



Cisco UCS Server BIOS Tokens, Release 4.2

First Published: 2021-06-24

Last Modified: 2023-01-06

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 NON-INFRINGEMENT 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.

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.

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)

© 2021–2023 Cisco Systems, Inc. All rights reserved.



CONTENTS

PREFACE

| | |
|---------------------------------|----------|
| Preface | v |
| Audience | v |
| Conventions | v |
| Related Cisco UCS Documentation | vii |
| Documentation Feedback | vii |

CHAPTER 1

| | |
|---------------------------------------|----------|
| UCS Server BIOS Tokens | 1 |
| Server BIOS Tokens in Release 4.2(3b) | 1 |
| Server BIOS Tokens in Release 4.2(2c) | 2 |
| Server BIOS Tokens in Release 4.2(1m) | 2 |
| Server BIOS Tokens in Release 4.2(1l) | 3 |
| Server BIOS Tokens in Release 4.2(1i) | 7 |
| Server BIOS Tokens in Release 4.2(1f) | 12 |
| Server BIOS Tokens in Release 4.2(1d) | 15 |



Preface

- [Audience, on page v](#)
- [Conventions, on page v](#)
- [Related Cisco UCS Documentation, on page vii](#)
- [Documentation Feedback, on page vii](#)

Audience

This guide is intended primarily for data center administrators with responsibilities and expertise in one or more of the following:

- Server administration
- Storage administration
- Network administration
- Network security

Conventions

| Text Type | Indication |
|-----------------|--|
| GUI elements | GUI elements such as tab titles, area names, and field labels appear in this font . Main titles such as window, dialog box, and wizard titles appear in this font . |
| Document titles | Document titles appear in <i>this font</i> . |
| TUI elements | In a Text-based User Interface, text the system displays appears in <code>this font</code> . |
| System output | Terminal sessions and information that the system displays appear in <code>this font</code> . |
| CLI commands | CLI command keywords appear in this font . Variables in a CLI command appear in <i>this font</i> . |
| [] | Elements in square brackets are optional. |

| Text Type | Indication |
|-------------|---|
| {x y z} | Required alternative keywords are grouped in braces and separated by vertical bars. |
| [x y z] | Optional alternative keywords are grouped in brackets and separated by vertical bars. |
| string | A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks. |
| <> | Nonprinting characters such as passwords are in angle brackets. |
| [] | Default responses to system prompts are in square brackets. |
| !, # | An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line. |



Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the document.



Tip Means *the following information will help you solve a problem*. The tips information might not be troubleshooting or even an action, but could be useful information, similar to a Timesaver.



Timesaver Means *the described action saves time*. You can save time by performing the action described in the paragraph.



Caution Means *reader be careful*. In this situation, you might perform an action that could result in equipment damage or loss of data.



Warning IMPORTANT SAFETY INSTRUCTIONS

This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device.

SAVE THESE INSTRUCTIONS

Related Cisco UCS Documentation

Documentation Roadmaps

For a complete list of all B-Series documentation, see the *Cisco UCS B-Series Servers Documentation Roadmap* available at the following URL: https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/overview/guide/UCS_roadmap.html

For a complete list of all C-Series documentation, see the *Cisco UCS C-Series Servers Documentation Roadmap* available at the following URL: https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/overview/guide/ucs_rack_roadmap.html.

For information on supported firmware versions and supported UCS Manager versions for the rack servers that are integrated with the UCS Manager for management, refer to [Release Bundle Contents for Cisco UCS Software](#).

Documentation Feedback

To provide technical feedback on this document, or to report an error or omission, please send your comments to ucs-docfeedback@external.cisco.com. We appreciate your feedback.



CHAPTER 1

UCS Server BIOS Tokens

- [Server BIOS Tokens in Release 4.2\(3b\), on page 1](#)
- [Server BIOS Tokens in Release 4.2\(2c\), on page 2](#)
- [Server BIOS Tokens in Release 4.2\(1m\), on page 2](#)
- [Server BIOS Tokens in Release 4.2\(1l\), on page 3](#)
- [Server BIOS Tokens in Release 4.2\(1i\), on page 7](#)
- [Server BIOS Tokens in Release 4.2\(1f\), on page 12](#)
- [Server BIOS Tokens in Release 4.2\(1d\), on page 15](#)

Server BIOS Tokens in Release 4.2(3b)

Cisco UCS Manager continues to support the following servers in 4.2(3b):

- C220 M6
- C240 M6
- C225 M6
- C245 M6
- B200 M6

For Cisco UCS C-series and B-series BIOS tokens supported on M4 and M5 servers, refer [Cisco UCS Server BIOS Tokens, Release 4.1](#).

New and Changed BIOS Tokens for 4.2(3b)

| Name | Default Value | M6 Server Supported Values | Platform | Dependencies | New/Changed |
|------------------------------|---------------|----------------------------|--|--------------|-------------|
| X2APIC Opt Out | Disabled | Disabled, Enabled | C220M6, C240M6, B200M6 | | New |
| Security Dev. Support | Enabled | Disabled, Enabled | C220M6, C240M6, C225M6, C245M6, B200M6 | | New |

Server BIOS Tokens in Release 4.2(2c)

Cisco UCS Manager supports the following servers in 4.2(2c) release:

- C220 M6
- C240 M6

For Cisco UCS C-series and B-series BIOS tokens supported on M4 and M5 servers, refer [Cisco UCS Server BIOS Tokens, Release 4.1](#).

BIOS Tokens for C220 M6 and C240 M6 in 4.2(2c)

The following table lists the new BIOS tokens for 4.2(2c) release:

| Name | Default Value | M6 Server Supported Values | Platform | New/Changed |
|--------------------------------------|---------------|----------------------------|---------------------|-------------|
| TPM Minimal Physical Presence | Disabled | Disabled, Enabled | C220 M6 and C240 M6 | New |
| DMA Control Opt-In Flag | Disabled | Disabled, Enabled | C220 M6 and C240 M6 | New |

Server BIOS Tokens in Release 4.2(1m)

Cisco UCS Manager continues to support the following servers in 4.2(1m):

- C220 M6
- C240 M6
- C225 M6
- C245 M6
- B200 M6

For Cisco UCS C-series and B-series BIOS tokens supported on M4 and M5 servers, refer [Cisco UCS Server BIOS Tokens, Release 4.1](#).

New and Changed BIOS Tokens for 4.2(1m)

| Name | Default Value | M6 Server Supported Values | Platform | Dependencies | New/Changed |
|----------------------------|---------------|----------------------------|---|--------------|-------------|
| Execute Disable Bit | Enabled | Disabled, Enabled | C220 M6, C240 M6, C225 M6, C245 M6, B200 M6 | | New |

Server BIOS Tokens in Release 4.2(11)

Cisco UCS Manager introduces support for the following servers in 4.2(11):

- C225 M6

Cisco UCS Manager continues to support the following servers in 4.2(11):

- C220 M6
- C240 M6
- C245 M6
- B200 M6

For Cisco UCS C-series and B-series BIOS tokens supported on M4 and M5 servers, refer [Cisco UCS Server BIOS Tokens, Release 4.1](#).

BIOS Tokens for C225 M6 in 4.2(11)

| Name | Default Value | M6 Server Supported Values | Platform | Dependencies |
|---------------------------------------|---------------|--|----------|---|
| MLOM Link Speed | Auto | Disabled, Auto, GEN1, GEN2, GEN3, GEN4 | C225 M6 | |
| MLOM OptionROM | Enabled | Disabled, Enabled | C225 M6 | |
| PCIe Slot <i>n</i> Link Speed | Auto | Disabled, Auto, GEN1, GEN2, GEN3, GEN4 | C225 M6 | The <i>n</i> refers to an integer from 1 to 3. |
| PCIe Slot <i>n</i> OptionROM | Enabled | Enabled, Disabled | C225 M6 | The <i>n</i> refers to an integer from 1 to 3. |
| MRAID Link Speed | Auto | Disabled, Auto, GEN1, GEN2, GEN3, GEN4 | C225 M6 | |
| MRAID OptionROM | Enabled | Disabled, Enabled | C225 M6 | |
| Front NVME <i>n</i> Link Speed | Auto | Disabled, Auto, GEN1, GEN2, GEN3, GEN4 | C225 M6 | The <i>n</i> refers to an integer from 1 to 10. |
| Front NVME-<i>n</i> OptionROM | Enabled | Enabled, Disabled | C225 M6 | The <i>n</i> refers to an integer from 1 to 10. |
| PCIe Slot MSTOR Link Speed | Auto | Disabled, Auto, GEN1, GEN2, GEN3, GEN4 | C225 M6 | |

| Name | Default Value | M6 Server Supported Values | Platform | Dependencies |
|---------------------------------------|---------------|--|------------|--------------|
| PCIe Slot MSTOR RAID OptionROM | Enabled | Enabled, Disabled | C225 M6 | |
| Core Performance Boost | Auto | Disabled, Auto | C225 M6 | |
| Global C-state Control | Auto | Disabled, Enabled, Auto | C225 M6 | |
| L1 Stream HW Prefetcher | Auto | Disabled, Enabled, Auto | C225 M6 | |
| L2 Stream HW Prefetcher | Auto | Disabled, Enabled, Auto | C225 M6 | |
| NUMA Nodes per Socket | Auto | NPS0, NPS1, NPS2, NPS4, Auto | C225 M6 | |
| Memory Interleaving Size | Auto | 256 Bytes, 512 Bytes, 1 KB, 2 KB, 4 KB, Auto | C225 M6 | |
| Chipselect Interleaving | Auto | Disabled, Auto | C225 M6 | |
| Bank Group Swap | Auto | Enabled, Disabled, Auto | C225 M6 | |
| Determinism Slider | Auto | Power, Performance, Auto | C225 M6 | |
| IOMMU | Auto | Disabled, Enabled, Auto | C225 M6 | |
| SMT Mode | Enabled | Disabled, Enabled, Auto | C225 M6 | |
| SVM Mode | Enabled | Disabled, Enabled | C225 M6 | |
| Efficiency Mode Enable | Auto | Auto, Enabled | C225 M6 | |
| SNP Memory Coverage | Auto | Auto, Enabled, Disabled, Custom | C225 M6 | |
| SNP Memory Size to Cover in MB | 0 | 0-1048576 | C225 M6 | |
| CPPC | Auto | Auto, Enabled, Disabled | C225 M6 | |

| Name | Default Value | M6 Server Supported Values | Platform | Dependencies |
|--|---------------|---|------------|--------------|
| SEV-SNP Support | Disabled | Enabled, Disabled | C225 M6 | |
| SMEE | Auto | Auto, Enabled, Disabled | C225 M6 | |
| CPU Downcore control 7xx3 | Auto | Auto, ONE (1 + 0), TWO (2 + 0), THREE (3 + 0), FOUR (4 + 0), FIVE (5 + 0), SIX (6 + 0), SEVEN (7 + 0) | C225 M6 | |
| Downcore control 7xx2 | Auto | Auto, TWO (1 + 1), FOUR (2 + 2), SIX (3 + 3) | C225 M6 | |
| Fixed SOC P-State | Auto | P0, P1, P2, P3, Auto | C225 M6 | |
| APBDIS | Auto | 0, 1, Auto | C225 M6 | |
| CCD Control | Auto | Auto, 2 CCDs, 3 CCDs, 4 CCDs, 6 CCDs | C225 M6 | |
| Cisco xGMI Max Speed | Disabled | Disabled, Enabled | C225 M6 | |
| ACPI SRAT L3 Cache As NUMA Domain | Auto | Disabled, Enabled, Auto | C225 M6 | |
| Streaming Stores Control | Auto | Disabled, Enabled, Auto | C225 M6 | |
| DF C-States | Auto | Disabled, Enabled, Auto | C225 M6 | |
| Burst and Postponed Refresh | Disabled | Enabled, Disabled | C225 M6 | |
| SR-IOV Support | Enabled | Enabled, Disabled | C225 M6 | |
| PCIe ARI Support | Auto | Auto, Enabled, Disabled | C225 M6 | |
| TSME | Auto | Auto, Enabled, Disabled | C225 M6 | |
| BIOS Techlog Level | Minimum | Maximum, Normal, Minimum | C225 M6 | |
| OptionROM Launch Optimization | Enabled | Enabled, Disabled | C225 M6 | |

| Name | Default Value | M6 Server Supported Values | Platform | Dependencies |
|---------------------------------------|---------------|---|------------|--|
| Above 4GB Decoding | Enabled | Enabled, Disabled | C225 M6 | |
| SMEE | Enabled | Enabled, Disabled | C225 M6 | |
| SMT Mode | Off | Auto, Off | C225 M6 | |
| SR-IOV Support | Enabled | Enabled, Disabled | C225 M6 | |
| SVM Mode | Enabled | Enabled, Disabled | C225 M6 | |
| Terminal type | VT 100 | PC-ANSI,VT100, VT100-PLUS, VT-UTF8 | C225 M6 | |
| SHA-1 PCR Bank | Enabled | Enabled, Disabled | C225 M6 | |
| SHA256 PCR Bank | Enabled | Enabled, Disabled | C245 M6 | |
| FRB 2 Timer | Enabled | Enabled, Disabled | C225 M6 | |
| OS Boot Watchdog Timer | Enabled | Enabled, Disabled | C225 M6 | |
| OS Boot Watchdog Timer Policy | Power Off | Power Off, Reset | C225 M6 | |
| OS Boot Watchdog Timer Timeout | 10 minutes | 5 minutes, 10 minutes, 15 minutes, 20 minutes | C225 M6 | |
| Flow Control | None | None, RTS-CTS | C225 M6 | |
| Baud rate | 115.2k | 9.6k, 9.2k, 38.4k, 57.6k, 115.2k | C225 M6 | |
| Terminal type | VT100 | PC-ANSI, VT100, VT100-PLUS, VT-UTF8 | C225 M6 | Applicable only when Console Redirection COM 0 |
| Console redirection | Disabled | Disabled, COM0, COM1 or serial-port-b | C225 M6 | |

Server BIOS Tokens in Release 4.2(1i)

Cisco UCS Manager introduces support for the following servers in 4.2(1i):

- C245 M6

Cisco UCS Manager continues to support the following servers in 4.2(1i):

- C220 M6
- C240 M6
- B200 M6

For Cisco UCS C-series and B-series BIOS tokens supported on M4 and M5 servers, refer [Cisco UCS Server BIOS Tokens, Release 4.1](#).

BIOS Tokens for C245 M6 in 4.2(1i)

| Name | Default Value | M6 Server Supported Values | Platform | Dependencies |
|---------------------------------------|---------------|--|----------|--|
| MLOM Link Speed | Auto | Disabled, Auto, GEN1, GEN2, GEN3, GEN4 | C245 M6 | |
| MLOM OptionROM | Enabled | Disabled, Enabled | C245 M6 | |
| PCIe Slot <i>n</i> Link Speed | Auto | Disabled, Auto, GEN1, GEN2, GEN3, GEN4 | C245 M6 | The <i>n</i> refers to an integer from 1 to 8. |
| PCIe Slot <i>n</i> OptionROM | Enabled | Enabled, Disabled | C245 M6 | The <i>n</i> refers to an integer from 1 to 8. |
| MRAID<i>n</i> Link Speed | Auto | Disabled, Auto, GEN1, GEN2, GEN3, GEN4 | C245 M6 | The <i>n</i> refers to an integer 1 or 2. |
| MRAID<i>n</i> OptionROM | Enabled | Disabled, Enabled | C245 M6 | The <i>n</i> refers to an integer 1 or 2. |
| Front NVME <i>n</i> Link Speed | Auto | Disabled, Auto, GEN1, GEN2, GEN3, GEN4 | C245 M6 | The <i>n</i> refers to an integer from 1 to 4. |
| Front NVME-<i>n</i> OptionROM | Enabled | Enabled, Disabled | C245 M6 | The <i>n</i> refers to an integer from 1 to 4. |

| Name | Default Value | M6 Server Supported Values | Platform | Dependencies |
|--------------------------------|---------------|--|------------|--|
| Rear NVME <i>n</i> Link Speed | Auto | Disabled, Auto, GEN1, GEN2, GEN3, GEN4 | C245 M6 | The <i>n</i> refers to an integer from 1 to 4. |
| Rear NVME <i>n</i> OptionROM | Enabled | Enabled, Disabled | C245 M6 | The <i>n</i> refers to an integer from 1 to 4. |
| PCIe Slot MSTOR Link Speed | Auto | Disabled, Auto, GEN1, GEN2, GEN3, GEN4 | C245 M6 | |
| PCIe Slot MSTOR RAID OptionROM | Enabled | Enabled, Disabled | C245 M6 | |
| FRB 2 Timer | Enabled | Enabled, Disabled | C245 M6 | |
| OS Boot Watchdog Timer Policy | Power Off | Power Off, Reset | C245 M6 | |
| Flow Control | None | None, RTS-CTS | C245 M6 | |
| Baud rate | 115.2k | 9.6k, 9.2k, 38.4k, 57.6k, 115.2k | C245 M6 | |
| Terminal type | VT100 | PC-ANSI, VT100, VT100-PLUS, VT-UTF8 | C245 M6 | Applicable only when Console Redirection COM 0 |
| Console redirection | Disabled | COM 0, COM 1, Disabled | C245 M6 | Applicable only when Console Redirection COM 0 |
| Trusted Platform Module State | Enabled | Enabled, Disabled | C245 M6 | |
| SHA-1 PCR Bank | Enabled | Enabled, Disabled | C245 M6 | |
| SHA256 PCR Bank | Enabled | Enabled, Disabled | C245 M6 | |
| Post Package Repair | Hard PPR | Disabled, Hard PPR | C245 M6 | |

| Name | Default Value | M6 Server Supported Values | Platform | Dependencies |
|--------------------------------------|---------------|--|------------|--------------|
| Above 4G Decoding | Enabled | Enabled, Disabled | C245 M6 | |
| CDN Control | Enabled | Enabled, Disabled | C245 M6 | |
| OptionROM Launch Optimization | Enabled | Enabled, Disabled | C245 M6 | |
| BIOS Techlog Level | Minimum | Maximum, Normal, Minimum | C245 M6 | |
| Power ON Password | Disabled | Enabled, Disabled | C245 M6 | |
| IPv6 PXE Support | Disabled | Enabled, Disabled | C245 M6 | |
| BME DMA Mitigation | Disabled | Enabled, Disabled | C245 M6 | |
| Network Stack | Enabled | Enabled, Disabled | C245 M6 | |
| IPv4 PXE Support | Enabled | Enabled, Disabled | C245 M6 | |
| IPv4 HTTP Support | Enabled | Enabled, Disabled | C245 M6 | |
| IPv6 HTTP Support | Enabled | Enabled, Disabled | C245 M6 | |
| Core Performance Boost | Auto | Disabled, Auto | C245 M6 | |
| Global C-state Control | Auto | Disabled, Enabled, Auto | C245 M6 | |
| L1 Stream HW Prefetcher | Auto | Disabled, Enabled, Auto | C245 M6 | |
| L2 Stream HW Prefetcher | Auto | Disabled, Enabled, Auto | C245 M6 | |
| NUMA Nodes per Socket | Auto | NPS0, NPS1, NPS2, NPS4, Auto | C245 M6 | |
| Memory Interleaving Size | Auto | 256 Bytes, 512 Bytes, 1 KB, 2 KB, 4 KB, Auto | C245 M6 | |

| Name | Default Value | M6 Server Supported Values | Platform | Dependencies |
|--------------------------------|---------------|---|------------|--------------|
| Chipselect Interleaving | Auto | Disabled, Auto | C245 M6 | |
| Bank Group Swap | Auto | Enabled, Disabled, Auto | C245 M6 | |
| Determinism Slider | Auto | Power, Performance, Auto | C245 M6 | |
| IOMMU | Auto | Disabled, Enabled, Auto | C245 M6 | |
| SMT Mode | Enabled | Disabled, Enabled, Auto | C245 M6 | |
| SVM Mode | Enabled | Disabled, Enabled | C245 M6 | |
| Efficiency Mode Enable | Auto | Auto, Enabled | C245 M6 | |
| SNP Memory Coverage | Auto | Auto, Enabled, Disabled, Custom | C245 M6 | |
| SNP Memory Size to Cover in MB | 0 | 0-1048576 | C245 M6 | |
| CPPC | Auto | Auto, Enabled, Disabled | C245 M6 | |
| SEV-SNP Support | Disabled | Enabled, Disabled | C245 M6 | |
| SMEE | Auto | Auto, Enabled, Disabled | C245 M6 | |
| CPU Downcore control 7xx3 | Auto | Auto, ONE (1 + 0), TWO (2 + 0), THREE (3 + 0), FOUR (4 + 0), FIVE (5 + 0), SIX (6 + 0), SEVEN (7 + 0) | C245 M6 | |
| Fixed SOC P-State | Auto | P0, P1, P2, P3, Auto | C245 M6 | |
| APBDIS | Auto | 0, 1, Auto | C245 M6 | |
| CCD Control | Auto | Auto, 2 CCDs, 3 CCDs, 4 CCDs, 6 CCDs | C245 M6 | |
| Cisco xGMI Max Speed | Disabled | Disabled, Enabled | C245 M6 | |

| Name | Default Value | M6 Server Supported Values | Platform | Dependencies |
|--|----------------------|------------------------------------|-----------------|---------------------|
| ACPI SRAT L3 Cache As NUMA Domain | Auto | Disabled, Enabled, Auto | C245 M6 | |
| Streaming Stores Control | Auto | Disabled, Enabled, Auto | C245 M6 | |
| DF C-States | Auto | Disabled, Enabled, Auto | C245 M6 | |
| Post Package Repair | Hard PPR | Disabled, Hard PPR | C245 M6 | |
| Burst and Postponed Refresh | Disabled | Enabled, Disabled | C245 M6 | |
| SR-IOV Support | Enabled | Enabled, Disabled | C245 M6 | |
| PCIe ARI Support | Auto | Auto, Enabled, Disabled | C245 M6 | |
| TSME | Auto | Auto, Enabled, Disabled | C245 M6 | |
| BIOS Techlog Level | Minimum | Maximum, Normal, Minimum | C245 M6 | |
| OptionROM Launch Optimization | Enabled | Enabled, Disabled | C245 M6 | |
| Above 4GB Decoding | Enabled | Enabled, Disabled | C245 M6 | |
| SMEE | Enabled | Enabled, Disabled | C245 M6 | |
| SMT Mode | Off | Auto, Off | C245 M6 | |
| SR-IOV Support | Enabled | Enabled, Disabled | C245 M6 | |
| SVM Mode | Enabled | Enabled, Disabled | C245 M6 | |
| Terminal type | VT 100 | PC-ANSI,VT100, VT100-PLUS, VT-UTF8 | C245 M6 | |
| OS Boot Watchdog Timer | Enabled | Enabled, Disabled | C245 M6 | |

| Name | Default Value | M6 Server Supported Values | Platform | Dependencies |
|---------------------------------------|---------------|---|----------|--------------|
| OS Boot Watchdog Timer Timeout | 10 minutes | 5 minutes, 10 minutes, 15 minutes, 20 minutes | C245 M6 | |

Server BIOS Tokens in Release 4.2(1f)

Cisco UCS Manager supports the following servers in 4.2(1f) release:

- C220 M6
- C240 M6
- B200 M6

The following table lists the new and updated BIOS tokens for 4.2(1f) release.

Table 1: New and Updated BIOS Tokens 4.2(1f)

| Name | Default Value | Server Supported Values | Platform | New/Changed |
|-----------------------------------|---------------|-------------------------|-------------------------------|-------------|
| Enhanced CPU Performance | Disabled | Disabled, Auto | C220 M6, C240 M6, and B200 M6 | New |
| UPI Link Enablement | Auto | Auto, 1, 2 | C220 M6, C240 M6, and B200 M6 | New |
| Virtual Numa | Disabled | Enabled, Disabled | C220 M6, C240 M6, and B200 M6 | New |
| LLC Dead Line | Enabled | Auto, Enabled, Disabled | C220 M6, C240 M6, and B200 M6 | New |
| C1 Auto Demotion | Enabled | Enabled, Disabled | C220 M6, C240 M6, and B200 M6 | New |
| C1 Auto UnDemotion | Enabled | Enabled, Disabled | C220 M6, C240 M6, and B200 M6 | New |
| XPT Remote Prefetch | Auto | Auto, Enabled, Disabled | C220 M6, C240 M6, and B200 M6 | New |
| UPI Power Management | Disabled | Disabled, Enabled | C220 M6, C240 M6, and B200 M6 | New |
| SHA-1 PCR Bank | Enabled | Disabled, Enabled | C220 M6, C240 M6, and B200 M6 | New |
| SHA256 PCR Bank | Enabled | Disabled, Enabled | C220 M6, C240 M6, and B200 M6 | New |

| Name | Default Value | Server Supported Values | Platform | New/Changed |
|---|---------------|---------------------------------------|-------------------------------|-------------|
| FRB 2 Timer | Enabled | Enabled, Disabled | C220 M6, C240 M6, and B200 M6 | New |
| OS Boot Watchdog Timer Policy | Power Off | Power Off, Reset | C220 M6, C240 M6, and B200 M6 | New |
| OS Boot Watchdog Timer | Enabled | Enabled, Disabled | C220 M6, C240 M6, and B200 M6 | New |
| Flow Control | None | None, RTS-CTS | C220 M6, C240 M6, and B200 M6 | New |
| Legacy USB Support | Enabled | Enabled, Disabled, Auto | C220 M6, C240 M6, and B200 M6 | New |
| Baud rate | 115.2k | 9.6k, 9.2k, 38.4k, 57.6k, 115.2k | C220 M6, C240 M6, and B200 M6 | New |
| Terminal type | VT100 | PC-ANSI, VT100, VT100-PLUS, VT-UTF8 | C220 M6, C240 M6, and B200 M6 | New |
| Console redirection | Disabled | Disabled, COM0, COM1 or serial-port-b | C220 M6, C240 M6, and B200 M6 | New |
| Trusted Platform Module Support | Enabled | Enabled, Disabled | C220 M6, C240 M6, and B200 M6 | New |
| TPM Pending operation | None | None, TpmClear | C220 M6, C240 M6, and B200 M6 | New |
| Intel VT for directed IO | Enabled | Enabled, Disabled | C220 M6, C240 M6, and B200 M6 | New |
| Intel VTD coherency support | Disabled | Enabled, Disabled | C220 M6, C240 M6, and B200 M6 | New |
| Intel Trusted Execution Technology Support | Disabled | Enabled, Disabled | C220 M6, C240 M6, and B200 M6 | New |

| Name | Default Value | Server Supported Values | Platform | New/Changed |
|--|---------------|--|-------------------------------|-------------|
| Intel Virtualization Technology | Enabled | Enabled, Disabled | C220 M6, C240 M6, and B200 M6 | New |
| MLOM OptionROM | Enabled | Disabled, Enabled | C220 M6, C240 M6, and B200 M6 | New |
| OS Boot Watchdog Timer Timeout | 10 minutes | 5 minutes, 10 minutes, 15 minutes, 20 minutes | C220 M6, C240 M6, and B200 M6 | New |
| Select Memory RAS Configuration | ADDDC Sparing | Maximum performance, Mirror-mode-1lm, ADDDC Sparing, Partial mirror-mode-1lm | C220 M6, C240 M6, and B200 M6 | New |
| Turbo Mode | Enabled | Enabled, Disabled | C220 M6, C240 M6, and B200 M6 | New |
| EIST PSD Function | HW all | HW all, SW all | C220 M6, C240 M6, and B200 M6 | New |
| Uncore Frequency Scaling | Enabled | Enabled, Disabled | C220 M6, C240 M6, and B200 M6 | New |
| SpeedStep (Pstates) | Enabled | Enabled, Disabled | C220 M6, C240 M6, and B200 M6 | New |
| LIMIT CPU PA to 46 Bits | Enabled | Enabled, Disabled | C220 M6, C240 M6, and B200 M6 | Changed |
| Virtual NUMA | Disabled | Enabled, Disabled, Auto | C220 M6, C240 M6, and B200 M6 | Changed |
| LLC Dead Line | Enabled | Enabled, Disabled, Auto | C220 M6, C240 M6, and B200 M6 | Changed |
| XPT Remote Prefetch | Auto | Enabled, Disabled, Auto | C220 M6, C240 M6, and B200 M6 | Changed |
| Slot 9 State | Disabled | Enabled, Disabled, UEFI Only, Legacy Only | C220 M6, C240 M6, and B200 M6 | Changed |

Server BIOS Tokens in Release 4.2(1d)

Cisco UCS Manager introduces support for the following servers in 4.2(1d):

- C220 M6—[BIOS Tokens for C220 M6 and C240 M6 in 4.2\(1d\), on page 15](#)
- C240 M6—[BIOS Tokens for C220 M6 and C240 M6 in 4.2\(1d\), on page 15](#)
- B200 M6—[BIOS Tokens for B200 M6 in 4.2\(1d\), on page 19](#)

Cisco UCS Manager continues to support the following servers in 4.2(1d):

- B200 M5
- B480 M5
- C220 M5
- C240 M5
- C240 SD M5
- C480 M5
- S3260 M5
- C125 M5
- C480 M5 ML
- C220 M4
- C240 M4
- C460 M4
- S3260 M4

For Cisco UCS C-series and B-series BIOS tokens supported on M4 and M5 servers, refer [Cisco UCS Server BIOS Tokens, Release 4.1](#). In addition, refer the following [New and Changed BIOS Tokens for M5 servers in 4.2\(1d\), on page 24](#) for updated M5 server support.

BIOS Tokens for C220 M6 and C240 M6 in 4.2(1d)

| Name | Default Value | Server Supported Values | Platform | Dependencies |
|-----------------------|---------------|-------------------------|---------------------|--------------|
| Core Multi Processing | All | All, 1 to 48 | C220 M6 and C240 M6 | |

| Name | Default Value | Server Supported Values | Platform | Dependencies |
|--|---------------------------------------|---|---------------------|--------------|
| CR QoS | Mode 0 - Disable the PMem QoS Feature | Recipe 1, Recipe 2, Recipe 3, Disabled, Mode 0 - Disable the PMem QoS Feature, Mode 1 - M2M QoS Enable ;CHA QoS Disable, Mode 2 - M2M QoS Enable;CHA QoS Enable | C220 M6 and C240 M6 | |
| IIO eDPC Support | OnFatal and Non-Fatal Errors | On Fatal Error, Disabled, OnFatal and Non-Fatal Errors | C220 M6 and C240 M6 | |
| Multikey Total Memory Encryption (MK-TME) | Disabled | Enabled, Disabled | C220 M6 and C240 M6 | |
| SW Guard Extensions (SGX) | Disabled | Enabled, Disabled | C220 M6 and C240 M6 | |
| Total Memory Encryption (TME) | Disabled | Enabled, Disabled | C220 M6 and C240 M6 | |
| Select Owner EPOCH input type | Manual User Defined Owner EPOCHs | SGX Owner EPOCH activated, Change to New Random Owner EPOCHs, Manual User Defined Owner EPOCHs | C220 M6 and C240 M6 | |
| UPI Prefetch | Auto | Auto, Enabled, Disabled | C220 M6 and C240 M6 | |
| Partial Cache Line Sparing | Enabled | Enabled, Disabled | C220 M6 and C240 M6 | |

| Name | Default Value | Server Supported Values | Platform | Dependencies |
|--------------------------------|---------------|---|---------------------|--------------|
| Select PPR type configuration | Hard PPR | Hard PPR, Soft PPR, Disabled | C220 M6 and C240 M6 | |
| SGX Auto MP Registration Agent | Disabled | Enabled, Disabled | C220 M6 and C240 M6 | |
| SProcessor Epoch n | 0 | n | C220 M6 and C240 M6 | |
| SGX Factory Reset | Disabled | Enabled, Disabled | C220 M6 and C240 M6 | |
| SGX PUBKEY HASH n | 0 | SGX PUBKEY HASH0-Between 7-0, SGX PUBKEY HASH1-Between 15-8, SGX PUBKEY HASH2-Between 23-16, SGX PUBKEY HASH3-Between 31-24 | C220 M6 and C240 M6 | |
| SGX Write Enable | Enabled | Enabled, Disabled | C220 M6 and C240 M6 | |
| SGX Pkg info In-Band Access | Disabled | Enabled, Disabled | C220 M6 and C240 M6 | |
| SGX QoS | Enabled | Enabled, Disabled | C220 M6 and C240 M6 | |
| Enhanced Memory Test | Auto | Auto, Disabled, Enabled | C220 M6 and C240 M6 | |
| Intel Dynamic Speed Select | Disabled | Enabled, Disabled | C220 M6 and C240 M6 | |
| Intel Speed Select | Base | Base, Config 1, Config 2, Config 3, Config 4 | C220 M6 and C240 M6 | |

| Name | Default Value | Server Supported Values | Platform | Dependencies |
|--|------------------------|---|---|---|
| UPI Link Frequency Select | Auto | 9.6GT/s, 10.4GT/s, 11.2GT/s, Auto, Use Per Link Setting | C220 M6 and C240 M6 | |
| UMA Clustering | Hemisphere(2-clusters) | Hemisphere(2-clusters), Disable(All-2-All) | C220 M6 and C240 M6 | |
| MLOM Link Speed | Auto | Auto, Disabled, Enabled, GEN1,GEN2, GEN3, GEN4 | C220 M6 and C240 M6 | |
| PCIe Slot MSTOR-RAID Link Speed | Auto | Auto, Disabled, Enabled, GEN1,GEN2, GEN3, GEN4 | C220 M6 and C240 M6 | |
| MRAID Link Speed | Auto | Auto, Disabled, Enabled, GEN1, GEN2, GEN3,GEN4 | C220 M6 | |
| MRAID-<i>n</i> Link Speed | Auto | Auto, Disabled, Enabled, GEN1,GEN2, GEN3, GEN4 | C240 M6 | The <i>n</i> refers to an integer from 1 to 2. |
| MRAID-<i>n</i> OptionROM | Enabled | Enabled, Disabled | C240 M6 | The <i>n</i> refers to an integer from 1 to 2. |
| Front Nvme-<i>n</i> OptionROM | Enabled | Disabled, Enabled | For <i>n</i> ranging from 1 to 10 supports C220 M6 and C240 M6 <i>n</i> ranging 11 and 24 supports C240 M6 | |
| Front NVME-<i>n</i> Link Speed | Auto | Auto, Disabled, Enabled, GEN1,GEN2, GEN3, GEN4 | For <i>n</i> ranging from 1 to 10 supports C220 M6 and C240 M6 <i>n</i> ranging 11 and 10 supports C240 M6 | The <i>n</i> refers to an integer from 1 to 12. |
| PCIe Slot <i>n</i> Link Speed | Auto | Auto, Disabled, GEN1,GEN2, GEN3, GEN4 | C240 M6 | The <i>n</i> refers to an integer from 4 to 8. |

| Name | Default Value | Server Supported Values | Platform | Dependencies |
|-------------------------------------|---------------|--|---------------------|--|
| PCIe Slot <i>n</i> OptionROM | Enabled | Enabled, Disabled | C240 M6 | The <i>n</i> refers to an integer from 4 to 8. |
| Rear NVME<i>n</i> Link Speed | Auto | Auto, Disabled, Enabled, GEN1, GEN2, GEN3, GEN4 | C240 M6 | The <i>n</i> refers to an integer from 1 to 4. |
| Rear NVME<i>n</i> Option ROM | Auto | Auto, Disabled, Enabled, GEN1, GEN2, GEN3, GEN4 | C240 M6 | The <i>n</i> refers to an integer from 1 to 4. |
| eADR Support | Disabled | Auto, Enabled, Disabled | C220 M6 and C240 M6 | |
| Volatile Memory Mode | 2LM | 2LM, 1LM | C220 M6 and C240 M6 | |
| Memory Bandwidth Boost | Enabled | Enabled, Disabled | C220 M6 and C240 M6 | |
| CR FastGo Config | Auto | Auto, Default, Option 1, Option 2, Option 3, Option 4, Option 5, Enable Optimization, Disable Optimization | C220 M6 and C240 M6 | |
| Memory Refresh Rate | 2x Refresh | 1x Refresh, 2x Refresh | C220 M6 and C240 M6 | |
| Console redirection | Disabled | Disabled, COM0, COM1 or serial-port-b | C220 M6 and C240 M6 | |

BIOS Tokens for B200 M6 in 4.2(1d)

| Name | Default Value | Server Supported Values | Platform | Dependencies |
|------------------------------|---------------|-------------------------|----------|--------------|
| Core Multi Processing | All | All, 1 to 48 | B200 M6 | |

| Name | Default Value | Server Supported Values | Platform | Dependencies |
|--|---------------------------------------|---|----------|--------------|
| CR QoS | Mode 0 - Disable the PMem QoS Feature | Recipe 1, Recipe 2, Recipe 3, Disabled, Mode 0 - Disable the PMem QoS Feature, Mode 1 - M2M QoS Enable ;CHA QoS Disable, Mode 2 - M2M QoS Enable;CHA QoS Enable | B200 M6 | |
| IIO eDPC Support | OnFatal and Non-Fatal Errors | On Fatal Error, Disabled, OnFatal and Non-Fatal Errors | B200 M6 | |
| Multikey Total Memory Encryption (MK-TME) | Disabled | Enabled, Disabled | B200 M6 | |
| SW Guard Extensions (SGX) | Disabled | Enabled, Disabled | B200 M6 | |
| Total Memory Encryption (TME) | Disabled | Enabled, Disabled | B200 M6 | |
| Select Owner EPOCH input type | Manual User Defined Owner EPOCHs | SGX Owner EPOCH activated, Change to New Random Owner EPOCHs, Manual User Defined Owner EPOCHs | B200 M6 | |
| UPI Prefetch | Auto | Auto, Enabled, Disabled | B200 M6 | |
| Partial Cache Line Sparing | Enabled | Enabled, Disabled | B200 M6 | |

| Name | Default Value | Server Supported Values | Platform | Dependencies |
|--------------------------------|---------------|---|----------|--------------|
| Select PPR type configuration | Hard PPR | Hard PPR, Soft PPR, Disabled | B200 M6 | |
| SGX Auto MP Registration Agent | Disabled | Enabled, Disabled | B200 M6 | |
| SProcessor Epoch n | 0 | n | B200 M6 | |
| SGX Factory Reset | Disabled | Enabled, Disabled | B200 M6 | |
| SGX PUBKEY HASH n | 0 | SGX PUBKEY HASH0-Between 7-0, SGX PUBKEY HASH1-Between 15-8, SGX PUBKEY HASH2-Between 23-16, SGX PUBKEY HASH3-Between 31-24 | B200 M6 | |
| SGX Write Enable | Enabled | Enabled, Disabled | B200 M6 | |
| SGX Pkg info In-Band Access | Disabled | Enabled, Disabled | B200 M6 | |
| SGX QoS | Enabled | Enabled, Disabled | B200 M6 | |
| Enhanced Memory Test | Auto | Auto, Disabled, Enabled | B200 M6 | |
| Intel Dynamic Speed Select | Disabled | Enabled, Disabled | B200 M6 | |
| Intel Speed Select | Base | Base, Config 1, Config 2, Config 3, Config 4 | B200 M6 | |

| Name | Default Value | Server Supported Values | Platform | Dependencies |
|----------------------------------|------------------------|---|----------|--------------|
| UPI Link Frequency Select | Auto | 9.6GT/s, 10.4GT/s, 11.2GT/s, Auto, Use Per Link Setting | B200 M6 | |
| UMA Clustering | Hemisphere(2-clusters) | Hemisphere(2-clusters), Disable(All-2-All) | B200 M6 | |
| eADR Support | Disabled | Auto, Enabled, Disabled | B200 M6 | |
| Volatile Memory Mode | 2LM | 2LM, 1LM | B200 M6 | |
| Memory Bandwidth Boost | Enabled | Enabled, Disabled | B200 M6 | |
| CR FastGo Config | Auto | Auto, Default, Option 1, Option 2, Option 3, Option 4, Option 5, Enable Optimization, Disable Optimization | B200 M6 | |
| Memory Refresh Rate | 2x Refresh | 1x Refresh, 2x Refresh | B200 M6 | |
| Console redirection | Disabled | Disabled, COM0, COM1 or serial-port-b | B200 M6 | |
| Terminal type | VT100 | PC-ANSI, VT100, VT100-PLUS, VT-UTF8 | B200 M6 | |
| TPM Support | Enabled | Enabled, Disabled | B200 M6 | |
| TPM Pending operation | None | None, TpmClear | B200 M6 | |
| SHA-1 PCR Bank | Enabled | Enabled, Disabled | B200 M6 | |

| Name | Default Value | Server Supported Values | Platform | Dependencies |
|---|---------------|---|----------|--------------|
| SHA256 PCR Bank | Enabled | Enabled, Disabled | B200 M6 | |
| Flow Control | None | None, RTS-CTS | B200 M6 | |
| Baud rate | 115.2k | 9.6k, 9.2k, 38.4k, 57.6k, 115.2k | B200 M6 | |
| OS Boot Watchdog Timer | Enabled | Enabled, Disabled | B200 M6 | |
| OS Boot Watchdog Timer Timeout | 10 minutes | 5 minutes, 10 minutes, 15 minutes, 20 minutes | B200 M6 | |
| OS Boot Watchdog Timer Policy | Power Off | Power Off, Reset | B200 M6 | |
| Intel VT for directed IO | Enabled | Enabled, Disabled | B200 M6 | |
| Intel VTD coherency support | Disabled | Enabled, Disabled | B200 M6 | |
| Intel Trusted Execution Technology Support | Disabled | Enabled, Disabled | B200 M6 | |
| Intel Virtualization Technology | Enabled | Enabled, Disabled | B200 M6 | |
| Legacy USB Support | Enabled | Enabled, Disabled, Auto | B200 M6 | |

New and Changed BIOS Tokens for M5 servers in 4.2(1d)

| Name | Default Value | Server Supported Values | Platform | Dependencies | New/Changed |
|---|---------------|---|--|--------------|-------------|
| MRAID Link Speed | Auto | Auto, Disabled, Enabled, GEN1, GEN2, GEN3, GEN4 | C220 M5 and C240 M5 | | Changed |
| RAID-<i>n</i> Link Speed | Auto | Auto, Disabled, Enabled, GEN1, GEN2, GEN3, GEN4 | C480 M5 | | Changed |
| PCIe Slot MRAID-<i>n</i> OptionROM | Enabled | Enabled, Disabled | C220 M5 and C240 M5 | | Changed |
| Front NVME_{<i>n</i>} Link Speed | Auto | Auto, Disabled, Enabled, GEN1, GEN2, GEN3, GEN4 | C220 M5 and C240 M5 | | Changed |
| PCIe Slot <i>n</i> Link Speed | Auto | Auto, Disabled, GEN1, GEN2, GEN3, GEN4 | C220 M5, C240 M5, C480 M5, and C125 M5 | | Changed |
| Rear NVME_{<i>n</i>} Link Speed | Auto | Auto, Disabled, Enabled, GEN1, GEN2, GEN3, GEN4 | C240 M5 | | Changed |
| Select Memory RAS Configuration | ADDDC Sparing | Maximum, Mirror-mode-1lm, ADDDC Sparing, Patch-mode-1lm | C240 M5 | | Changed |
| Turbo Mode | Enabled | Enabled, Disabled | C240 M5 | | Changed |
| EIST PSD Function | HW all | HW all, SW all | C240 M5 | | Changed |

| Name | Default Value | Server Supported Values | Platform | Dependencies | New/Changed |
|---------------------------------|----------------------|--------------------------------|-----------------|---------------------|--------------------|
| Uncore Frequency Scaling | Enabled | Enabled, Disabled | C240 M5 | | Changed |
| SpeedStep (Pstates) | Enabled | Enabled, Disabled | C240 M5 | | Changed |

