UCS Server BIOS Tokens

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(1l)

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

- C225 M6

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

- 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(1l)

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 *n* Link Speed	Auto	Disabled, Auto, GEN1, GEN2, GEN3, GEN4	C225 M6	The *n* refers to an integer from 1 to 3.
PCIe Slot *n* OptionROM	Enabled	Enabled, Disabled	C225 M6	The *n* 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 *n* Link Speed	Auto	Disabled, Auto, GEN1, GEN2, GEN3, GEN4	C225 M6	The *n* refers to an integer from 1 to 10.
Front NVME-*n* OptionROM	Enabled	Enabled, Disabled	C225 M6	The *n* 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 *n* Link Speed	Auto	Disabled, Auto, GEN1, GEN2, GEN3, GEN4	C245 M6	The *n* refers to an integer from 1 to 8.
PCIe Slot *n* OptionROM	Enabled	Enabled, Disabled	C245 M6	The *n* refers to an integer from 1 to 8.
MRAID*n* Link Speed	Auto	Disabled, Auto, GEN1, GEN2, GEN3, GEN4	C245 M6	The *n* refers to an integer 1 or 2.
MRAID*n* OptionROM	Enabled	Disabled, Enabled	C245 M6	The *n* refers to an integer 1 or 2.
Front NVME *n* Link Speed	Auto	Disabled, Auto, GEN1, GEN2, GEN3, GEN4	C245 M6	The *n* refers to an integer from 1 to 4.
Front NVME-*n* OptionROM	Enabled	Enabled, Disabled	C245 M6	The *n* refers to an integer from 1 to 4.

Name	Default Value	M6 Server Supported Values	Platform	Dependencies
Rear NVME *n* Link Speed	Auto	Disabled, Auto, GEN1, GEN2, GEN3, GEN4	C245 M6	The *n* refers to an integer from 1 to 4.
Rear NVME *n* OptionROM	Enabled	Enabled, Disabled	C245 M6	The *n* 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-*n* Link Speed	Auto	Auto, Disabled, Enabled, GEN1,GEN2, GEN3, GEN4	C240 M6	The *n* refers to an integer from 1 to 2.
MRAID-*n* OptionROM	Enabled	Enabled, Disabled	C240 M6	The *n* refers to an integer from 1 to 2.
Front Nvme-*n* OptionROM	Enabled	Disabled, Enabled	For *n*ranging from 1 to 10 supports C220 M6 and C240 M6 *n*ranging 11 and 24 supports C240 M6	
Front NVME*n* Link Speed	Auto	Auto, Disabled, Enabled, GEN1,GEN2, GEN3, GEN4	For *n*ranging from 1 to 10 supports C220 M6 and C240 M6 *n*ranging 11 and 10 supports C240 M6	The *n* refers to an integer from 1 to 12.
PCIe Slot *n* Link Speed	Auto	Auto, Disabled, GEN1,GEN2, GEN3, GEN4	C240 M6	The *n* refers to an integer from 4 to 8.

Name	Default Value	Server Supported Values	Platform	Dependencies
PCIe Slot *n* OptionROM	Enabled	Enabled, Disabled	C240 M6	The *n* refers to an integer from 4 to 8.
Rear NVME*n* Link Speed	Auto	Auto, Disabled, Enabled, GEN1,GEN2, GEN3, GEN4	C240 M6	The *n* refers to an integer from 1 to 4.
Rear NVME*n* Option ROM	Auto	Auto, Disabled, Enabled, GEN1,GEN2, GEN3, GEN4	C240 M6	The *n* 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-*n* Link Speed	Auto	Auto, Disabled, Enabled, GEN1,GEN2, GEN3, GEN4	C480 M5		Changed
PCIe Slot MRAID-*n* OptionROM	Enabled	Enabled, Disabled	C220 M5 and C240 M5		Changed
Front NVME*n* Link Speed	Auto	Auto, Disabled, Enabled, GEN1,GEN2, GEN3, GEN4	C220 M5 and C240 M5		Changed
PCIe Slot *n* Link Speed	Auto	Auto, Disabled, GEN1,GEN2, GEN3, GEN4	C220 M5, C240 M5, C480 M5, and C125 M5		Changed
Rear NVME*n* Link Speed	Auto	Auto, Disabled, Enabled, GEN1,GEN2, GEN3, GEN4	C240 M5		Changed
Select Memory RAS Configuration	ADDDC Sparing	Maximum performance, Mirror-mode-1lm, ADDDC Sparing, Partial-mirror-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