.1(2)	C220 M5, C240 M5 servers, C220 M6, C240 M6 servers, X210c M6 servers, C220 M7, C240 M7, X210c M7, X410c M7 servers.	0–**255** (Unit is (n/10)%)	

Name	Description	Supported Attributes			
		Versions	Platforms	Values	Dependencies
MRAID*n* Link Speed where n ranges from 1-2.	This option allows you to restrict the maximum speed of MRAID.	4.0(2), 4.0(4), 4.1(1), 4.2(1)	C220 M5, C240 M5, C225 M6, C245 M6, C240 M7	**Auto**, Disabled, Enabled, Gen 1, Gen 2, Gen 3, Gen 4, Gen 5 • **Disabled**—The maximum speed is not restricted. • **Enabled**—The maximum speed is restricted. • **Auto**—The maximum speed is set automatically. • **Gen 1**—2.5GT/s (gigatransfers per second) is the maximum speed allowed. • **Gen 2**—5GT/s is the maximum speed allowed. • **Gen 3**—8GT/s is the maximum speed allowed. • **Gen 4**—16GT/s is the maximum speed allowed. • **Gen 5**—32GT/s is the maximum speed allowed.	
MRAID *n* OptionROM where n ranges from 1-2.	Whether Option ROM is available on the MRAID port.	4.0(2), 4.0(4), 4.1(1), 4.2(1)	C220 M5, C240 M5, C225 M6, C245 M6, C240 M7	Disabled, **Enabled** • **Disabled**—The expansion slot is not available. • **Enabled**—The expansion slot is available. .	

Name	Description	Supported Attributes			
		Versions	Platforms	Values	Dependencies
PCIe Slot MSTOR Link Speed	This option allows you to restrict the maximum speed of an MSTOR adapter.	4.2(1)	C225 M6 and C245 M6	**Auto**, Disabled, Gen 1, Gen 2, Gen 3, Gen 4 • **Disabled**—The maximum speed is not restricted. • **Auto**—The maximum speed is set automatically. • **Gen 1**—2.5GT/s (gigatransfers per second) is the maximum speed allowed. • **Gen 2**—5GT/s is the maximum speed allowed. • **Gen 3**—8GT/s is the maximum speed allowed. • **Gen 4**—16GT/s is the maximum speed allowed.	
PCIe Slot MSTOR RAID OptionROM	Whether the server can use the Option ROMs present in the PCIe MSTOR RAID.	4.2(1)	C225 M6 and C245 M6, C220 M7, C240 M7	**Disabled**, Enabled, Legacy only, UEFI only • **Disabled**—Option ROM is not available. • **Enabled**—Option ROM is available.	

Name	Description	Supported Attributes			
		Versions	Platforms	Values	Dependencies
NVME *n* Link Speed where *n* ranges from 0-6 and 13-24.	This option allows you to restrict the maximum speed of an NVME card installed in the PCIe slot.	4.0(2), 4.0(4), 4.1(1), 4.2(1), 4.3(2)	C220 M5, C240 M5, C225 M6, C245 M6 **Note** NVME *24* Link Speed supports C220 M7 and C240 M7 servers, and X210c M7 server.	Disabled, **Auto**, GEN1, GEN2, GEN3, GEN4, GEN5 • **Disabled**—Maximum speed is not restricted. • **Auto**—The maximum speed is set automatically. • **Gen 1**—2.5GT/s (gigatransfers per second) is the maximum speed allowed. • **Gen 2**—5GT/s is the maximum speed allowed • **Gen 3**—8GT/s is the maximum speed allowed • **Gen 4**—16GT/s is the maximum speed allowed • **Gen 5**—32GT/s is the maximum speed allowed	
NVME *n* OptionROM where *n* ranges from 0-6.	This options allows you to control the Option ROM execution of the PCIe adapter connected to the SSD:NVMe slot n.	4.0(2), 4.0(4), 4.1(1), 4.2(1)	C220 M5, C240 M5, C225 M6, C245 M6	Enabled, Disabled • **Disabled**—Option is not restricted. • **Enabled**—Option is restricted.	

Name	Description	Supported Attributes			
		Versions	Platforms	Values	Dependencies
PCIe Slot *n* Link Speed where *n* ranges from 1 to 12 .	Link speed for PCIe Slot designated by slot n.	4.0(1), 4.0(2), 4.0(4), 4.1(1), 4.2(1)	C220 M5, C240 M5, C480 M5, C125 M5, C225 M6, C245 M6, C220 M7, C240 M7(Slots 4–8)	Disabled, **Auto**, GEN1, GEN2, GEN3, GEN4, GEN5 GEN5 is supported only for speeds 1 to 6. • **Disabled**—Maximum speed is not restricted. • **Auto**—The maximum speed is set automatically. • **Gen 1**—2GT/s (gigatransfers per second) is the maximum speed allowed. • **Gen 2**—5GT/s is the maximum speed allowed • **Gen 3**—8GT/s is the maximum speed allowed • **Gen 4**—16GT/s is the maximum speed allowed • **Gen 5**—32 GT/s is the maximum speed allowed	

Name	Description	Supported Attributes			
		Versions	Platforms	Values	Dependencies
Slot *n* State where *n* ranges from 1 to 14.	The state of the adapter card installed in PCIe slot n.	4.0(2), 4.0(4), 4.1(1), 4.2(1)	C480 M5 ML, C220 M6, C240 M6, B200 M6	Disabled, **Enabled**, Legacy only, UEFI only • **Disabled**—The expansion slot is not available. • **Enabled**—The expansion slot is available. • **UEFI only**—The expansion slot is available only for UEFI. • **Legacy only**—The expansion slot is available only for legacy.	C220 M6, C240 M6, B200 M6 supports Slot 9 State only.
PCIe Slot:FLOM Link Speed	To configure link speed for PCIe Slot:FLOM.	4.0 (1), 4.0(2), 4.0(4), 4.1(1), 4.2(1)	C220 M5, C240 M5, C225 M6, C245 M6	Disabled, **Auto**, GEN1, GEN2, GEN3 • **Disabled**—Maximum speed is not restricted. • **Auto**—The maximum speed is set automatically. • **Gen 1**—2GT/s (gigatransfers per second) is the maximum speed allowed. • **Gen 2**—5GT/s is the maximum speed allowed • **Gen 3**—8GT/s is the maximum speed allowed	

Name	Description	Supported Attributes			
		Versions	Platforms	Values	Dependencies
Front NVME *n* Link Speed where *n* ranges from 1 to 12.	This option allows you to restrict the maximum speed of an NVME card installed in the front PCIe slot.	4.0(4), 4.1(1), 4.2(1)	C220 M5, C240 M5, C225 M6, C245 M6, C220 M7, C240 M7 (Slots 11–24)	Disabled, **Auto**, GEN1, GEN2, GEN3, GEN4, GEN5 • **Disabled**—Maximum speed is not restricted. • **Auto**—The maximum speed is set automatically. • **Gen 1**—2.5GT/s (gigatransfers per second) is the maximum speed allowed. • **Gen 2**—5GT/s is the maximum speed allowed • **Gen 3**—8GT/s is the maximum speed allowed • **Gen 4**—16GT/s is the maximum speed allowed • **Gen 5**—32GT/s is the maximum speed allowed	
Front NVME *n* OptionROM where *n* ranges from 1 to 24.	This options allows you to control the Option ROM execution of the PCIe adapter connected to the SSD:NVMe slot n.	4.2(1)	C225 M6, C245 M6, C220 M7, C240 M7(Slots 11–24)	**Enabled**, Disabled • **Disabled**—Option is not restricted. • **Enabled**—Option is restricted.	

Name	Description	Supported Attributes			
		Versions	Platforms	Values	Dependencies
Front 1 and 2 Link Speed	This options allows you to control the link speed execution of the front PCIe adapter connected to the slot 1 and 2.	4.0(4), 4.1(1), 4.2(1)	C220 M5, C240 M5, C225 M6, C245 M6	Disabled, **Auto**, GEN1, GEN2, GEN3, GEN4 • **Disabled**—Maximum speed is not restricted. • **Auto**—The maximum speed is set automatically. • **Gen 1**—2.5GT/s (gigatransfers per second) is the maximum speed allowed. • **Gen 2**—5GT/s is the maximum speed allowed • **Gen 3**—8GT/s is the maximum speed allowed • **Gen 4**—16GT/s is the maximum speed allowed	

Name	Description	Supported Attributes			
		Versions	Platforms	Values	Dependencies
PCIe Slot:HBA Link Speed	This option allows you to restrict the maximum speed of an HBA card.	4.2(1)	C225 M6, C245 M6	Disabled, **Auto**, GEN1, GEN2, GEN3, GEN4 • **Disabled**—Maximum speed is not restricted. • **Auto**—The maximum speed is set automatically. • **Gen 1**—2.5GT/s (gigatransfers per second) is the maximum speed allowed. • **Gen 2**—5GT/s is the maximum speed allowed • **Gen 3**—8GT/s is the maximum speed allowed • **Gen 4**—16GT/s is the maximum speed allowed	
PCIe Slot:HBA OptionROM	This option allows you to configure the option ROM execution of an HBA card.	4.2(1)	C225 M6, C245 M6	Disabled, **Enabled**, Legacy only, UEFI only • **Disabled**—The expansion slot is not available. • **Enabled**—The expansion slot is available. • **UEFI only**—The expansion slot is available only for UEFI. • **Legacy only**—The expansion slot is available only for legacy.	

Name	Description	Supported Attributes			
		Versions	Platforms	Values	Dependencies
GPU *n* OptionROM where *n* ranges from 1 to 8.	Whether the Option ROM is enabled on GPU slot n.	4.0(4), 4.1(1)	C480 M5 ML	**Enabled**, Disabled • **Disabled**—Option is not restricted. • **Enabled**—Option is restricted.	
PCIe LOM:1 and 2 Link	This option allows you to restrict the maximum speed of an adapter card installed in PCIe slot 1 and 2.	4.0 (1), 4.0(2), 4.0(4), 4.1(1)	All M5 servers	Enabled, Disabled • **Disabled**—Option is not restricted. • **Enabled**—Option is restricted.	
Slot Mezz State	This option allows you to configure the Mezz state for PCIe slot.	4.0 (1), 4.0(2), 4.1(1)	All M5 servers	Disabled, **Enabled**, Legacy only, UEFI only • **Disabled**—The expansion slot is not available. • **Enabled**—The expansion slot is available. • **UEFI only**—The expansion slot is available only for UEFI. • **Legacy only**—The expansion slot is available only for legacy.	

Name	Description	Supported Attributes			
		Versions	Platforms	Values	Dependencies
PCIe Slot:MLOM Link Speed	This option allows you to restrict the maximum speed of an MLOM adapter.	4.0 (1), 4.0(2), 4.0(4), 4.1(1)	C220 M5, C240 M5, C480 M5, C125 M5, C220 M6, C240 M6, C220 M7, C240 M7	**Auto**, Disabled, Gen 1, Gen 2, Gen 3, Gen 4, Gen 5 • **Disabled**—The maximum speed is not restricted. • **Auto**—The maximum speed is set automatically. • **Gen 1**—2.5GT/s (gigatransfers per second) is the maximum speed allowed. • **Gen 2**—5GT/s is the maximum speed allowed. • **Gen 3**—8GT/s is the maximum speed allowed. • **Gen 4**—16GT/s is the maximum speed allowed. • **Gen 5**—32GT/s is the maximum speed allowed.	

Name	Description	Supported Attributes			
		Versions	Platforms	Values	Dependencies
PCIe Slot:MLOM OptionROM	Whether Option ROM is available on the MLOM port.	4.0 (1), 4.0(2), 4.0(4), 4.1(1), 5.0(1), 5.0(2)	C220 M5, C240 M5, C480 M5, C125 M5, B200 M6, C220 M6, C240 M6, C220 M7, C240 M7	Disabled, **Enabled**, Legacy only, UEFI only • **Disabled**—The expansion slot is not available. • **Enabled**—The expansion slot is available. • **UEFI only**—The expansion slot is available only for UEFI. • **Legacy only**—The expansion slot is available only for legacy.	

Name	Description	Supported Attributes			
		Versions	Platforms	Values	Dependencies
MRAID Link Speed	This option allows you to restrict the maximum speed of MRAID.	4.0(2), 4.0(4), 4.1(1), 4.2(1)	C220 M5, C240 M5, C220 M6, C240 M6, C225 M6, C220 M7	**Auto**, Disabled, Gen 1, Gen 2, Gen 3, Gen 4, Gen 5 • **Disabled**—The maximum speed is not restricted. • **Auto**—The maximum speed is set automatically. • **Gen 1**—2.5GT/s (gigatransfers per second) is the maximum speed allowed. • **Gen 2**—5GT/s is the maximum speed allowed. • **Gen 3**—8GT/s is the maximum speed allowed. • **Gen 4**—16GT/s is the maximum speed allowed. • **Gen 5**—32GT/s is the maximum speed allowed.	
PCIe Slot:MRAID OptionROM	Whether Option ROM is available on the MLOM port.	4.0(2), 4.0(4), 4.1(1)	C220 M5, C240 M5, C480 M5, C125 M5, C220 M6, C225 M6, C220 M7	Disabled, Enabled, Legacy only, UEFI only • **Disabled**—The expansion slot is not available. • **Enabled**—The expansion slot is available.	

Name	Description	Supported Attributes			
		Versions	Platforms	Values	Dependencies
PCIe Slot N*n*OptionROM, where n ranges from 1 to 24.	Whether Option ROM is available on the port.	4.0(2), 4.0(4), 4.1(1)	C220 M5, C240 M5, C480 M5, C125 M5, C220 M6, C240 M6, C220 M7, C240 M7 (Slots 4–8)	Disabled, **Enabled**, Legacy only, UEFI only • **Disabled**—The expansion slot is not available. • **Enabled**—The expansion slot is available.	
RAID Link Speed	This option allows you to restrict the maximum speed of RAID.	4.0 (1), 4.0(4), 4.1(1),	C480 M5	Disabled, **Auto**, GEN1, GEN2, GEN3 • **Disabled**—Maximum speed is not restricted. • **Auto**—The maximum speed is set automatically. • **Gen 1**—2GT/s (gigatransfers per second) is the maximum speed allowed. • **Gen 2**—5GT/s is the maximum speed allowed • **Gen 3**—8GT/s is the maximum speed allowed	
PCIe Slot RAID OptionROM	Whether Option ROM is available on the RAID slot or not.	4.0 (1), 4.0(4), 4.1(1),	C480 M5	**Enabled**, Disabled • **Disabled**—Option is not restricted. • **Enabled**—Option is restricted.	

Name	Description	Supported Attributes			
		Versions	Platforms	Values	Dependencies
Rear NVME *n* Link Speed, where n ranges from 1 to 4.	This option allows you to restrict the maximum speed of rear NVME.	4.0(4), 4.0 (1), 4.2(1)	C240 M5, C240 M6, C245 M6, C220 M7, C240 M7 **Note** NVME *4* Link Speed supports C240 M7 servers, and X210c M7 server.	**Auto**, Disabled, Gen 1, Gen 2, Gen 3, Gen 4, Gen 5 • **Disabled**—The maximum speed is not restricted. • **Auto**—The maximum speed is set automatically. • **Gen 1**—2.5GT/s (gigatransfers per second) is the maximum speed allowed. • **Gen 2**—5GT/s is the maximum speed allowed. • **Gen 3**—8GT/s is the maximum speed allowed. • **Gen 4**—16GT/s is the maximum speed allowed. • **Gen 5**—32GT/s is the maximum speed allowed.	
Rear NVME *n* OptionROM, where n ranges from 1 to 8.	Whether Option ROM is available on the rear NVME or not.	4.0(4), 4.0 (1), 4.2(1)	C240 M5, C240 M6, C245 M6, C220 M7, C240 M7	**Enabled**, Disabled • **Disabled**—Option is not restricted. • **Enabled**—Option is restricted.	

Name	Description	Supported Attributes			
		Versions	Platforms	Values	Dependencies
PCIe Slot:Riser Link Speed*n*, where n is 1 and 2.	This option allows you to restrict the maximum speed of Riser.	4.0(4), 4.0 (1), 4.2(1)	C220 M5, C240 M5, C480 M5, C125 M5,	Disabled, **Auto**, GEN1, GEN2, GEN3 • **Disabled**—Maximum speed is not restricted. • **Auto**—The maximum speed is set automatically. • **Gen 1**—2GT/s (gigatransfers per second) is the maximum speed allowed. • **Gen 2**—5GT/s is the maximum speed allowed • **Gen 3**—8GT/s is the maximum speed allowed	
PCIe Slot:Riser *n*Slot*x* Link Speed, where *n* is 1 and 2 and *x* is from 1 to 6.	This option allows you to restrict the maximum speed of Riser in the *x* slot .	4.0(2), 4.0(4), 4.1(1)	C220 M5, C240 M5, C480 M5, C125 M5,	Disabled, **Auto**, GEN1, GEN2, GEN3 • **Disabled**—Maximum speed is not restricted. • **Auto**—The maximum speed is set automatically. • **Gen 1**—2GT/s (gigatransfers per second) is the maximum speed allowed. • **Gen 2**—5GT/s is the maximum speed allowed • **Gen 3**—8GT/s is the maximum speed allowed	

Name	Description	Supported Attributes			
		Versions	Platforms	Values	Dependencies
PCIe Slot:SAS OptionROM	Whether Option ROM is available on SAS slot or not.	4.0(2), 4.0(4), 4.1(1)	C220 M5, C240 M5, C480 M5, C125 M5	Disabled, **Enabled**, Legacy only, UEFI only • **Disabled**—The expansion slot is not available. • **Enabled**—The expansion slot is available. • **UEFI only**—The expansion slot is available only for UEFI. • **Legacy only**—The expansion slot is available only for legacy.	
PCIe Slot:FrontSSD *n*Link Speed, where *n* is 1 and 2.	This option allows you to restrict the maximum speed of Front SSD.	4.0(2), 4.0(4), 4.1(1)	C220 M5, C240 M5, C480 M5, C125 M5	Disabled, **Auto**, GEN1, GEN2, GEN3 • **Disabled**—Maximum speed is not restricted. • **Auto**—The maximum speed is set automatically. • **Gen 1**—2GT/s (gigatransfers per second) is the maximum speed allowed. • **Gen 2**—5GT/s is the maximum speed allowed • **Gen 3**—8GT/s is the maximum speed allowed	

CHAPTER 5

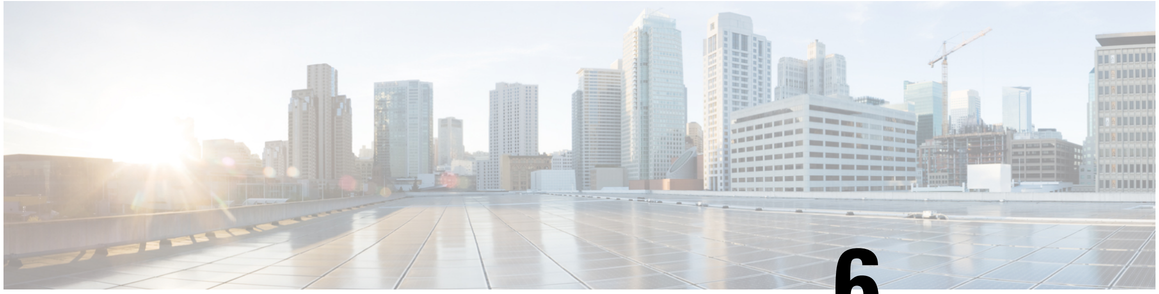
Main

Main

The following table lists the main BIOS settings that you can configure through a BIOS policy or the default BIOS settings:

Name	Description	Supported Attributes			
		Versions	Platforms	Values	Dependencies
PCIe Slots Consistent Device Naming (CDN)	PCIe Slots Consistent Device Naming (CDN) control allows PCIe slots to be named in a consistent manner. This makes PCIe slot names more uniform, easy to identify, and persistent when the configuration changes are made.	4.0(2), 4.0(4), 4.1(1), 4.2(1)	B200 M5, B480 M5, C220 M5, C240 M5, C480 M5, C125 M5, C225 M6, C245 M6, C220 M7, C240 M7	Enabled, **Disabled** • **Disabled**—Option is not restricted. • **Enabled**—Option is restricted.	Consistent Device Naming is same as CDN Control in the UCSM Manager.
Consistent Device Naming (CDN)	PCIe Slots Consistent Device Naming (CDN) control allows PCIe slots to be named in a consistent manner. This makes PCIe slot names more uniform, easy to identify, and persistent when the configuration changes are made.	4.0(2), 4.0(4), 4.1(1), 4.2(1)	B200 M5, B480 M5, C220 M5, C240 M5, C480 M5, C125 M5, C225 M6, C245 M6, C220 M7, C240 M7, X210c M7, X410c M7	Enabled, **Disabled** • **Disabled**—Option is not restricted. • **Enabled**—Option is restricted.	Consistent Device Naming is same as CDN Control in the UCSM Manager.

Name	Description	Supported Attributes			
		Versions	Platforms	Values	Dependencies
POST Error Pause	This is to know what happens when the server encounters a critical error during POST.	4.0 (1), 4.0(2), 4.0(4), 4.1(1)	All M5 servers.	Enabled, **Disabled** • **Disabled**—Option is not restricted. • **Enabled**—Option is restricted.	
TPM Support	Whether to enable or disable the Trusted Platform Module (TPM), which is a component that securely stores artifacts that are used to authenticate the server.	4.2(1)	All M5, M6, and X210c M6 servers.	**Enabled**, Disabled • **Disabled**—Option is not restricted. • **Enabled**—Option is restricted.	



CHAPTER 6

Memory

Memory

The following table lists the memory BIOS settings that you can configure through a BIOS policy or the default BIOS settings:

Name	Description	Supported Attributes			
		Versions	Platforms	Values	Dependencies
Enhanced Memory Test	Enables enhanced memory tests during the system boot and increases the boot time based on the memory.	4.0 (1), 4.0(2), 4.0(4), 4.1(1), 4.2(1), 5.0(1), 5.0(2)	C220 M5, C240 M5, B200 M6, C220 M6,C240 M6, C225 M6, C245 M6, X210c M6, C220 M7, C240 M7, X210c M7, X410c M7	Disabled, Enabled, **Auto** • **Disabled**—Options are Disabled. • **Enabled**—Options are enabled. • **Auto**—Option is in auto mode.	It is recommended to leave this setting in the default state of Auto.

Name	Description	Supported Attributes			
		Versions	Platforms	Values	Dependencies
BME DMA Mitigation	Allows you to disable the PCI BME bit to mitigate the threat from an unauthorized external DMA	4.0 (1), 4.0(2), 4.0(4), 4.1(1), 4.2(1)	C220 M5, C240 M5, B200 M6, C240 M6, C225 M6, C245 M6, X210c M6, C220 M7, C240 M7, X210c M7, X410c M7	Enabled, **Disabled** • Disabled—Option is not restricted. • Enabled—Option is restricted.	
Burst and Postponed Refresh	Allows the memory controller to defer the refresh cycles when the memory is active and accomplishes the refresh within a specified window. The deferred refresh cycles may run in a burst of several refresh cycles.	4.0 (1), 4.0(2), 4.0(4), 4.1(1), 4.2(1)	C225 M6 and C245 M6	Enabled, **Disabled** • Disabled—Option is not restricted. • Enabled—Option is restricted.	

Name	Description	Supported Attributes			
		Versions	Platforms	Values	Dependencies
CPU SMEE	Whether the processor uses the Secure Memory Encryption Enable (SMEE) function, which provides memory encryption support.	4.0(2), 4.0(4), 4.1(1), 4.2(1)	C125 M6, C225 M6, C245 M6	Disabled, **Enabled**, Auto • Disabled—Options are Disabled. • Enabled—Options are enabled. • **Auto**—Option is in auto mode.	
IOMMU	Input Output Memory Management Unit(IOMMU) allows AMD processors to map virtual addresses to physical addresses.	4.0(2), 4.0(4), 4.1(1), 4.2(1)	C125 M6, C225 M6, C245 M6	Disabled, Enabled, **Auto** • Disabled—Options are Disabled. • Enabled—Options are enabled. • Auto—Option is in auto mode.	
Bank Group Swap	Determines how physical addresses are assigned to applications.	4.0 (1), 4.0(4), 4.1(1)4.2(10	C125 M5, C225 M6, C245 M6	Disabled, Enabled, **Auto** • Disabled—Options are Disabled. • Enabled—Options are enabled. • Auto—Option is in auto mode.	
Chipset Interleave	Whether memory blocks across the DRAM chip selects for node 0 are interleaved.	4.2(1)	C225 M6, C245 M6	Disabled, Enabled, **Auto** • Disabled—Options are Disabled. • Enabled—Options are enabled. • Auto—Option is in auto mode.	

Name	Description	Supported Attributes			
		Versions	Platforms	Values	Dependencies
SNP Memory Coverage	This option selects the operating mode of the Secured Nested Paging (SNP) Memory and the reverse Map Table (RMP). The RMP is used to ensure a one-to-one mapping between system physical addresses and guest physical addresses.	4.2(1)	C225 M6, C245 M6	Disabled, Enabled, **Auto** • Disabled—Options are Disabled. • Enabled—Options are enabled. • Auto—Option is in auto mode.	
SNP Memory Size to Cover in MiB	Allows you to configure SNP memory size.	4.2(1)	C225 M6, C245 M6	Disabled, Enabled, **Auto** • Disabled—Options are Disabled. • Enabled—Options are enabled. • Auto—Option is in auto mode.	
NUMA Nodes per Socket	Enables or disables MMIO above 4GB or not.	4.2(1)	C225 M6, C245 M6	**Auto**, NPS0, NPS1, NPS2, NPS4 • NPS0—Zero NUMA node per socket. • NPS1—One NUMA node per socket. • NPS2—Two NUMA node per socket. • NPS4—Four NUMA node per socket. • Auto—Number of channels are set to auto.	

Name	Description	Supported Attributes			
		Versions	Platforms	Values	Dependencies
AMD Memory Interleaving	Determines the memory blocks to be interleaved. It also determines the starting address of the interleave (bit 8,9,10 or 11).	4.0(2), 4.0(4), 4.1(1)	C125 M5	**Auto**, Channel, Die, none, Socket	
AMD Memory Interleaving Size	Determines the size of the memory blocks to be interleaved. It also determines the starting address of the interleave (bit 8,9,10 or 11).	4.0(2), 4.0(4), 4.1(1)	C125 M5	1 KB, 2 KB, 256 Bytes, 512 Bytes, **Auto**	
SEV-SNP Support	Allows you to enable Secure Nested Paging feature.	4.2(1)	C225 M6, C245 M6	**Disabled**, Enabled • Disabled—Options are Disabled. • Enabled—Options are enabled.	

Name	Description	Supported Attributes			
		Versions	Platforms	Values	Dependencies
CR QoS	Prevents DRAM and overall system BW drop in the presence of concurrent DCPMM BW saturating threads, with minimal impact to homogenous DDRT-only usages, Good for multi-tenant use cases, VMs, etc. Targeted for App Direct, but also improves memory mode. Targets the "worst-case" degradations.	4.1(2), 4.2(1), 5.0(1), 5.0(2)	C220 M5, C240 M5, C220 M6, C240 M6 servers, B200 M6, and X210c M6, C220 M7, C240 M7, X210c M7, X410c M7	**Disabled**, Recipe 1, Recipe 2, Recipe 3, Mode 0, Mode 1, Mode 2 • Disabled—Feature disabled. • Recipe 1—6 modules, 4 modules per socket optimized • Recipe 2—2 modules per socket optimized • Recipe 3—1 module per socket optimized • Mode 0 - Disable the PMem QoS Feature • Mode 1 - M2M QoS Enable;CHA QoS Disable • Mode 2 - M2M QoS Enable;CHA QoS Enable	

Name	Description	Supported Attributes			
		Versions	Platforms	Values	Dependencies
CR FastGo Config	CR FastGo Config improves DDRT non-temporal write bandwidth when FastGO is disabled. When FastGO is enabled, it gives faster flow of NT writes into the uncore, When FastGO is disabled, it lessens NT writes queueing up in the CPU uncore, thereby improving sequentially at DCPMM, resulting in improved bandwidth.	4.1(2), 4.2(1), 5.0(1), 5.0(2)	C220 M5, C240 M5, C220 M6, C240 M6, X210c M6, C220 M7, C240 M7, X210c M7, X410c M7	**Auto**, Option 1—5, Enable Optimization, Disable Optimization	

Name	Description	Supported Attributes			
		Versions	Platforms	Values	Dependencies
DCPMM Firmware Downgrade	To configure DCPMM Firmware Downgrade.	4.0 (1), 4.0(2), 4.0(4), 4.1(1), 4.2(1)	B480 M5, C220 M5, C240 M5, C480 M5, C220 M6, C240 M6, C220 M7, C240 M7, X210c M7, X410c M7 servers	**Disabled**, Enabled • Disabled—Options are Disabled. • Enabled—Options are enabled.	
DRAM Refresh Rate	To configure the refresh interval rate for internal memory.	4.0 (1), 4.0(2), 4.0(4), 4.1(1), 4.2(1)	C125 M5	Auto, 1x, **2x**, 3x, 4x	
DRAM SW Thermal Throttling	To configure DRAM SW thermal throttling.	4.0 (1), 4.0(2), 4.0(4), 4.1(1)	C125 M5	Disabled, Enabled • Disabled—Options are Disabled. • Enabled—Options are enabled.	

Name	Description	Supported Attributes			
		Versions	Platforms	Values	Dependencies
eADR Support	Extended asynchronous DRAM refresh (eADR) ensures that CPU caches lines with data are flushed at the right time and in the desired order and are also included in the power fail protected domain.	4.2(1), 5.0(1), 5.0(2)	B200 M6, X210c M6, C220 M7, C240 M7, X210c M7, X410c M7	**Disabled**, Enabled, Auto • Disabled—Options are Disabled. • Enabled—Options are enabled. • Auto—Option is in auto mode.	
Low Voltage DDR Mode	Whether the system prioritizes low voltage or high frequency memory operations.	4.0 (1), 4.0(2), 4.0(4), 4.1(1)	All M5 servers	**Auto**, Power Saving Mode, Performance Mode • Auto—The CPU determines whether to prioritize low voltage or high frequency memory operations. • Power Saving Mode—The system prioritizes low voltage memory operations over high frequency memory operations. This mode may lower memory frequency in order to keep the voltage low • Performance Mode—The system prioritizes high frequency operations over low voltage operations • Auto—Option is in auto mode.	

Name	Description	Supported Attributes			
		Versions	Platforms	Values	Dependencies
Memory Bandwidth Boost	Allows to boost the memory bandwidth.	4.2(1), 5.0(1), 5.0(2)	C220 M6, C240 M6, B200 M6, X210c M6, C220 M7, C240 M7, X210c M7, X410c M7	Disabled, Enabled • Disabled—Options are Disabled. • Enabled—Options are enabled.	
Memory Refresh Rate	Controls the refresh rate of the memory controller and might affect the memory performance and power depending on memory configuration and workload.	4.0(2), 4.0(4), 4.1(1), 4.2(1), 5.0(1), 5.0(2)	C220 M5, C240 M5, B200 M6, C220 M6, C240 M6, X210c M6, C220 M7, C240 M7, X210c M7, X410c M7	1x Refresh, **2x Refresh** **Note** Default value for M7 servers is 1x Refresh	

Name	Description	Supported Attributes			
		Versions	Platforms	Values	Dependencies
Memory Size Limit in GiB	Limits the capacity in Partial Memory Mirror Mode up to 50 percent of the total memory capacity. The memory size can range from 0 GB to 65535 GB in increments of 1 GB.	4.0(2), 4.0(4), 4.1(1), 4.2(1)	C220 M5, C240 M5, B200 M6, C240 M6, C225 M6, C245 M6, X210c M6, C220 M7, C240 M7, X210c M7, X410c M7	**0** - 65535 with a step size of 1	

Name	Description	Supported Attributes			
		Versions	Platforms	Values	Dependencies
Memory Thermal Throttling Mode	Provides a protective mechanism to ensure the memory temperature is within the limits. When the temperature exceeds the maximum threshold value, the memory accessrate isreduced and Baseboard Management Controller (BMC) adjusts the fan to cool down the memory to avoid DIMM damage due to overheat	4.0 (1), 4.0(2), 4.0(4), 4.1(1)	All M5 servers and , C220 M7, C240 M7 , X210c M7, X410c M7 servers	**CLTT with PECI**, Disabled • Disabled—Options are Disabled. • CLTT with PECI—Closed Loop Thermal Throttling (CLTT) with Platform Environment Control Interface (PECI).	This token is not supported on C125 M5 servers.
Mirroring Mode	Memory mirroring enhances system reliability by keeping two identical data images in memory.	4.0 (1), 4.0(2), 4.0(4), 4.1(1)	All M5 servers	**Inter-socket**, Intra-socket • Inter-Socket—Memory is mirrored between two Integrated Memory Controllers (IMCs) across CPU sockets. • Intra-Socket—One IMC is mirrored with another IMC in the same socket.	

Name	Description	Supported Attributes			
		Versions	Platforms	Values	Dependencies
NUMA Optimized	Whether the BIOS supports NUMA.	4.0 (1), 4.0(2), 4.0(4), 4.1(1)	C220 M5, C240 M5, B200 M6, C220 M6, C240 M6, X210c M6, C220 M7, C240 M7, X210c M7, X410c M7	**Enabled**, Disabled • Disabled—The BIOS does not support NUMA. • Enabled—The BIOS includes the ACPI tables that are required for NUMA-aware operating systems. If you enable this option, the system must disable Inter-Socket Memory interleaving on some platforms.	
NVM Performance Setting	enables efficient major mode arbitration between DDR and DDRT transactions on the DDR channel to optimize channel BW and DRAM latency.	4.0(2), 4.0(4), 4.1(1)	C220 M5, C240 M5, B200 M6, C220 M6, C240 M6, X210c M6, C220 M7, C240 M7, X210c M7, X410c M7	**BW Optimized**, Latency Optimized, Balanced Profile • BW Optimized—Optimized for DDR and DDRT BW. This is the default option. • Latency Optimized—Better DDR latency in the presence of DDRT BW. • Balanced Profile—Optimized for Memory mode.	
Operation Mode	This option allows you to configure Operation Mode.	4.2(1), 4.2(2)	C225 M5, C245 M5	**Test-Only**, Test and Repair	

Name	Description	Supported Attributes			
		Versions	Platforms	Values	Dependencies
Panic and High Watermark	Controls the delayed refresh capability of the memory controller.	4.2(1)	B200 M6, C220 M6, C240 M6, C220 M7, C240 M7, X210c M7, X410c M7	High, **Low** • High—The memory controller is allowed to postpone up to a maximum of eight refresh commands. The memory controller executes all the postponed refreshes within the refresh interval.For the ninth refresh command, the refresh priority becomes Panic and the memory controller pauses the normal memory transactions until all the postponed refresh commands are executed. • Low—The memory controller is not allowed to postpone refresh commands. **Note** It is recommended to leave this setting in the default state (Low) which will help to reduce susceptibility to Rowhammer-style attacks.	It is recommended to leave this setting in the default state (**Low**) which will help to reduce susceptibility to Rowhammer-style attacks.

Name	Description	Supported Attributes			
		Versions	Platforms	Values	Dependencies
Partial Cache Line Sparing	Partial cache line sparing (PCLS) is an error-prevention mechanism in memory controllers. PCLS statically encodes the locations of the faulty nibbles of bits into a sparing directory along with the corresponding data content for replacement during memory accesses.	4.2(1), 5.0(1), 5.0(2)	B200 M6, C240 M6, C220 M6, X210c M6, C220 M7, C240 M7, X210c M7, X410c M7	Disabled, **Enabled** **Note** For M7 servers, **Disabled** is the default value. • Disabled—Options are Disabled. • Enabled—Options are enabled.	

Name	Description	Supported Attributes			
		Versions	Platforms	Values	Dependencies
Partial Memory Mirror Mode	enables you to partially mirror by GB or by a percentage of the memory capacity. Depending on the option selected here, you can define either a partial mirror percentage or a partial mirror capacity in GB in available fields. You can partially mirror up to 50 percent of the memory capacity.	4.1(1),	B200 M5, B480 M5, C220 M5, C240 M5, C480 M5, B200 M6, C220 M6, C240 M6, X210c M6, C220 M7, C240 M7, X210c M7, X410c M7	**Disabled**, Percentage, Value in GB • Disabled—Options are Disabled. • Percentage—The amount of memory to be mirrored in the Partial Memory Mode is defined as a percentage of the total memory. • Value in GB—The amount of memory to be mirrored in the Partial Memory Mode is defined in GB. **Note** Partial Memory Mirror Mode is mutually exclusive to standard Mirroring Mode. Partial Mirrors 1-4 can be used in any number or configuration, provided they do not exceed the capacity limit set in GB or Percentage in the related options.	

Name	Description	Supported Attributes			
		Versions	Platforms	Values	Dependencies
Partial Mirror Percentage	Limits the amount of available memory to be mirrored as a percentage of the total memory. This can range from 0.000.01 % to 50.00 % in increments of 0.01 %.	4.1(1)	B200 M5, B480 M5, C220 M5, C240 M5, C480 M5, B200 M6, C220 M6, C240 M6, X210c M6, C220 M7, C240 M7, X210c M7, X410c M7	**0.00** - 50.00 with a step size of 0.01	**Note** Applicable only when partial mirror mode is set to a value in GB. • In Memory RAS Configuration, select **Partial Mirror Mode 1LM** • Partial Memory Mirror Mode configuration should be set to **Percentage**.

Name	Description	Supported Attributes			
		Versions	Platforms	Values	Dependencies
Partial Mirror*n* Size in GB, where *n* ranges from 1 to 4.	Limits the amount of memory in Partial Mirror*n* in GB. This can range from 0 GB to 65535 GB in increments of 1 GB.	4.1(1)	B200 M5, B480 M5, C220 M5, C240 M5, C480 M5, C125 M5, C220 M7, C240 M7, X210c M7, X410c M7	**0** - 65535 with a step size of 1	**Note** Applicable only when partial mirror mode is set to a value in GB. When *n=2:* • In Memory RAS Configuration, select **Partial Mirror Mode 1LM** • Partial Memory Mirror Mode configuration should be set to **Percentage**.
PCIe RAS Support	Whether the PCIe RAS port is enabled or disabled.	4.0 (1), 4.0(2), 4.0(4), 4.1(1), 4.1(3)	All M5 servers and , C220 M7, C240 M7 , X210c M7, X410c M7 servers	Disabled, **Enabled**, Auto • Disabled—This option is Disabled. • Enabled—This options is enabled. • Auto—PCIe RAS Support is in auto mode.	
Post Package Repair	Post Package Repair (PPR) provides the ability to repair faulty memory cells by replacing them with spare cells.	4.2(1)	B200 M6, C240 M6, C220 M6, C225 M6, C245 M6, X210c M6	Disabled, **Hard PPR** • Disabled—This option is Disabled. • Hard PPR—This results in a permanent remapping of damaged storage cells.	

Name	Description	Supported Attributes			
		Versions	Platforms	Values	Dependencies
Memory RAS Configuration	How the memory reliability, availability, and serviceability (RAS) is configured for the server.	4.0 (1), 4.0(2), 4.0(4), 4.1(1), 4.1(3), 4.2(1), 5.0(1), 5.0(2)	C220 M5, C240 M5, B200 M6, C240 M6, C220 M6, C220 M7, C240 M7, X210c M7, X410c M7		

Name	Description	Supported Attributes			
		Versions	Platforms	Values	Dependencies
				Maximum Performance, Mirroring, Lockstep, Mirror Mode 1LM, Partial Mirror Mode 1LM, Sparing, **ADDDC Sparing** • Maximum Performance—Optimizes the system performance and disables all the advanced RAS features. • Mirroring—System reliability is optimized by using half the system memory as backup. This mode is used for UCS M4 and lower blade servers • Lockstep—If the DIMM pairs in the server have an identical type, size, and organization and are populated across the SMI channels, you can enable lockstep mode to minimize memory access latency and provide better performance. Lockstep is enabled by default for B440 servers. • Mirror Mode 1LM—Mirror Mode 1LM willset the entire 1LM memory in the system to be mirrored, consequently reducing the memory capacity by half. This mode is used for UCS M5 and M6 blade servers. • Partial Mirror Mode 1LM—Partial Mirror Mode 1LM will set a part of the 1LM memory in the system to be mirrored, consequently reducing the memory capacity by half. This mode is used for UCS M5 and M6 blade servers. • Sparing—System reliability	

Name	Description	Supported Attributes			
		Versions	Platforms	Values	Dependencies
				is optimized by holding memory in reserve so that it can be used in case other DIMMs fail. This mode provides some memory redundancy, but does not provide as much redundancy as mirroring. • ADDDC Sparing—System reliability is optimized by holding memory in reserve so that it can be used in case other DIMMs fail. This mode provides some memory redundancy, but does not provide as much redundancy as mirroring.	
PPR Type	Post Package Repair (PPR) provides the ability to repair faulty memory cells by replacing them with spare cells.	4.1(1), 4.2(1)	C220 M5, C240 M5, B200 M5, B200 M6, C240 M6, C220 M6, C225 M6, C245 M6, C220 M7, C240 M7, X210c M7, X410c M7	Disabled, **Hard PPR** • Disabled—Options are Disabled. • Hard PPR—This results in a permanent remapping of damaged storage cells.	

Name	Description	Supported Attributes			
		Versions	Platforms	Values	Dependencies
Secured Encrypted Virtualization	Enables running encrypted virtual machines(VMs) in which the code and data of the VM are isolated.	4.2(1)	C125 M5, C225 M6, C245 M6	253 ASIDs, 509 ASIDs, Auto • 253 ASIDs • 509 ASIDs • Auto **Note** It is recommended to leave this setting in the default state of Auto to mitigate Rowhammer-style attacks.	
SMEE	Whether the processor uses the Secure Memory Encryption Enable (SMEE) function, which provides memory encryption support.	4.0(4), 4.1(1), 4.1(3), 4.2(1)	C125 M5, C225 M6, C245 M6	Disabled, **Enabled** • Disabled—This option is Disabled. • Enabled—This options is enabled.	

Name	Description	Supported Attributes			
		Versions	Platforms	Values	Dependencies
Snoopy Mode for 2LM		4.0 (1), 4.0(2), 4.0(4), 4.1(1), 4.1(3), 4.2(1)	All M5 servers and , C220 M7, C240 M7 , X210c M7, X410c M7 servers	**Disabled**, Enabled • Disabled—This option is Disabled. • Enabled—This options is enabled.	

Name	Description	Supported Attributes			
		Versions	Platforms	Values	Dependencies
	Enables snoop-mode for DCPMM accesses while maintaining directory on all DRAM accesses. Snoops maintain cache coherence between sockets. Directory reducessnoops by keeping the remote node information locally (in memory). Directory lookups and updates add memory traffic Directory is a good tradeoff for DRAM, but not necessarily for DCPMM. For non-NUMA workload, when the feature is enabled, directory updates to DCPMM are eliminated, thereby helping DDRT bandwidth bound workloads. Directory is disabled for far memory				

Name	Description	Supported Attributes			
		Versions	Platforms	Values	Dependencies
	accesses and instead snoops remote sockets to check for ownership. Directory is used only for DRAM (near memory).				

Name	Description	Supported Attributes			
		Versions	Platforms	Values	Dependencies
Snoopy Mode for AD		4.0 (1), 4.0(2), 4.0(4), 4.1(1), 4.1(3), 4.2(1)	All M5 servers and , C220 M7, C240 M7 , X210c M7, X410c M7 servers	**Disabled**, Enabled • Disabled—This option is Disabled. • Enabled—This options is enabled.	

Name	Description	Supported Attributes			
		Versions	Platforms	Values	Dependencies
	Enables snoop-mode for DCPMM accesses while maintaining directory on all DRAM accesses. Snoops maintain cache coherence between sockets. Directory reducessnoops by keeping the remote node information locally (in memory). Directory lookups and updates add memory traffic. Directory is a good tradeoff for DRAM, but not necessarily for DCPMM. For non-NUMA workload, when the feature is enabled, directory updates to DCPMM are eliminated, thereby helping DDRT bandwidth bound workloads. Directory is disabled for				

Name	Description	Supported Attributes			
		Versions	Platforms	Values	Dependencies
	accesses to AD and instead snoops remote sockets to check for ownership. Directory is used only for DRAM accesses.				
Transparent Secure Memory Encryption	Provides transparent hardware memory encryption of all data stored on system memory.	4.1(3)	C125 M5 servers	Disabled, Enabled, **Auto** • Disabled—This option is Disabled. • Auto—This options is set to auto mode.	
UMA Based Clustering	As the name implies, UMA based clustering is the suggested clustering mode when the processor is configured as Uniform Memory Access (UMA) node, i.e. SNC is disabled.	4.2(1)	C220 M6, C240 M6, B200 M6, X210 M6, C220 M7, C240 M7, X210c M7, X410c M7	Disable-All-2All, **Hemisphere-2-clusters**, Quadrant-4-clusters **Note** For M7 servers, the default value is **Quadrant-4-clusters**.	

Name	Description	Supported Attributes			
		Versions	Platforms	Values	Dependencies
Volatile Memory Mode	Allows the memory mode configuration.	4.0(2), 4.0(4), 4.1(1), 4.2(1), 5.0(1), 5.0(2)	C220 M6, C240 M6, B200 M6, X210c M6, C220 M7, C240 M7, X210c M7, X410c M7	1LM, **2LM** • 1LM—Configures 1 Layer Memory(1LM).This is the default value for M7 servers. • 2LM—Configures 2 Layer Memory(1LM).	
Error Check Scrub	Allows you to enable a memory device to perform memory checking, correction and count errors.	4.0(2), 4.0(4), 4.1(1), 4.2(1), 5.0(1), 5.0(2)	C220 M6, C240 M6, B200 M6, X210c M6, C220 M7, C240 M7, X210c M7, X410c M7	Disabled, **Enabled with result collection**, Enabled without result collection	
Rank Margin Tool	Allows automated memory margin testing and is used to identify DDR margins at the rank level.	4.0(2), 4.0(4), 4.1(1), 4.2(1), 5.0(1), 5.0(2)	C220 M6, C240 M6, B200 M6, X210c M6, C220 M7, C240 M7, X210c M6	Enable, **Disable**	

Name	Description	Supported Attributes			
		Versions	Platforms	Values	Dependencies
Adaptive Refresh Management Level	Selects Adaptive Refresh Management (ARFM) Level when refresh management (RFM) is required.	4.0(2), 4.0(4), 4.1(1), 4.2(1), 5.0(1), 5.0(2)	C220 M6, C240 M6, X210c M6 , C220 M7, C240 M7, X210c M7, X410c M7	Enable, **Disable**	

CHAPTER 7

PCI

PCI

The following table lists the PCI BIOS settings that you can configure through a BIOS policy or the default BIOS settings:

Name	Description	Supported Attributes			
		Versions	**Platforms**	**Values**	**Dependencies**
ASPM Support	Allows you to set the level of ASPM (Active Power State Management) support in the BIOS.	4.0 (1), 4.0(2), 4.0(4), 4.1(1)	All M5 servers	Disabled, **Auto**, ForceL0 • **ForceL0**—Force all links to L0 standby (L0s) state.	
Memory Mapped IO above 4GB	Whether to enable or disable memory mapped I/O of 64-bitPCI devices to 4GB or greater address space. Legacy option ROMs are not able to access addresses above 4GB. PCI devices that are 64-bit compliant but use a legacy option ROM may not function correctly with this setting enabled.	4.0 (1), 4.0(2), 4.0(4), 4.1(1), 4.1(3)	All M5 servers and , C220 M7, C240 M7, X210c M7, X410c M7 servers	**Disabled**, Enabled • **Disabled**—This option is Disabled. • **Enable**—This options is enabled.	

Name	Description	Supported Attributes			
		Versions	Platforms	Values	Dependencies
VGA Priority	Allows you to set the priority for VGA graphics devices if multiple VGA devices are found in the system.	4.0(2), 4.0(4), 4.1(1)	C220 M5, C240 M5, C220 M7, C240 M7	Offboard, **Onboard**, Onboard VGA Disabled • **Onboard**—Priority is given to the onboard VGA device. BIOS post screen and OS boot are driven through the onboard VGA port • **Offboard**——Priority is given to thePCIE Graphics adapter. BIOS post screen and OS boot are driven through the external graphics adapter port. • **Onboard VGA Disabled** —Priority is given to the PCIE Graphics adapter, and the onboard VGA device is disabled **Note** The vKVM does not function when the onboard VGA is disabled.	

CHAPTER 8

Power and Performance

Power and Performance

The following table lists the power and performance BIOS settings that you can configure through a BIOS policy or the default BIOS settings:

Name	Description	Supported Attributes			
		Versions	Platforms	Values	Dependencies
Optimized Power Mode	Automatically varies processor speed and power usage based on processor utilization to increase performance per watt. Most effective under moderate utilization.	4.3(2)	C220 M7, C240 M7, X210c M7, X410c M7	**Disabled**, Enabled • Disabled—This option is Disabled. • Enable—This options is enabled.	
C1 Auto Demotion	If enabled, CPU automatically demotes to C1 based on un-core auto-demote information.	4.0(2), 4.0(4), 4.1(1), 4.1(3), 4.2(1), 4.3(3a)	All M5 servers, C220 M6, C240 M6, B200 M6, X210c M6, C220 M7, C240 M7, X210c M7, X410c M7	Disabled, Enabled, **Auto** • Disabled—This option is Disabled. • Enable—This options is enabled.	

Name	Description	Supported Attributes			
		Versions	**Platforms**	**Values**	**Dependencies**
C1 Auto UnDemotion	Select whether to enable processors to automatically undemote from C1.	4.0(2), 4.0(4), 4.1(1), 4.1(3), 4.2(1), 4.3(3a)	All M5 servers, C220 M6, C240 M6, B200 M6, X210c M6, C220 M7, C240 M7, X210c M7, X410c M7	Disabled, Enabled, **Auto** • Disabled—This option is Disabled. • Enable—This options is enabled.	
Core Performance Boost	Whether the AMD processor increases its frequency on some cores when it is idle or not being used much	4.0(2), 4.0(4), 4.1(1), 4.1(3), 4.2(1)	C225 M6, C245 M6	Disabled, **Auto** • Disabled—This option is Disabled. • Auto—The CPU automatically determines how to boost performance.	
Global C State Control	Whether the AMD processors control IO-based C-state generation and DF C-states.	4.0(2), 4.0(4), 4.1(1), 4.1(3), 4.2(1)	C225 M6, C245 M6	**Auto**, Disabled, Enabled • Auto—This options is set to auto mode. • Disabled—This option is Disabled. • Enable—This options is enabled.	
L*n* Stream HW Prefetcher, where n value is 1 and 2.	Whether the processor allows the AMD hardware prefetcher to speculatively fetch streams of data and instruction from memory into the L1 or L2 cache when necessary.	4.0(2), 4.0(4), 4.1(1), 4.1(3), 4.2(1)	C225 M6, C245 M6	**Auto**, Disabled, Enabled • Auto—This options is set to auto mode. • Disabled—This option is Disabled. • Enable—This options is enabled.	

Name	Description	Supported Attributes			
		Versions	Platforms	Values	Dependencies
Determinism Slider	Allows AMD processors to determine how to operate.	4.0(2), 4.0(4), 4.1(1), 4.1(3), 4.2(1)	C225 M6, C245 M6	**Auto**, Performance, Power • Auto—The CPU automatically uses default power determinism settings. • Performance—Processor operates at the best performance in a consistent manner. • Power—Processor operates at the maximum allowable performance on a per die basis.	
Efficiency Mode Enable	Allows you to configure power consumption based on efficiency.	4.0(2), 4.0(4), 4.1(1), 4.1(3), 4.2(1)	C225 M6, C245 M6	**Auto**, Enabled • Enabled—This option is enabled. • Auto—The CPU automatically uses default settings.	
CPPC	Allows you to configure Collaborative Processor Performance Control.	4.0(2), 4.0(4), 4.1(1), 4.1(3), 4.2(1)	C225 M6, C245 M6	**Auto**, Disabled, Enabled • Enabled—This option is enabled. • Disbled—This option is disabled. • Auto—The CPU automatically uses default settings.	
cTDP Control	Allows you to set customized value for Thermal Design Power (TDP).	4.0(2), 4.0(4), 4.1(1), 4.1(3), 4.2(1)	C225 M6, C245 M6	Auto, Manual • Auto—Uses the rated TDP value of the processor. • Manual—Allows you to customize the TDP value.	

Name	Description	Supported Attributes			
		Versions	Platforms	Values	Dependencies
Enhanced CPU Performance	Enhances CPU performance by adjusting server settings automatically.	4.0(2), 4.0(4), 4.1(1), 4.1(3), 4.2(1), 5.0(1), 5.0(2)	C220 M6, C240 M6, B200 M6, X210c M6, C220 M7, C240 M7, X210c M7, X410c M7	Disabled, **Auto** • Disabled—This option is Disabled. • Auto—Allows to adjust server settings to increase the processor performance. **Note** Enabling this functionality may increase power consumption.	The server should meet the following requirements in order to use this functionality: • The server should not contain Barlow Pass DIMMs. • DIMM module size present in the Cisco UCS C220 M6 server should be less than 64GB and in Cisco UCS C240 M6 server should be less than 256GB. • No GPU cards are present in the server.

Name	Description	Supported Attributes			
		Versions	Platforms	Values	Dependencies
LLC Dead Line	In CPU non-inclusive cache scheme, Mid-Level Cache (MLC) evictions are filled into the Last-Level Cache (LLC). When lines are evicted from the MLC, the core can flag them as dead (not likely to be read again). The LLC has the option to drop dead lines and not fill them in the LLC.	4.0(2), 4.0(4), 4.1(1), 4.1(3), 4.2(1)	C220 M6, C240 M6, B200 M6, X210c M6, C220 M7, C240 M7, X210c M7, X410c M7	Disabled, Enabled, **Auto** • **Disabled**—The dead lines are always dropped and are never filled into the LLC. • **Enable**—Allows the LLC to fill dead lines into the LLC if there is free space available. This is the default option. • Auto—The CPU determines the LLC dead line allocation.	
UPI Link Enablement	Enables the number of Ultra Path Interconnect (UPI) links required by the processor.	4.0(2), 4.0(4), 4.1(1), 4.1(3), 4.2(1), 5.0(1), 5.0(2)	All M5 servers, C220 M6, C240 M6, B200 M6, X210c M6, C220 M7, C240 M7, X210c M7, X410c M7	**Auto**, 1, 2, 3	
UPI Power Manangement	The UPI power management can be used for conserving power on the server.	4.0(2), 4.0(4), 4.1(1), 4.1(3), 4.2(1)	All M5 servers, C220 M6, C240 M6, B200 M6, X210c M6, C220 M7, C240 M7, X210c M7, X410c M7	Disabled, **Enabled** • **Disabled**—This option is Disabled. • **Enable**—This options is enabled.	
Virtual NUMA	The Virtual NUMA (virtual non-uniform memory access) is a memory-access optimization method for VMware virtual machines (VMs), which helps prevent memory-bandwidth bottlenecks.	4.0(2), 4.0(4), 4.1(1), 4.1(3), 4.2(1), 5.0(1), 5.0(2)	All M5 servers, C220 M6, C240 M6, B200 M6, X210c M6, C220 M7, C240 M7, X210c M7, X410c M7	**Disabled**, Enabled • **Disabled**—This option is Disabled. • **Enable**—This options is enabled.	

Name	Description	Supported Attributes			
		Versions	Platforms	Values	Dependencies
XPT Remote Prefetch	This feature allows an LLC request to be duplicated and sent to an appropriate memory controller in a remote machine based on the recent LLC history to reduce latency.	4.0(2), 4.0(4), 4.1(1), 4.1(3), 4.2(1), 5.0(1), 5.0(2)	All M5 servers, C220 M6, C240 M6, B200 M6, X210c M6, C220 M7, C240 M7, X210c M7, X410c M7	**Disabled**, Enabled • **Disabled**—This option is Disabled. • **Enable**—This options is enabled. • **Auto**—The CPU determines the functionality.	

CHAPTER 9

Processor

Processor

The following table lists the Processor BIOS settings that you can configure through a BIOS policy or the default BIOS settings:

Name	Description	Supported Attributes			
		Versions	Platforms	Values	Dependencies
PRMRR Size	Processor Reserved Memory Range Registers (PRMRR) is the size of the protected region in the systems DRAM.	4.3(2)	X210c M7, X410c M7, C220M7, C240M7, C220M6, C240M6, C220 M7, C240 M7, X210c M7, X410c M7	Invalid Config, 128M, **256M**, 512M,1G, 2G, 4G, 8G, 16G, 32G, 64G, 128G, 256G, 512G	
Adjacent Cache Line Prefetcher	Whether the processor fetches cache lines in even/odd pairs instead of fetching just the required line.	4.0(2), 4.0(4), 4.1(1), 4.1(3), 4.2(1)	All M5 servers, B200 M6, C220 M6, C240 M6, C220 M7, C240 M7, X210c M7, X410c M7	**Disabled**, Enabled • Disabled—This option is Disabled. • Enable—This options is enabled.	**CPU Performance** must be set to **Custom** in order to specify this value. For any value other than **Custom**, this option is overridden by the setting in the selected CPU performance profile.

Name	Description	Supported Attributes			
		Versions	Platforms	Values	Dependencies
Altitude	The approximate number of meters above sea level at which the physical server is installed.	4.0(2), 4.0(4), 4.1(1), 4.1(3), 4.2(1)	All M5 servers, C220 M6, C240 M6, C225 M6, C245 M6	**Auto**, 300, 900, 1500, 3000 • Auto—The CPU determines the physical elevation. • .*n* M, where *n* is 300, 900, 1500, 3000—The server is approximately *n* meters above sea level.	
Autonomous Core C State	Enables CPU Autonomous C-State, which converts the HALT instructions to the MWAIT instructions.	4.0(2), 4.0(4), 4.1(1), 4.1(3), 4.2(1)	All M5 servers, C220 M6, C240 M6, C225 M6, C245 M6, C220 M7, C240 M7, X210c M7, X410c M7	**Disabled**, Enabled	
CPU Autonomous C State	This enables or disables CPU Autonomous state.	4.0(2), 4.0(4), 4.1(1), 4.1(3), 4.2(1)	All M5 servers, C220 M6, C240 M6, C225 M6, C245 M6	**Disabled**, Enabled	
Boot Performance Mode	Allows the user to select the BIOS performance state that is set before the operating system handoff.	4.0(2), 4.0(4), 4.1(1), 4.1(3), 4.2(1)	All M5 servers, C220 M6, C240 M6, C225 M6, C245 M6, C220 M7, C240 M7, X210c M7, X410c M7	**Disabled**, Enabled	

Name	Description	Supported Attributes			
		Versions	Platforms	Values	Dependencies
Burst and Postponed Refresh	Allows the memory controller to defer the refresh cycles when the memory is active and accomplishes the refresh within a specified window. The deferred refresh cycles may run in a burst of several refresh cycles.	4.0(2), 4.0(4), 4.1(1), 4.1(3), 4.2(1)	C225 M6, C245 M6	**Disabled**, Enabled	It is recommended to leave this setting in the default state of **Disabled** to mitigate Rowhammer-style attacks.
APBDIS	Allows you to select the Algorithm Performance Boost (APB) Disable value for the SMU.	4.0(2), 4.0(4), 4.1(1), 4.1(3), 4.2(1)	C225 M6, C245 M6	**Auto**, 0, 1 • **Auto**—Sets an auto ApbDis for the SMU. This is the default option. • **0**—Clear ApbDis to SMU • **1**—Set ApbDis to SMU	

Name	Description	Supported Attributes			
		Versions	Platforms	Values	Dependencies
Downcore Control	Provides the ability to remove one or more cores from operation is supported in the silicon. It may be desirable to reduce the number of cores due to OS restrictions, or power reduction requirements of the system. This item allows the control on the number of cores that are running. This setting can only reduce the number of cores from only those available in the processor.	4.0(2), 4.0(4), 4.1(1), 4.1(3), 4.2(1)	All M5 servers, C220 M6, C240 M6, C225 M6, C245 M6	**Auto**, Two (2+0), Two (1+1), Three (3+0), Six (3+3), Four (2+2), Four (2+0) • **Auto**—The CPU determines how many cores need to be enabled. This is the default option. • **Two (2+0)(1+1)**—Two cores enabled on one CPU complex. • **Three (3+0)**—Three cores enabled on one CPU complex. • **Four (4+0)(2+2)**—Four cores enabled on one CPU complex. • **Six (3+3)**—Six cores enabled on one CPU complex.	This token is applicable only for the servers with 7xx2 and 7xx3 Model processors.

Name	Description	Supported Attributes			
		Versions	Platforms	Values	Dependencies
Streaming Stores Control	Enables the streaming stores functionality.	4.0(2), 4.0(4), 4.1(1), 4.1(3), 4.2(1)	All M5 servers, C220 M6, C240 M6, C225 M6, C245 M6	**Auto**, Disabled, Enabled	
Fixed SOC P-State	This option defines the target P-state when APBDIS (to disable Algorithm Performance Boost (APB)) is set. The **P-x** specify a valid P-state for the processor installed.	4.0(2), 4.0(4), 4.1(1), 4.1(3), 4.2(1)	All M5 servers, C220 M6, C240 M6, C225 M6, C245 M6	**Auto**, P0, P1, P2, P3 • **Auto**—Sets a valid P-state suitable for the processor. This is the default option. • **P0 to P3**—Highest-performing SOC P-state to lowest-performing SOC P-state.	
DF C-States	When long duration idleness is expected in a system, this control allows the system to transition into a DF Cstate which can set the system into an even lower power state.	4.0(2), 4.0(4), 4.1(1), 4.1(3), 4.2(1)	All M5 servers, C220 M6, C240 M6, C225 M6, C245 M6	**Auto**, Disabled, Enabled	
CCD Control	Allows you to specify the number of charge-coupled device CCDs that are desired to be enable in the system.	4.0(2), 4.0(4), 4.1(1), 4.1(3), 4.2(1)	C225 M6, C245 M6	**Auto**, Disabled, Enabled	

Name	Description	Supported Attributes			
		Versions	Platforms	Values	Dependencies
CPU Downcore control	Provides the ability to remove one or more cores from operation is supported in the silicon. It may be desirable to reduce the number of cores due to OS restrictions, or power reduction requirements of the system. This item allows the control on the number of cores that are running. This setting can only reduce the number of cores from only those available in the processor.	4.0(2), 4.0(4), 4.1(1), 4.1(3), 4.2(1)	All M5 servers, C220 M6, C240 M6, C225 M6, C245 M6	**Auto**, Disabled, Enabled	
CPU SMT Mode	Simultaneous multithreading (SMT) is a processor technology that allows multiple instruction streams (threads) to run concurrently on the same physical processor, improving overall throughput.	4.2(1)	C225 M6, C245 M6	Disabled, **Enabled**	
ACPI SRAT L3 Cache As NUMA Domain	Creates a layer of virtual domains on top of the physical domains in which each CCX is declared to be in its on domain.	4.2(1)	C225 M6, C245 M6	**Auto**, Disabled, Enabled	

Name	Description	Supported Attributes			
		Versions	Platforms	Values	Dependencies
Channel Interleaving	Whether the CPU divides memory blocks and spreads contiguous portions of data across interleaved channels to enable simultaneous read operations.	4.0(2), 4.0(4), 4.1(1), 4.1(3), 4.2(1)	All M5 servers, C220 M6, C240 M6, C225 M6, C245 M6	**Auto**, 1-way to 4-way	
Cisco xGMI Max Speed	This option enables 18 Gbps XGMI link speed.	4.0(2), 4.0(4), 4.1(1), 4.1(3), 4.2(1)	C225 M6, C245 M6	**Disabled**, Enabled	
Closed Loop Thermal Throttling	To configure Closed Loop Thermal Throttling	4.0(2), 4.0(4), 4.1(1), 4.1(3), 4.2(1)	All M5 servers, C220 M6, C240 M6	**Disabled**, Enabled	
Processor CMCI	Enables CMCI generation.	4.0(2), 4.0(4), 4.1(1), 4.1(3), 4.2(1)	All M5 servers, C220 M6, C240 M6, C225 M6, C245 M6, C220 M7, C240 M7, X210c M7, X410c M7	**Disabled**, Enabled	
Config TDP	To configure TDP.	4.0(2), 4.0(4), 4.1(1), 4.1(3), 4.2(1)	All M5 servers, C220 M6, C240 M6, C225 M6, C245 M6	**Disabled**, Enabled	
Configurable TDP Level	Allows you to set customized value for Thermal Design Power (TDP).	4.0(2), 4.0(4), 4.1(1), 4.1(3), 4.2(1)	All M5 servers, C220 M6, C240 M6, C225 M6, C245 M6, C220 M7, C240 M7, X210c M7, X410c M7	**Normal**, Level 1, Level 2	

Name	Description	Supported Attributes			
		Versions	Platforms	Values	Dependencies
Core Multi Processing	Sets the state of logical processor cores per CPU in a package. If you choose All as the value, Intel Hyper Threading technology is also enabled.	4.0(2), 4.0(4), 4.1(1), 4.1(3), 4.2(1), 5.0(1), 5.0(2)	All M5 servers, C220 M6, C240 M6, C225 M6, C245 M6, B200 M6, X210c M6, C220 M7, C240 M7, X210c M7, X410c M7	**All**, 1 through 64 • All—Enables multiprocessing on all logical processor cores. • 1 through 64—Specifies the number of logical processor cores per CPU that can run on the server. To disable multiprocessing and have only one logical processor core per CPU running on the server, choose 1	We recommend that you contact your operating system vendor to make sure your operating system supports this feature.
Energy Performance	Allows you to determine whether system performance or energy efficiency is more important on this server.	4.0(2), 4.0(4), 4.1(1), 4.1(3), 4.2(1)	All M5 servers, C220 M6, C240 M6, C225 M6, C245 M6, C220 M7, C240 M7, X210c M7, X410c M7	**Performance** , Balanced Performance, Balanced Energy, Energy Efficient	**Power Technology** must be set to **Custom** or the server ignores the setting for this parameter.
Frequency Floor Override	Whether the CPU is allowed to drop below the maximum non-turbo frequency when idle.	4.0(2), 4.0(4), 4.1(1), 4.1(3), 4.2(1)	All M5 servers, C220 M6, C240 M6	**Disabled**, Enabled	

Name	Description	Supported Attributes			
		Versions	Platforms	Values	Dependencies
CPU Performance	CPU performance by adjusting server settings automatically.	4.0(2), 4.0(4), 4.1(1), 4.1(3), 4.2(1)	All M5 servers, B200 M6, C220 M6, C240 M6, C220 M7, C240 M7, X210c M7, X410c M7	**Disabled**, Enabled	
Power Technology	Enables you to configure the CPU power management settings for Enhanced Intel Speedstep Technology, Intel Turbo Boost Technology and Processor Power State C6.	4.0(2), 4.0(4), 4.1(1), 4.1(3), 4.2(1)	All M5 servers, B200 M6, C220 M6, C240 M6	**Disabled**, Energy efficient, Custom, Performance	
Demand Scrub	Whether the system corrects single bit memory errors encountered when the CPU or I/O makes a demand read.	4.0(2), 4.0(4), 4.1(1), 4.1(3), 4.2(1)	All M5 servers, C220 M6, C240 M6	**Disabled**, Enabled	
Direct Cache Access Support	Allows processors to increase I/O performance by placing data from I/O devices directly into the processor cache. This setting helps to reduce cache misses.	4.0(2), 4.0(4), 4.1(1), 4.1(3), 4.2(1)	All M5 servers, C220 M6, C240 M6, C225 M6, C245 M6	**Auto**, Disabled, Enabled	
DRAM Clock Throttling	Allows you to tune the system settings between the memory bandwidth and power consumption.	4.0(2), 4.0(4), 4.1(1), 4.1(3), 4.2(1)	All M5 servers, C220 M6, C240 M6, C225 M6, C245 M6	**Auto**, Balanced, Performance, Energy Efficient	

Name	Description	Supported Attributes			
		Versions	Platforms	Values	Dependencies
Energy Efficient Turbo	When energy efficient turbo is enabled, the optimal turbo frequency of the CPU turns dynamic based on CPU utilization. The power/performance bias setting also influences energy efficient turbo.	4.0(2), 4.0(4), 4.1(1), 4.1(3), 4.2(1)	All M5 servers, B200 M6, C220 M6, C240 M6, C220 M7, C240 M7, X210c M7, X410c M7	**Disabled**, Enabled	
Energy Performance Tuning	Determines if the BIOS or Operating System can turn on the energy performance bias tuning. The options are BIOS and OS.	4.0(2), 4.0(4), 4.1(1), 4.1(3), 4.2(1)	All M5 servers, C220 M6, C240 M6, C225 M6, C245 M6	**Disabled**, Enabled	
Enhanced Intel Speedstep(R) Technology	Whether the processor uses Enhanced Intel SpeedStep Technology, which allows the system to dynamically adjust processor voltage and core frequency. This technology can result in decreased average power consumption and decreased average heat production.	4.0(2), 4.0(4), 4.1(1), 4.1(3), 4.2(1)	All M5 servers, C220 M6, C240 M6, C220 M7, C240 M7, X210c M7, X410c M7	**Disabled**, Enabled	
Processor EPP Enable	Allows you to determine whether system performance or energy efficiency is more important on this server.	4.0(2), 4.0(4), 4.1(1), 4.1(3), 4.2(1)	All M5 servers, C220 M6, C240 M6, C225 M6, C245 M6	**Disabled**, Enabled	

Name	Description	Supported Attributes			
		Versions	Platforms	Values	Dependencies
EPP Profile	Allows you to determine whether system performance or energy efficiency is more important on this server.	4.0(2), 4.0(4), 4.1(1), 4.1(3), 4.2(1)	All M5 servers, C220 M6, C240 M6, C225 M6, C245 M6, C220 M7, C240 M7, X210c M7, X410c M7	**Disabled**, Enabled	
Execute Disable Bit	Classifies memory areas on the server to specify where the application code can execute. As a result of this classification, the processor disables code execution if a malicious worm attempts to insert code in the buffer. This setting helps to prevent damage, worm propagation, and certain classes of malicious buffer overflow attacks.	4.0(2), 4.0(4), 4.1(1), 4.1(3), 4.2(1)	All M5 servers, C220 M6, C240 M6, C225 M6, C245 M6, X210c M6	**Disabled**, Enabled	
Local X2 Apic	Allows you to set the type of Advanced Processor Interrupt controller (APIC) architecture.	4.0(2), 4.0(4), 4.1(1), 4.1(3), 4.2(1)	All M5 servers, C220 M6, C240 M6, C225 M6, C245 M6, C220 M7, C240 M7, X210c M7, X410c M7	**Disabled**, Enabled, X2APIC, XAPIC	
Hardware Prefetcher	Whether the processor allows the Intel hardware prefetcher to fetch streams of data and instruction from memory into the unified second-level cache when necessary.	4.0(2), 4.0(4), 4.1(1), 4.1(3), 4.2(1)	All M5 servers, C220 M6, C240 M6, C220 M7, C240 M7, X210c M7, X410c M7	**Disabled**, Enabled	

Name	Description	Supported Attributes			
		Versions	Platforms	Values	Dependencies
CPU Hardware Power Management	nables processor Hardware Power Management (HWPM).	4.0(2), 4.0(4), 4.1(1), 4.1(3), 4.2(1)	All M5 servers, C220 M6, C240 M6, C220 M7, C240 M7, X210c M7, X410c M7	**Disabled**, HWPM Native Mode, HWPM OOB Mode	
IMC Interleaving	This BIOS option controls the interleaving between the Integrated Memory Controllers (IMCs).	4.0(2), 4.0(4), 4.1(1), 4.1(3), 4.2(1)	All M5 servers, C220 M6, C240 M6	**Auto**, 1-way Interleave, 2-way Interleave	
Intel Dynamic Speed Select	Intel Dynamic Speed Select modes allow you to run the CPU with different speed and cores in auto mode.	4.0(2), 4.0(4), 4.1(1), 4.1(3), 5.0(1), 5.0(2)	All M5 servers, B200 M6, C220 M6, C240 M6, X210c M6, C220 M7, C240 M7, X210c M7, X410c M7	**Disabled**, Enabled	
Intel HyperThreading Tech	Whether the processor uses Intel Hyper-Threading Technology, which allows multithreaded software applications to execute threads in parallel within each processor.	4.0(2), 4.0(4), 4.1(1), 4.1(3)	All M5 servers, B200 M6, C220 M6, C240 M6, X210c M6, C220 M7, C240 M7, X210c M7, X410c M7 servers	**Disabled**, Enabled	
Intel Turbo Boost Tech	Whether the processor uses Intel Turbo Boost Technology, which allows the processor to automatically increase its frequency if it is running below power, temperature, or voltage specifications.	4.0(2), 4.0(4), 4.1(1), 4.1(3),	All M5 servers, B200 M6, C220 M6, C240 M6, X210c M6, C220 M7, C240 M7, X210c M7, X410c M7 servers	**Disabled**, Enabled	

Name	Description	Supported Attributes			
		Versions	Platforms	Values	Dependencies
Intel(R) VT	Whether the processor uses Intel Virtualization Technology for Directed I/O (VT-R)	4.0(2), 4.0(4), 4.1(1), 4.1(3)	All M5 servers, B200 M6, C220 M6, C240 M6, X210c M6, C220 M7, C240 M7, X210c M7, X410c M7 servers	**Disabled**, Enabled	
DCU IP Prefetcher	Whether the processor uses the DCU IP Prefetch mechanism to analyze historical cache access patterns and preload the most relevant lines in the L1 cache.	4.0(2), 4.0(4), 4.1(1), 4.1(3)	All M5 servers, B200 M6, C220 M6, C240 M6, X210c M6, C220 M7, C240 M7, X210c M7, X410c M7 servers	**Disabled**, Enabled	
KTI Prefetch	KTI prefetch is a mechanism to get the memory read started early on a DDR bus.	4.0(2), 4.0(4), 4.1(1), 4.1(3)	All M5 servers, B200 M6, C220 M6, C240 M6, X210c M6, C220 M7, C240 M7, X210c M7, X410c M7 servers	**Disabled**, Enabled	
LLC Prefetch	Whether the processor uses the LLC Prefetch mechanism to fetch the date into the LLC.	4.0(2), 4.0(4), 4.1(1), 4.1(3), 4.2(1)	All M5 servers, B200 M6, C220 M6, C240 M6, X210c M6, C220 M7, C240 M7, X210c M7, X410c M7 servers.	**Disabled**, Enabled	
Intel Memory Interleaving	Whether the CPU interleaves the physical memory so that the memory can be accessed while another is being refreshed.	4.0(2), 4.0(4), 4.1(1), 4.1(3)	All M5 servers	**Disabled**, Enabled	

Name	Description	Supported Attributes			
		Versions	Platforms	Values	Dependencies
Package C State Limit	The amount of power available to the server components when they are idle.	4.0(2), 4.0(4), 4.1(1), 4.1(3), 4.2(1)	All M5 servers, B200 M6, C220 M6, C240 M6, C220 M7, C240 M7, X210c M7, X410c M7	No Limit, Auto, **C0 C1 State**, C2, C6 Non Retention, C6 Retention	If you are changing the **Package C State Limit** token then ensure that the **Power Technology** is set to **Custom**.

Name	Description	Supported Attributes			
		Versions	Platforms	Values	Dependencies
Patrol Scrub	It sets the interval for a full memory scan.	4.0(2), 4.0(4), 4.1(1), 4.1(3), 4.2(1)	All M5 servers, B200 M6, C220 M6, C240 M6, C220 M7, C240 M7, X210c M7, X410c M7	**Disabled**, Enabled • Enable—The system periodically reads and writes memory searching for ECC errors. If any errors are found, the system attempts to fix them. This option may correct single bit errors before they become multi-bit errors, but it may adversely affect performance when the patrol scrub is running. • Disable—The system checks for memory ECC errors only when the CPU reads or writes a memory address.	The lower the interval, the more memory bandwidth is used for scrubbing.

Name	Description	Supported Attributes			
		Versions	Platforms	Values	Dependencies
Patrol Scrub Interval	Whether the system actively searches for, and corrects, single bit memory errors even in unused portions of the memory on the server at an interval of 5 to 23 hours.	4.0(2), 4.0(4), 4.1(1), 4.1(3), 4.2(1)	All M5 servers, C220 M6, C240 M6	Platform default	
Processor C1E	Allows the processor to transition to its minimum frequency upon entering C1. This setting does not take effect until after you have rebooted the server.	4.0(2), 4.0(4), 4.1(1), 4.1(3), 4.2(1)	All M5 servers, C220 M6, C240 M6, C220 M7, C240 M7, X210c M7, X410c M7	**Disabled**, Enabled	
Processor C3 Report	Whether the processor sends the C3 report to the operating system.	4.0(2), 4.0(4), 4.1(1), 4.1(3), 4.2(1)	All M5 servers, C220 M6, C240 M6	**Disabled**, Enabled, ACPI C2, ACPI C3	
Processor C6 Report	Whether the processor sends the C6 report to the operating system.	4.0(2), 4.0(4), 4.1(1), 4.1(3), 4.2(1)	All M5 servers, C220 M6, C240 M6, C220 M7, C240 M7, X210c M7, X410c M7	**Disabled**, Enabled	
CPU C State	Whether the AMD processors control IO-based C-state generation and DF C-states.	4.0(2), 4.0(4), 4.1(1), 4.1(3), 4.2(1)	C225 M5, C245 M5	**Auto**, Disabled, Enabled	

Name	Description	Supported Attributes			
		Versions	Platforms	Values	Dependencies
P-STATE Coordination **Note** It is also called EIST PSD Function in UCSM.	Allows you to define how BIOS communicates the P-state support model to the operating system. There are 3 models as defined by the Advanced Configuration and Power Interface (ACPI) specification.	4.0(2), 4.0(4), 4.1(1), 4.1(3), 4.2(1)	All M5 servers, C220 M6, C240 M6, C225 M6, C245 M6, C220 M7, C240 M7, X210c M7, X410c M7	**SW All**, HW All, SW Any	**Power Technology** must be set to **Custom** or the server ignores the setting for this parameter.
Power Performance Tuning	Determines if the BIOS or Operating System can turn on the energy performance bias tuning. The options are BIOS and OS.	4.0(2), 4.0(4), 4.1(1), 4.1(3), 4.2(1), C220 M7, C240 M7	All M5 servers, C220 M6, C240 M6, C220 M7, C240 M7, X210c M7, X410c M7	BIOS, **OS**, PECI	
UPI Link Frequency Select	Allows you to select different UPI link frequency running.	4.0(2), 4.0(4), 4.1(1), 4.1(3), 4.2(1), 5.0(1), 5.0(2)	All M5 servers, C220 M6, C240 M6, B200 M6, X210c M6, C220 M7, C240 M7, X210c M7, X410c M7	**Auto**, 9.6GT/S, 10.4GT/S, 11.2GT/S, 12.8GT/s, 14.4GT/s, 16.0GT/s, 20.0GT/s	
Rank Interleaving	Whether the CPU interleaves physical ranks of memory so that one rank can be accessed while another is being refreshed	4.0(2), 4.0(4), 4.1(1), 4.1(3), 4.2(1)	All M5 servers, C220 M6, C240 M6	**Auto**, 1-way, 2-way, 4-way, 8-way	
SMT Mode	Whether the processor uses AMD Simultaneous MultiThreading Technology, which allows multithreaded software applications to execute threads in parallel within each processor.	4.0(2), 4.0(4), 4.1(1), 4.1(3), 4.2(1)	C225 M6, C245 M6	**Disabled**, Enabled	

Name	Description	Supported Attributes			
		Versions	Platforms	Values	Dependencies
Sub Numa Clustering	Whether the CPU supports sub NUMA clustering, in which the tag directory and the memory channel are always in the same region.	4.0(2), 4.0(4), 4.1(1), 4.1(3), 4.2(1)	All M5 servers, C220 M6, C240 M6, C220 M7, C240 M7, X210c M7, X410c M7	**Disabled**, Enabled, SNC2, SNC4	
DCU Streamer Prefetch	Whether the processor uses the DCU IP Prefetch mechanism to analyze historical cache access patterns and preload the most relevant lines in the L1 cache.	4.0(2), 4.0(4), 4.1(1), 4.1(3), 4.2(1)	All M5 servers, C220 M6, C240 M6, C220 M7, C240 M7, X210c M7, X410c M7	**Disabled**, Enabled	
SVM Mode	Whether the processor uses AMD Secure Virtual Machine Technology.	4.0(2), 4.0(4), 4.1(1), 4.1(3), 4.2(1)	C225 M6, C245 M6	**Disabled**, Enabled	
Uncore Frequency Scaling	Allows you configure the scaling of the uncore frequency of the processor.	4.0(2), 4.0(4), 4.1(1), 4.1(3), 4.2(1), 5.0(1), 5.0(2)	All M5 servers, C220 M6, C240 M6, B200 M6, X210c M6, C220 M7, C240 M7, X210c M7, X410c M7	Disabled, **Enabled**	
Workload Configuration	This feature allows for workload optimization.	4.0(2), 4.0(4), 4.1(1), 4.1(3), 4.2(1)	All M5 servers, C220 M6, C240 M6, C220 M7, C240 M7, X210c M7, X410c M7	Balanced, **IO Sensitive**, NUMA, UMA	
XPT Prefetch	Whether XPT prefetch is used to enable a read request sent to the last level cache to issue a copy of that request to the memory controller prefetcher.	4.0(2), 4.0(4), 4.1(1), 4.1(3), 4.2(1)	All M5 servers, C220 M6, C240 M6, C220 M7, C240 M7, X210c M7, X410c M7	**Disabled**, Enabled	

Name	Description	Supported Attributes			
		Versions	Platforms	Values	Dependencies
X2APIC Opt-Out Flag	Prevents the OS from enabling extended xAPIC (x2APIC) mode when the OS is not working with x2APIC.	4.2(3)	C220M6, C240M6, B200M6, X210c M6, C220 M7, C240 M7, X210c M7, X410c M7	**Disabled**, Enabled	
Intel Speed Select	Allows you to adjust different core to operate in different frequency to have a better power efficiency. The values **Config 1** and **Config 2** are not supported on Cisco UCS M6 and M7 servers. For Cisco UCS M6 and Cisco UCS M7 servers, the values **Config 3** and **Config 4** (4th Gen Intel Xeon Scalable processors and 5th Gen Intel Xeon Scalable processors) are equivalent to the values **Config 1** and **Config 2** (3rd Gen Intel Xeon Scalable processors).	4.0(2), 4.0(4), 4.1(1), 4.1(3), 4.2(1), 5.0(1), 5.0(2), 4.2(3)	C220M6, C240M6, B200M6, X210c M6, C220 M7, C240 M7, X210c M7, X410c M7	**Auto**, Base, Config 1, Config 2, Config 3, Config 4	

CHAPTER 10

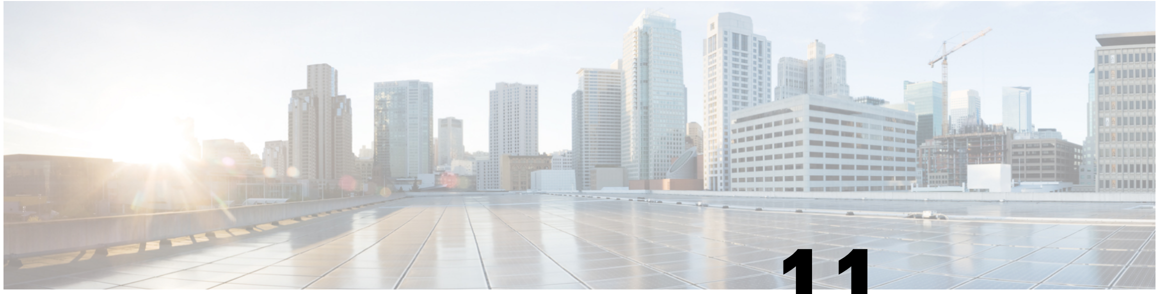
QPI

QPI

The following table lists the QPI BIOS settings that you can configure through a BIOS policy or the default BIOS settings:

Name	Description	Supported Attributes			
		Versions	Platforms	Values	Dependencies
QPI Link Frequency Select	The Intel QuickPath Interconnect (QPI) link frequency, in megatransfers per second (MT/s).	4.0(4), 4.1(1), 4.1(3), 4.2(1), 4.3(3a)	X410c M7, X210c M7,C220 M7, C240 M7, C240 M6, C220 M6, C225 M6, C245 M6, C220 M5, C240 M5, B200 M5	**Auto**, 20.0GT/s,12.8GT/s, 14.4GT/s, 16.0GT/s, 9.6 GT/s, 8.0 GT/s, 7.2 GT/s, 6.4 GT/s	

Name	Description	Supported Attributes			
		Versions	Platforms	Values	Dependencies
QPI Snoop Mode	Allows you to configure QPI in one of the snoop mode.	4.2(1)	C240 M6, C220 M6	Home Snoop, Cluster On Die, Home Directory Snoop with OSB, Early Snoop, **Auto** • **Home Snoop**—The snoop is always spawned by the home agent (centralized ring stop) for the memory controller. This mode has a higher local latency than early snoop, but it provides extra resources for a larger number of outstanding transactions. • **Cluster on Die**—This mode is available only for processors that have 10 or more cores. It is the best mode for highly NUMA optimized workloads • **Early Snoop**—The distributed cache ring stops can send a snoop probe or a request to another caching agent directly. This mode has lower latency and it is best for workloadsthat have shared data sets across threads and can benefit from a cache-to-cache transfer, or for workloads that are not NUMA optimized.	



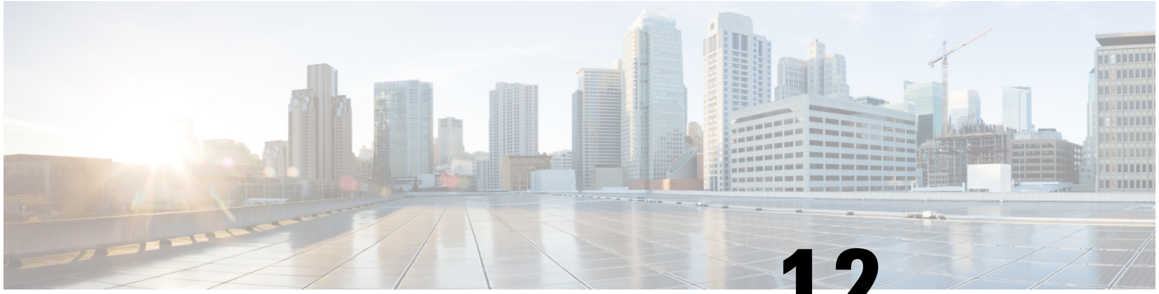
CHAPTER 11

Serial Port

Serial Port

The following table lists the serial port BIOS settings that you can configure through a BIOS policy or the default BIOS settings:

Name	Description	Supported Attributes			
		Versions	Platforms	Values	Dependencies
Serial A Enable	Whether serial port A is enabled or disabled.	4.2(1)	C225 M6, C245 M6, B200 M6, X210c M6	**Enabled**, Disabled	



CHAPTER 12

Server Management

Server Management

The following table lists the server management BIOS settings that you can configure through a BIOS policy or the default BIOS settings:

Name	Description	Supported Attributes			
		Versions	**Platforms**	**Values**	**Dependencies**
Assert NMI on PERR	Whether the BIOS generates a non-maskable interrupt (NMI) and logs an error when a processor bus parity error (PERR) occurs.	4.2(1)	C240 M6, C220 M6, C225 M6, C245 M6	**Enabled**, Disabled	
Assert NMI on SERR	Whether the BIOS generates a non-maskable interrupt (NMI) and logs an error when a system error (SERR) occurs.	4.2(1)	C240 M6, C220 M6, C225 M6, C245 M6	**Enabled**, Disabled	
Baud Rate	What Baud rate is used for the serial port transmission speed. If you disable Console Redirection, this option is not available.	4.2(1), 5.0(1), 5.0(2)	C240 M6, C220 M6, C225 M6, C245 M6, B200 M6, X210c M6, C220 M7, C240 M7, X210c M7, X410c M7	9.6k, 19.2k, 38.4k, 57.6k, **115.2k**	This setting must match the setting on the remote terminal application.

Name	Description	Supported Attributes			
		Versions	Platforms	Values	Dependencies
Consistent Device Naming	Consistent Device Naming allows Ethernet interfaces to be named in a consistent manner. This makes Ethernet interface names more uniform, easy to identify, and persistent when adapter or other configuration changes are made.	4.2(1)	C240 M6, C220 M6, C225 M6, C245 M6	Enabled, **Disabled**	
Adaptive Memory Training	When this token is enabled, the BIOS saves the memory training results (optimized timing/voltage values) along with CPU/memory configuration information and reuses them on subsequent reboots to save boot time. The saved memory training results are used only if the reboot happens within 24 hours of the last save operation.	4.2(1)	C240 M6, C220 M6, C225 M6, C245 M6, X210c M6, C220 M7, C240 M7, X210c M7, X410c M7	**Enabled**, Disabled	
BIOS Techlog Level	This option denotes the type of messages in BIOS tech log file.	4.2(1)	C240 M6, C220 M6, C225 M6, C245 M6, C220 M7, C240 M7, X210c M7, X410c M7	Maximum, **Minimum**, Normal • Maximum—Critical messages will be displayed in the log file. This is the default option • Minimum—Warning and loading messages will be displayed in the log file. • Normal—Normal and information related messages will be displayed in the log file.	

Name	Description	Supported Attributes			
		Versions	Platforms	Values	Dependencies
OptionROM Launch Optimization	The Option ROM launch is controlled at the PCI Slot level, and is enabled by default. In configurations that consist of a large number of network controllers and storage HBAs having Option ROMs, all the Option ROMs may get launched if the PCI Slot Option ROM Control is enabled for all. However, only a subset of controllers may be used in the boot process. When this token is enabled, Option ROMs are launched only for those controllers that are present in boot policy.	4.2(1)	C240 M6, C220 M6, C225 M6, C245 M6, C220 M7, C240 M7, X210c M7, X410c M7	**Enabled**, Disabled	

Name	Description	Supported Attributes			
		Versions	Platforms	Values	Dependencies
Console Redirection	Allows a serial port to be used for console redirection during POST and BIOS booting. After the BIOS has booted and the operating system is responsible for the server, console redirection is irrelevant and has no effect	4.2(1), 5.0(1), 5.0(2)	C240 M6, C220 M6, C225 M6, C245 M6, B200 M6, X210c M6, C220 M7, C240 M7, X210c M7, X410c M7	**Disabled**, COM0, COM 1, serial-port-b Platform Default • COM0 enables serial port for console redirection during POST. This option is valid only for M6 blade servers and rack-mount servers. • COM1 or serial-port-b enables serial port B for console redirection and allows it to perform server management tasks. This option is only valid for rack-mount servers.	If you enable this option, you also disable the display of the Quiet Boot logo screen during POST.
Flow Control	Whether a handshake protocol is used for flow control. Request to Send / Clear to Send (RTS/CTS) helps to reduce frame collisions that can be introduced by a hidden terminal problem.	4.2(1), 5.0(1), 5.0(2)	C240 M6, C220 M6, C225 M6, C245 M6, B200 M6, X210c M6, C220 M7, C240 M7, X210c M7, X410c M7	**None**, RTC-CTS	This setting must match the setting on the remote terminal application.
FRB-2 Timer	Whether the FRB2 timer is used for recovering the system if it hangs during POST.	4.2(1), 5.0(1), 5.0(2)	C240 M6, C220 M6, C225 M6, C245 M6, B200 M6, X210c M6, C220 M7, C240 M7, X210c M7, X410c M7	**Enabled**, Disabled	

Name	Description	Supported Attributes			
		Versions	Platforms	Values	Dependencies
Legacy OS Redirection	Whether redirection from a legacy operating system, such as DOS, is enabled on the serial port.	4.2(1)	C240 M6, C220 M6, C225 M6, C245 M6	**Enabled**, Disabled	
OS Boot Watchdog Timer	Whether the BIOS programs the watchdog timer with a predefined timeout value. If the operating system does not complete booting before the timer expires, the CIMC resets the system and an error is logged.	4.2(1), 5.0(1), 5.0(2)	C240 M6, C220 M6, C225 M6, C245 M6, B200 M6, X210c M6, C220 M7, C240 M7, X210c M7, X410c M7	**Enabled**, Disabled	
OS Boot Watchdog Timer Policy	What action the system takesif the watchdog timer expires.	4.2(1), 5.0(1), 5.0(2)	C240 M6, C220 M6, C225 M6, C245 M6, B200 M6, X210c M6, C220 M7, C240 M7, X210c M7, X410c M7	**Power-off**, Reset	
OS Boot Watchdog Timer Timeout	What timeout value the BIOS uses to configure the watchdog timer.	4.2(1), 5.0(1), 5.0(2)	C240 M6, C220 M6, C225 M6, C245 M6, B200 M6, X210c M6, C220 M7, C240 M7, X210c M7, X410c M7	5 minutes, **10 minutes**, 15 minutes, 20 minutes	
Out-of-Band Mgmt Port	Used for Windows Special Administration Control (SAC). This option allows you to configure the COM port 0 that can be used for Windows Emergency Management services. ACPI SPCR table is reported based on this setup option.	4.2(1)	C240 M6, C220 M6, C225 M6, C245 M6	**Enabled**, Disabled	

Name	Description	Supported Attributes			
		Versions	Platforms	Values	Dependencies
Putty KeyPad	Allows you to change the action of the PuTTY function keys and the top row of the numeric keypad.	4.2(1)	C240 M6, C220 M6, C225 M6, C245 M6		

Name	Description	Supported Attributes			
		Versions	Platforms	Values	Dependencies
				VT100, **Linux**, XTERMR6, SCO, ESCN, VT400 • VT100—The function keys generate ESC OP through ESC O[. • Linux—Mimicsthe Linux virtual console.Function keys F6 to F12 behave like the default mode, but F1 to F5 generate ESC [[A through ESC [[E. • VT400—The function keys behave like the default mode. The top row of the numeric keypad generates ESC OP through ESC OS. • ESCN—The default mode. The function keys match the general behavior of Digital terminals. The function keys generate sequences such as ESC [11~ and ESC [12~. • SCO—The function keys F1 to F12 generate ESC [M through ESC [X. The function and	

Name	Description	Supported Attributes			
		Versions	Platforms	Values	Dependencies
				shift keys generate ESC [Y through ESC [j. The control and function keys generate ESC [k through ESC [v. The shift, control and function keys generate ESC [w through ESC [{.	
Redirection After BIOS POST	Whether BIOS console redirection should be active after BIOS POST is complete and control given to the OS bootloader.	4.2(1), 5.0(1), 5.0(2)	C240 M6, C220 M6, C225 M6, C245 M6, B200 M6, X210c M6	**Always Enable**, Bootloader • Always Enable—BIOS Legacy console redirection is active during the OS boot and run time. • Bootloader—BIOS Legacy console redirection is disabled before giving control to the OS boot loader.	
Terminal Type	What type of character formatting is used for console redirection.	4.2(1), 5.0(1), 5.0(2)	C240 M6, C220 M6, C225 M6, C245 M6, B200 M6, X210c M6, C220 M7, C240 M7, X210c M7, X410c M7	PC-ANSI, **VT100**, VT100-PLUS, VT-UTF8	This setting must match the setting on the remote terminal application.

CHAPTER 13

Trusted Platform

Trusted Platform

The following table lists the trusted platform BIOS settings that you can configure through a BIOS policy or the default BIOS settings:

Name	Description	Supported Attributes			
		Versions	Platforms	Values	Dependencies
Multikey Total Memory Encryption (MK-TME)	MK-TME allows you to have multiple encryption domains with one with own key. Different memory pages can be encrypted with different keys.	4.2(1), 5.0(1), 5.0(2)	C240 M6, C220 M6, C225 M6, C245 M6, B200 M6, X210c M6, C220 M7, C240 M7, X210c M7, X410c M7	**Enabled**, Disabled	
Software Guard Extensions (SGX)	Allows you to enableSoftware Guard Extensions(SGX) feature.	4.2(1), 5.0(1), 5.0(2)	C240 M6, C220 M6, C225 M6, C245 M6, B200 M6, X210c M6, C220 M7, C240 M7, X210c M7, X410c M7	**Enabled**, Disabled	
Total Memory Encryption (TME)	Allows you to provide the capability to encrypt the entirety of the physical memory of a system.	4.2(1), 5.0(1), 5.0(2)	C240 M6, C220 M6, C225 M6, C245 M6, B200 M6, X210c M6, C220 M7, C240 M7, X210c M7, X410c M7	**Enabled**, Disabled	

Name	Description	Supported Attributes			
		Versions	Platforms	Values	Dependencies
Select Owner EPOCH Input Type	Allows you to change the seed for the security key used for the locked memory region that is created.	4.2(1), 5.0(1), 5.0(2)	C240 M6, C220 M6, C225 M6, C245 M6, B200 M6, X210c M6, C220 M7, C240 M7, X210c M7, X410c M7	SGX Owner EPOCH activated, Change to New Random Owner EPOCHs, **Manual User Defined Owner EPOCHs**	
SGX Auto MP Registration Agent	Allows you to enable the registration authority service to store the platform keys.	4.2(1), 5.0(1), 5.0(2)	C240 M6, C220 M6, C225 M6, C245 M6, B200 M6, X210c M6, C220 M7, C240 M7, X210c M7, X410c M7	**Enabled**, Disabled	
SGX Epoch 0	Allows you to define the SGX EPOCH owner value for the EPOCH number designated by 0.	4.2(1), 5.0(1), 5.0(2)	C240 M6, C220 M6, C225 M6, C245 M6, B200 M6, X210c M6, C220 M7, C240 M7, X210c M7, X410c M7	**Enabled**, Disabled	
SGX Epoch 1	Allows you to define the SGX EPOCH owner value for the EPOCH number designated by 1.	4.2(1), 5.0(1), 5.0(2)	C240 M6, C220 M6, C225 M6, C245 M6, B200 M6, X210c M6, C220 M7, C240 M7, X210c M7, X410c M7	**Enabled**, Disabled	
SGX Factory Reset	Allows the system to perform SGX factory reset on subsequent boot.	4.2(1), 5.0(1), 5.0(2)	C240 M6, C220 M6, C225 M6, C245 M6, B200 M6, X210c M6, C220 M7, C240 M7, X210c M7, X410c M7	**Enabled**, Disabled	

Name	Description	Supported Attributes			
		Versions	Platforms	Values	Dependencies
SGX PubKey Hash*n* where *n* ranges from 0 to 3.	Allows you to set the Software Guard Extensions (SGX) value.	4.2(1), 5.0(1), 5.0(2)	C240 M6, C220 M6, C225 M6, C245 M6, B200 M6, X210c M6, C220 M7, C240 M7, X210c M7, X410c M7	**SGX PUBKEY HASH0**, SGX PUBKEY HASH1, SGX PUBKEY HASH2, SGX PUBKEY HASH3 • SGX PUBKEY HASH0—Between 7-0. • SGX PUBKEY HASH1—Between 15-8. • SGX PUBKEY HASH2—Between 23-16. • SGX PUBKEY HASH3—Between 31-24.	
SGX Write Enable	Allows you to enable SGX Write feature.	4.2(1), 5.0(1), 5.0(2)	C240 M6, C220 M6, C225 M6, C245 M6, B200 M6, X210c M6, C220 M7, C240 M7, X210c M7, X410c M7	**Enabled**, Disabled	
SGX Package Information In-Band Access	Allows you to enable SGX Package Info In-Band Access.	4.2(1), 5.0(1), 5.0(2)	C240 M6, C220 M6, C225 M6, C245 M6, B200 M6, X210c M6, C220 M7, C240 M7, X210c M7, X410c M7	Enabled, **Disabled**	

Name	Description	Supported Attributes			
		Versions	Platforms	Values	Dependencies
SGX QoS	Allows you to enable SGX QoS.	4.2(1), 5.0(1), 5.0(2)	C240 M6, C220 M6, C225 M6, C245 M6, B200 M6, X210c M6, C220 M7, C240 M7, X210c M7, X410c M7	**Enabled**, Disabled	
SHA-1 PCR Bank	The Platform Configuration Register (PCR) is a memory location in the TPM. Multiple PCRs are collectively referred to as a PCR bank. A Secure Hash Algorithm 1 or SHA-1 PCR Bank allows to enable or disable TPM security.	4.2(1), 5.0(1), 5.0(2)	C240 M6, C220 M6, C225 M6, C245 M6, B200 M6, X210c M6, C220 M7, C240 M7, X210c M7, X410c M7	**Enabled**, Disabled	If the Security Device Support is disabled then the entire TPM operation will fail.
SHA256 PCR Bank	The Platform Configuration Register (PCR) is a memory location in the TPM. Multiple PCRs are collectively referred to as a PCR bank. A Secure Hash Algorithm 256-bit or SHA-256PCR Bank allows to enable or disable TPM security.	4.2(1), 5.0(1), 5.0(2)	C240 M6, C220 M6, C225 M6, C245 M6, B200 M6, X210c M6, , C220 M7, C240 M7, X210c M7, X410c M7	**Enabled**, Disabled	If the Security Device Support is disabled then the entire TPM operation will fail.

Name	Description	Supported Attributes			
		Versions	Platforms	Values	Dependencies
SHA384 PCR Bank	The Platform Configuration Register (PCR) is a memory location in the TPM. Multiple PCRs are collectively referred to as a PCR bank. A Secure Hash Algorithm 256-bit or SHA-384PCR Bank allows to enable or disable TPM security.	4.3(3a)	X410c M7, X210c M7, C220 M7, C240 M7	Enabled, **Disabled**	If the Security Device Support is disabled then the entire TPM operation will fail.
Trusted Platform Module State	Whether to enable or disable the TrustedPlatform Module (TPM), which is a component that securely stores artifactsthat are used to authenticate the server.	4.2(1), 5.0(1), 5.0(2)	C240 M6, C220 M6, C225 M6, C245 M6, B200 M6, X210c M6, C220 M7, C240 M7, X210c M7, X410c M7	**Enabled**, Disabled	If the Security Device Support is disabled then the entire TPM operation will fail.
Trust Domain Extension	Whether to enable or disable the Trust Domain Extension (TDX), which protects the sensitive data and applications from unauthorized access.	4.3(3a)	X410c M7, X210c M7, C220 M7, C240 M7	Enabled, **Disabled**	To enable Trust Domain Extension, ensure that: • Total Memory Encryption (TME) is Enabled. • Software Guard Extensions (SGX) is Enabled. • Multikey Total Memory Encryption (MK-TME) is Enabled. • LIMIT CPU PA to 46 Bits token is Disabled.

Name	Description	Supported Attributes			
		Versions	Platforms	Values	Dependencies
TDX Secure Arbitration Mode Loader	Whether to enable or disable the TDX Secure Arbitration Mode (SEAM) Loader, which helps to verify the digital signature on the Intel TDX module and load it into the SEAM-memory range.	4.3(3a)	X410c M7, X210c M7, C220 M7, C240 M7	Enabled, **Disabled**	To enable TDX Secure Arbitration Mode Loader, ensure that: • Total Memory Encryption (TME) is Enabled. • Software Guard Extensions (SGX) is Enabled. • Multikey Total Memory Encryption (MK-TME) is Enabled. • LIMIT CPU PA to 46 Bits token is Disabled. • Trust Domain Extension (TDX) is Enabled.
TPM Pending Operation	Trusted Platform Module (TPM) Pending Operation option allows you to control the status of the pending operation.	4.2(1), 5.0(1), 5.0(2)	C240 M6, C220 M6, C225 M6, C245 M6, B200 M6, X210c M6, C220 M7, C240 M7, X210c M7, X410c M7	**None**, TpmClear	If the Security Device Support is disabled then the entire TPM operation will fail.
TPM Minimal Physical Presence	Whether to enable or disable TPM Minimal Physical Presence, which enables or disables the communication between the OS and BIOS for administering the TPM without compromising the security.	4.2(1)	C240 M6, C220 M6, C225 M6, C245 M6, B200 M6, X210c M6, C220 M7, C240 M7, X210c M7, X410c M7	Enabled, **Disabled**	If the Security Device Support is disabled then the entire TPM operation will fail.
Intel Trusted Execution Technology Support	Whether to enable or disable Intel Trusted Execution Technology (TXT), which provides greater protection for information that is used and stored on the business server.	4.2(1), 5.0(1), 5.0(2)	C240 M6, C220 M6, C225 M6, C245 M6, B200 M6, X210c M6, C220 M7, C240 M7, X210c M7, X410c M7	**Enabled**, Disabled	TPM cannot be disabled unless TXT is disabled.

Name	Description	Supported Attributes			
		Versions	Platforms	Values	Dependencies
Security Device Support	It controls the entire TPM functionality.	4.2(3)	C220M6, C240M6, C225M6, C245M6, B200M6, X210c M6, C220 M7, C240 M7, X210c M7, X410c M7	**Enabled**, Disabled	
DMA Control Opt-In Flag	Enabling this token enables Windows 2022 Kernel DMA Protection feature. The OS treats this as a hint that the IOMMU should be enabled to prevent DMA attacks from possible malicious devices.	4.2(2), 4.2(3)	C220 M6 and C240 M6, B200 M6, X210c M6, C220 M7, C240 M7, X210c M7, X410c M7	Enabled, **Disabled**	
LIMIT CPU PA to 46 Bits	Limits CPU physical address to 46 bits to support the older Hyper-v CPU platform.	4.2(2), 4.2(3)	C220 M6, C240 M6, B200 M6, X210c M6, C220 M7, C240 M7, X210c M7, X410c M7	**Enabled**, Disabled	

CHAPTER 14

USB

USB

The following table lists the USB BIOS settings that you can configure through a BIOS policy or the default BIOS settings:

Name	Description	Supported Attributes			
		Versions	Platforms	Values	Dependencies
All USB Devices	Whether all physical and virtual USB devices are enabled or disabled	4.2(1)	C240 M6, C220 M6, B200 M6, X210c M6	**Enabled**, Disabled	
Legacy USB Support	Whether the system supports legacy USB devices.	4.2(1), 5.0(1), 5.0(2)	C240 M6, C220 M6, B200 M6, X210c M6	**Auto**,Enabled, Disabled	
Make Device Non Bootable	Whether the server can boot from a USB device.	4.2(1)	C240 M5, C220 M5, C480 M5	**Enabled**, Disabled	
xHCI Mode	Whether xHCI mode is enabled or disabled.	4.2(1)	C240 M5, C220 M5, C480 M5	**Enabled**, Disabled	
Port 60/64 Emulation	Whether the system supports 60h/64h emulation for complete USB keyboard legacy support.	4.2(1)	C240 M5, C220 M5, C480 M5	Enabled, **Disabled**	You should select Enabled option if you are using a non-USB aware operating system on the server.

Name	Description	Supported Attributes			
		Versions	Platforms	Values	Dependencies
USB Port Front	Whether the front panel USB devices are enabled or disabled.	4.2(1)	C240 M5, C220 M5, C480 M5, B200 M6, X210c M6, X210c M7, X410c M7	**Enabled**, Disabled	
USB Port Internal	Whether the internal USB devices are enabled or disabled.	4.2(1)	C240 M5, C220 M5, C480 M5	**Enabled**, Disabled	
USB Port KVM	Whether the USB Port KVM devices are enabled or disabled.	4.2(1)	C240 M5, C220 M5, C480 M5, B200 M6, X210c M6, X210c M7, X410c M7	**Enabled**, Disabled	
USB Port Rear	Whether the USB port rear devices are enabled or disabled.	4.2(1)	C240 M5, C220 M5, C480 M5, C220 M7, C240 M7	**Enabled**, Disabled	
USB Port SD Card	Whether the SD card drives are enabled or disabled.	4.2(1)	C240 M5, C220 M5, C480 M5, B200 M6, X210c M6, X210c M7, X410c M7	**Enabled**, Disabled	
USB Port VMedia	Whether the virtual media devices are enabled or disabled.	4.2(1)	C240 M5, C220 M5, C480 M5	**Enabled**, Disabled	
XHCI Legacy Support	Whether xHCI mode is enabled or disabled.	4.2(1)	C240 M5, C220 M5, C480 M5	**Enabled**, Disabled	