Cisco UCS Server BIOS Tokens, Release 4.3

First Published: 2023-04-13

Last Modified: 2023-02-15

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

Preface

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 *this font*.
TUI elements	In a Text-based User Interface, text the system displays appears in `this font`.
System output	Terminal sessions and information that the system displays appear in `this font`.
CLI commands	CLI command keywords appear in **this font**. Variables in a CLI command appear in *this font*.
[ ]	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

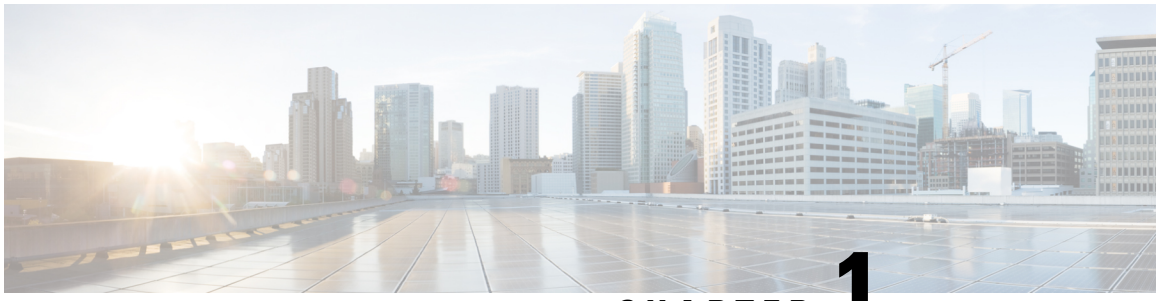
For a complete list of all B-Series documentation, see the *Cisco UCS B-Series Servers Documentation Roadmap* available at the following URL: https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/overview/guide/UCS_roadmap.html

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 4.3(3a)

Cisco UCS Manager continues to support the following servers in 4.3(3a):

- Cisco UCS X410c M7 Compute Node
- Cisco UCS X210c M7 Compute Node
- Cisco UCS X210c M6 Compute Node
- Cisco UCS C220 M7 Server
- Cisco UCS C240 M7 Server
- Cisco UCS C220 M6
- Cisco UCS C240 M6
- Cisco UCS C245 M6
- Cisco UCS C225 M6
- Cisco UCS B200 M6
- Cisco UCS B200 M5
- Cisco UCS B480 M5
- Cisco UCS C220 M5
- Cisco UCS C240 M5
- Cisco UCS C240 SD M5
- Cisco UCS C480 M5
- Cisco UCS C480 M5 ML
- Cisco UCS S3260 M5

- Cisco UCS C125 M5

Related Documentation

- For Cisco UCS C-series and B-series BIOS tokens supported on M7 servers, see Server BIOS Tokens in Release 4.3(2c) and Server BIOS Tokens in Release 4.3(2b).
- For Cisco UCS C-series and B-series BIOS tokens supported on M6 servers, see Cisco UCS Server BIOS Tokens, Release 4.2.
- For Cisco UCS C-series and B-series BIOS tokens supported on M5 servers, see Cisco UCS Server BIOS Tokens, Release 4.1.

New/Changed BIOS Tokens for 4.3(3a)

Name	Default Value	M7 Server Supported Values	Platform	New/Changed
Trust Domain Extension (TDX)	Disabled	Enabled, Disabled	X410c M7, X210c M7, C220 M7, C240 M7	New
TDX Secure Arbitration Mode (SEAM) Loader	Disabled	Enabled, Disabled	X410c M7, X210c M7, C220 M7, C240 M7	New
SHA384 PCR Bank	Disabled	Enabled, Disabled	X410c M7, X210c M7, C220 M7, C240 M7	New
QpiLinkSpeed	Auto	20.0GT/s,12.8GT/s, 14.4GT/s, 16.0GT/s, Auto	X410c M7, X210c M7, C220 M7, C240 M7	New
C1 Auto demotion	Auto	Auto, Enabled, Disabled	X410c M7, X210c M7, C220 M7, C240 M7	Changed
C1 Auto UnDemotion	Auto	Auto, Enabled, Disabled	X410c M7, X210c M7, C220 M7, C240 M7	Changed

Server BIOS Tokens in Release 4.3(2c)

Cisco UCS Manager introduces support for the following server in release 4.3(2c):

- Cisco UCS X410c M7 Compute Node

Cisco UCS Manager continues to support the following servers in 4.3(2c):

- Cisco UCS X210c M7 Compute Node
- Cisco UCS X210c M6 Compute Node
- Cisco UCS C220 M7 Server
- Cisco UCS C240 M7 Server

- Cisco UCS C220 M6
- Cisco UCS C240 M6
- Cisco UCS C245 M6
- Cisco UCS C225 M6
- Cisco UCS B200 M6
- Cisco UCS B200 M5
- Cisco UCS B480 M5
- Cisco UCS C220 M5
- Cisco UCS C240 M5
- Cisco UCS C240 SD M5
- Cisco UCS C480 M5
- Cisco UCS C480 M5 ML
- Cisco UCS S3260 M5
- Cisco UCS C125 M5

Related Documentation

- For Cisco UCS C-series and B-series BIOS tokens supported on M7 servers, see Server BIOS Tokens in Release 4.3(2b).
- For Cisco UCS C-series and B-series BIOS tokens supported on M6 servers, see Cisco UCS Server BIOS Tokens, Release 4.2.
- For Cisco UCS C-series and B-series BIOS tokens supported on M5 servers, see Cisco UCS Server BIOS Tokens, Release 4.1.

BIOS Tokens for X410c M7 in 4.3(2c)

Name	Default Value	M7 Server Supported Values	Platform	New/Changed
PRMRR Size	256M	Invalid Config, 128M, 256M, 512M,1G, 2G, 4G, 8G, 16G, 32G, 64G, 128G, 256G, 512G	X410c M7	Changed
Optimized Power Mode	Disable	Enabled, Disabled	X410c M7	Changed
Adaptive Refresh Management Level	Default	Default, Level A, Level B, Level C	X410c M7	Changed
Rank Margin Tool	Disabled	Enabled Disabled	X410c M7	Changed

Name	Default Value	M7 Server Supported Values	Platform	New/Changed
Error Check Scrub	Enabled without result collection	Disabled, Enabled without Result Collection, Enabled with Result Collection	X410c M7	Changed
PCIe PLL SSC Percent	255	0–20	X410c M7	Changed
Above 4G Decoding	Enabled	Enabled Disabled	X410c M7	Changed
VMD Enablement	Disabled	Enabled Disabled	X410c M7	Changed
PCIe RAS Support	Enabled	Enabled Disabled	X410c M7	Changed
CDN Support for LOM	Disabled	Enabled, Disabled	X410c M7	Changed
External SSC Enable	Off	0P3_Percent,P5_Percent, Hardware, Off	X410c M7	Changed
CDN Control	Enabled	Enabled, Disabled	X410c M7	Changed
Intel VT for directed IO	Enabled	Enabled, Disabled	X410c M7	Changed
Intel VTD Coherency Support	Disabled	Enabled, Disabled	X410c M7	Changed
USB Port Front	Enabled	Enabled, Disabled	X410c M7	Changed
USB Port KVM	Enabled	Enabled, Disabled	X410c M7	Changed
USB Port:M.2 Storage	Enabled	Enabled, Disabled	X410c M7	Changed
NTB Test Mode	Disabled	Enabled, Disabled	X410c M7	Changed
NTB Device Type	Upstream	Upstream, Downstream	X410c M7	Changed
C1 Auto demotion	Enabled	Enabled, Disabled	X410c M7	Changed
C1 Auto Demotion	Enabled	Enabled, Disabled	X410c M7	Changed

Name	Default Value	M7 Server Supported Values	Platform	New/Changed
FRB 2 Timer	Enabled	Enabled, Disabled	X410c M7	Changed
OS Watchdog Timer Policy	Power Off	Reset, Power Off	X410c M7	Changed
OS Watchdog Timer Timeout	10 minutes	5 minutes, 10 minutes, 15 minutes, 20 minutes	X410c M7	Changed
OS Watchdog timer	Disabled	Enabled, Disabled	X410c M7	Changed
Flow Control	None	None, RTS-CTS	X410c M7	Changed
Baud Rate	115.2k	9.6k, 19.2k,38.4k, 57.6k, 115.2k	X410c M7	Changed
Terminal Type	VT100	PC-ANSI, VT100, VT100-PLUS, VT-UTF8	X410c M7	Changed
Console Redirection	VT100	PC-ANSI, VT100, VT100-PLUS, VT-UTF8	X410c M7	Changed
Adaptive Memory Training	Enabled	Enabled, Disabled	X410c M7	Changed
OptionROM Launch Optimization	Enabled	Enabled, Disabled	X410c M7	Changed
BIOS Techlog level	Minimum	Maximum, Minimum, Normal	X410c M7	Changed
IPV6 PXE support	Enabled	Enabled, Disabled	X410c M7	Changed
Network stack	Enabled	Enabled, Disabled	X410c M7	Changed
IPv4 PXE Support	Enabled	Enabled, Disabled	X410c M7	Changed
IPv4 HTTP Support	Enabled	Enabled, Disabled	X410c M7	Changed
IPv6 HTTP Support	Enabled	Enabled, Disabled	X410c M7	Changed
Security Device Support	Enabled	Enabled, Disabled	X410c M7	Changed
Trusted Platform Module State	Enabled	Enabled, Disabled	X410c M7	Changed

Name	Default Value	M7 Server Supported Values	Platform	New/Changed
SHA-1 PCR Bank	Enabled	Enabled, Disabled	X410c M7	Changed
SHA256 PCR Bank	Enabled	Enabled, Disabled	X410c M7	Changed
TPM Pending Operation	None	None, TpmClear	X410c M7	Changed
TPM Minimal Physical Presence	Disabled	Enabled, Disabled	X410c M7	Changed
Intel Trusted Execution Technology Support	Enabled	Enabled, Disabled	X410c M7	Changed
Total Memory Encryption (TME)	Disabled	Enabled, Disabled	X410c M7	Changed
SGX QoS	Enabled	Enabled, Disabled	X410c M7	Changed
SGX write Enable	Enabled	Enabled, Disabled	X410c M7	Changed
DMA Control Opt-In Flag	Disabled	Enabled, Disabled	X410c M7	Changed
Multikey Total Memory Encryption	Disabled	Enabled, Disabled	X410c M7	Changed
SW Guard Extensions (SGX)	Disabled	Enabled, Disabled	X410c M7	Changed
SGX Factory Reset	Disabled	Enabled, Disabled	X410c M7	Changed
SGX Pkg info In-Band Access	Disabled	Enabled, Disabled	X410c M7	Changed
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	X410c M7	Changed
SGX Auto MP Registration Agent	Disabled	Enabled, Disabled	X410c M7	Changed
SProcessor Epoch 0	0	Between 7-0	X410c M7	Changed
Pubkey Hash 0	0	Between 7-0	X410c M7	Changed

Name	Default Value	M7 Server Supported Values	Platform	New/Changed
SGX Pubkey Hash 1	0	Between 15-8	X410c M7	Changed
NUMA	Disabled	Enabled, Disabled	X410c M7	Changed
Select Memory RAS Configuration	ADDDC Sparing	Mirror Mode 1LM, Partial Mirror mode 1LM, Maximum Performance, ADDDC Sparing	X410c M7	Changed
Select PPR type	Hard PPR	Disabled, Hard PPR	X410c M7	Changed
Partial Cache Line Sparing	Disabled	Enabled, Disabled	X410c M7	Changed
BME DMA Mitigation	Disabled	Enabled, Disabled	X410c M7	Changed
Partial Memory Mirror Mode	Disabled	Percentage, Value in GB, Disabled	X410c M7	Changed
Partial Mirror Percentage	0	Between 0-50	X410c M7	Changed
Intel Virtualization Technology	Enabled	Enabled, Disabled	X410c M7	Changed
Memory size limit in GB	0	Between 0-65535	X410c M7	Changed
CR QoS	Disabled	Profile 1, Disabled	X410c M7	Changed
NVM Performance Setting	BW Optimized	BW Optimized, Balanced Profile	X410c M7	Changed
CR FastGo Config	Auto	Enable optimization, Disable Optimization	X410c M7	Changed
Snoopy mode for AD	Disabled	Enabled, Disabled	X410c M7	Changed
Snoopy for 2LM	Disabled	Enabled, Disabled	X410c M7	Changed
Memory refresh rate	1x Refresh	1x Refresh, 2x Refresh	X410c M7	Changed
Panic and High Watermark	Low	High, Low	X410c M7	Changed

Name	Default Value	M7 Server Supported Values	Platform	New/Changed
Memory Thermal Throttling Mode	CLTT with PECI	CLTT with PECI, Disabled	X410c M7	Changed
Enhanced Memory Test	Auto	Enabled, Disabled, Auto	X410c M7	Changed
UMA	Quadrant(4-clusters)	Quadrant(4-clusters), Hemisphere(2-clusters), Disabled	X410c M7	Changed
Volatile Memory Mode	1LM	1LM, 2LM	X410c M7	Changed
eADR	Disabled	Enabled, Disabled, Auto	X410c M7	Changed
Memory Bandwidth Boost	Enabled	Enabled, Disabled	X410c M7	Changed
Virtual NUMA	Disabled	Enabled, Disabled	X410c M7	Changed
XPT remote prefetch	Auto	Enabled, Disabled, Auto	X410c M7	Changed
LLC Dead Line	Enabled	Enabled, Disabled, Auto	X410c M7	Changed
Extended APIC	Enabled	Enabled, Disabled	X410c M7	Changed
Hardware Prefetcher	Enabled	Enabled, Disabled	X410c M7	Changed
Adjacent Cache Line Prefetcher	Enabled	Enabled, Disabled	X410c M7	Changed
DCU Streamer Prefetch	Enabled	Enabled, Disabled	X410c M7	Changed
DCU IP Prefetcher	Enabled	Enabled, Disabled	X410c M7	Changed
Processor C1E	Disabled	Enabled, Disabled	X410c M7	Changed
Processor C6 Report	Enabled	Enabled, Disabled	X410c M7	Changed
Turbo Mode	Enabled	Enabled, Disabled	X410c M7	Changed

Name	Default Value	M7 Server Supported Values	Platform	New/Changed
EIST PSD Function	HW All	HW all, SW all	X410c M7	Changed
Boot Performance Mode	Max Performance	Max Efficient, Max Performance,	X410c M7	Changed
Uncore Frequency Scaling	Enabled	Enabled, Disabled	X410c M7	Changed
SpeedStep (Pstates)	Enabled	Enabled, Disabled	X410c M7	Changed
Configurable TDP Level	Normal	Level 1, Level 2, Normal	X410c M7	Changed
Intel HyperThreading Tech	Enabled	Enabled, Disabled	X410c M7	Changed
CPU Performance	Custom	Enterprise, High Throughput, HPC, Custom	X410c M7	Changed
Processor CMCI	Enabled	Enabled, Disabled	X410c M7	Changed
Cores Enabled	Enabled	All, 1–64	X410c M7	Changed
Workload Configuration	IO Sensitive	Balanced, IO Sensitive	X410c M7	Changed
Sub NUMA Clustering	Disabled	Auto, Disabled, SNC 2, SNC 4	X410c M7	Changed
UPI Prefetch	Auto	Enabled, Disabled, Auto	X410c M7	Changed
XPT Prefetch	Auto	Enabled, Disabled, Auto	X410c M7	Changed
Power Performance Tuning	OS	OS, BIOS, PECI	X410c M7	Changed
Energy/Performance Bias Config	Balanced Performance	Performance, Balanced Performance, Power, Balanced Power	X410c M7	Changed
Package C State	C0 C1 State	No limit, Auto, C0 C1 State, C2, C6 Non Retension, C6 Retention	X410c M7	Changed
LLC Prefetch	Enabled	Enabled, Disabled	X410c M7	Changed

Name	Default Value	M7 Server Supported Values	Platform	New/Changed
Hardware P-States	HWPM Native Mode	HWPM Native Mode, HWPM OOB Mode, Native Mode with no Legacy, Disabled	X410c M7	Changed
Energy Efficient Turbo	Disabled	Enabled, Disabled	X410c M7	Changed
Autonomous Core C-state	Disabled	Enabled, Disabled	X410c M7	Changed
Processor EPP Profile	Balanced Performance	Performance, Balanced Performance, Power, Balanced Power	X410c M7	Changed
Patrol Scrub	Enable at End of POST	Enable at End of POST, Disabled	X410c M7	Changed
Intel Dynamic Speed Select	Disabled	Enabled, Disabled	X410c M7	Changed
DCPMM Firmware Downgrade	Disabled	Enabled, Disabled	X410c M7	Changed
Enhanced CPU Performance	Disabled	Auto, Disabled	X410c M7	Changed
UPI Power Management	Disabled	Enabled, Disabled	X410c M7	Changed
UPI Link Speed	Auto	12.8GT/s, 14.4GT/s, 16.0GT/s, Auto	X410c M7	Changed
LIMIT CPU PA to 46 Bit	Enabled	Enabled, Disabled	X410c M7	Changed
X2APIC Opt Out	Disabled	Enabled, Disabled	X410c M7	Changed

Server BIOS Tokens in Release 4.3(2b)

Cisco UCS Manager supports the following servers in release 4.3(2b):

- Cisco UCS X210c M7 Compute Node
- Cisco UCS X210c M6 Compute Node
- Cisco UCS C220 M7 Server
- Cisco UCS C240 M7 Server
- Cisco UCS C220 M6

- Cisco UCS C240 M6
- Cisco UCS C245 M6
- Cisco UCS C225 M6
- Cisco UCS B200 M6
- Cisco UCS B200 M5
- Cisco UCS B480 M5
- Cisco UCS C220 M5
- Cisco UCS C240 M5
- Cisco UCS C240 SD M5
- Cisco UCS C480 M5
- Cisco UCS C480 M5 ML
- Cisco UCS S3260 M5
- Cisco UCS C125 M5

Related Documentation

- For Cisco UCS C-series and B-series BIOS tokens supported on M6 servers, see Cisco UCS Server BIOS Tokens, Release 4.2.
- For Cisco UCS C-series and B-series BIOS tokens supported on M5 servers, see Cisco UCS Server BIOS Tokens, Release 4.1.

New BIOS Tokens for 4.3(2b)

Name	Default Value	Server Supported Values	Platform	Dependencies	New/Changed
PRMRR Size	256M	Invalid Config, 128M, 256M, 512M,1G, 2G, 4G, 8G, 16G, 32G, 64G, 128G, 256G, 512G	X210c M7, C220M7, C240M7, C220M6, C240M6, B200M6, X210M6	SGX, Total Memory Encryption must be enabled.	New
Burst and Postponed Refresh	Disable	Enabled, Disabled	C225M6, C245M6,		New
Optimized Power Mode	Disable	Enabled, Disabled	X210c M7, C220M7, C240M7		New
Adaptive Refresh Management Level	Default	Default, Level A, Level B, Level C	X210c M7, C220M7, C240M7		New

Name	Default Value	Server Supported Values	Platform	Dependencies	New/Changed
Rank Margin Tool	Disable	Enabled, Disabled	X210c M7, C220M7, C240M7		New
Error Check Scrub	Enabled without result collection	Disabled, Enabled without Result Collection, Enabled with Result Collection	X210c M7, C220M7, C240M7		New
PCIe PLL SSC Percent	255	0–20	X210c M7, C220M7, C240M7		New

BIOS Tokens Supported for UCS C220 M7, UCS C240 M7 and UCS X210c M7 in 4.3(2b)

The following table lists the new BIOS tokens for 4.3(2b) release:

Name	Default Value	M7 Server Supported Values	Platform	New/Changed
PCIe Slot MSTOR RAID OptionROM	Enabled	Enabled Disabled	C220 M7, C240 M7	Changed
Above 4G Decoding	Enabled	Enabled Disabled	C220 M7, C240 M7, X210c M7	Changed
VMD Enablement	Disabled	Enabled Disabled	C220 M7, C240 M7, X210c M7	Changed
PCIe RAS Support	Enabled	Enabled Disabled	C220 M7, C240 M7, X210c M7	Changed
CDN Support for LOM	Disabled	Enabled, Disabled	X210c M7	Changed
External SSC Enable	Off	0P3_Percent,P5_Percent, Hardware, Off	C220 M7, C240 M7, X210c M7	Changed
IIO eDPC Support	On fatal and non-fatal error	Disabled, On fatal error, On fatal and non-fatal error	C220 M7, C240 M7	Changed
CDN Control	Enabled	Enabled, Disabled	C220 M7, C240 M7, X210c M7	Changed
PCIe Slots CDN Control	Disabled	Enabled, Disabled	C220 M7, C240 M7	Changed
Intel VT for directed IO	Enabled	Enabled, Disabled	C220 M7, C240 M7, , X210c M7	Changed
Intel VTD Coherency Support	Disabled	Enabled, Disabled	C220 M7, C240 M7, X210c M7	Changed

Name	Default Value	M7 Server Supported Values	Platform	New/Changed
USB Port Front	Enabled	Enabled, Disabled	X210c M7	Changed
USB Port Rear	Enabled	Enabled, Disabled	C220 M7, C240 M7	Changed
USB Port KVM	Enabled	Enabled, Disabled	X210c M7	Changed
USB Port:M.2 Storage	Enabled	Enabled, Disabled	X210c M7	Changed
NTB Test Mode	Disabled	Enabled, Disabled	X410c M7, X210c M7	Changed
NTB Device Type	Upstream	Upstream, Downstream	X410c M7, X210c M7	Changed
C1 Auto demotion	Enabled	Enabled, Disabled	C220 M7, C240 M7, X210c M7	Changed
C1 Auto Demotion	Enabled	Enabled, Disabled	C220 M7, C240 M7, X210c M7	Changed
FRB 2 Timer	Enabled	Enabled, Disabled	C220 M7, C240 M7, X210c M7	Changed
OS Watchdog Timer Policy	Power Off	Reset, Power Off	C220 M7, C240 M7, X210c M7	Changed
OS Watchdog Timer Timeout	10 minutes	5 minutes, 10 minutes, 15 minutes, 20 minutes	C220 M7, C240 M7, X210c M7	Changed
OS Watchdog timer	Disabled	Enabled, Disabled	C220 M7, C240 M7, X210c M7	Changed
Flow Control	None	None, RTS-CTS	C220 M7, C240 M7, X210c M7	Changed
Baud Rate	115.2k	9.6k, 19.2k,38.4k, 57.6k, 115.2k	C220 M7, C240 M7, X210c M7	Changed
Terminal Type	VT100	PC-ANSI, VT100, VT100-PLUS, VT-UTF8	C220 M7, C240 M7, X210c M7	Changed
Console Redirection	VT100	PC-ANSI, VT100, VT100-PLUS, VT-UTF8	C220 M7, C240 M7, X210c M7	Changed
Adaptive Memory Training	Enabled	Enabled, Disabled	C220 M7, C240 M7, X210c M7	Changed
OptionROM Launch Optimization	Enabled	Enabled, Disabled	C220 M7, C240 M7, X210c M7	Changed

Name	Default Value	M7 Server Supported Values	Platform	New/Changed
BIOS Techlog level	Minimum	Maximum, Minimum, Normal	C220 M7, C240 M7, X210c M7	Changed
VGA priority	Onboard	Onboard, Offboard, Onboard VGA Disabled	C220 M7, C240 M7	Changed
IPV6 PXE support	Enabled	Enabled, Disabled	C220 M7, C240 M7, X210c M7	Changed
Network stack	Enabled	Enabled, Disabled	C220 M7, C240 M7, X210c M7	Changed
IPv4 PXE Support	Enabled	Enabled, Disabled	C220 M7, C240 M7, X210c M7	Changed
IPv4 HTTP Support	Enabled	Enabled, Disabled	C220 M7, C240 M7, X210c M7	Changed
IPv6 HTTP Support	Enabled	Enabled, Disabled	C220 M7, C240 M7, X210c M7	Changed
Security Device Support	Enabled	Enabled, Disabled	C220 M7, C240 M7, X210c M7	Changed
Trusted Platform Module State	Enabled	Enabled, Disabled	C220 M7, C240 M7, X210c M7	Changed
SHA-1 PCR Bank	Enabled	Enabled, Disabled	C220 M7, C240 M7, X210c M7	Changed
SHA256 PCR Bank	Enabled	Enabled, Disabled	C220 M7, C240 M7, X210c M7	Changed
TPM Pending Operation	None	None, TpmClear	C220 M7, C240 M7, X210c M7	Changed
TPM Minimal Physical Presence	Disabled	Enabled, Disabled	C220 M7, C240 M7, X210c M7	Changed
Intel Trusted Execution Technology Support	Enabled	Enabled, Disabled	C220 M7, C240 M7, X210c M7	Changed
Total Memory Encryption (TME)	Disabled	Enabled, Disabled	C220 M7, C240 M7, X210c M7	Changed
SGX QoS	Enabled	Enabled, Disabled	C220 M7, C240 M7, X210c M7	Changed
SGX write Enable	Enabled	Enabled, Disabled	C220 M7, C240 M7, X210c M7	Changed

Name	Default Value	M7 Server Supported Values	Platform	New/Changed
DMA Control Opt-In Flag	Disabled	Enabled, Disabled	C220 M7, C240 M7,X210c M7	Changed
Power on Password	Disabled	Enabled, Disabled	C220 M7, C240 M7	Changed
Multikey Total Memory Encryption	Disabled	Enabled, Disabled	C220 M7, C240 M7, X210c M7	Changed
SW Guard Extensions (SGX)	Disabled	Enabled, Disabled	C220 M7, C240 M7, X210cM7	Changed
SGX Factory Reset	Disabled	Enabled, Disabled	C220 M7, C240 M7, X210c M7	Changed
SGX Pkg info In-Band Access	Disabled	Enabled, Disabled	C220 M7, C240 M7, X210c M7	Changed
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 M7, C240 M7, X210c M7	Changed
SGX Auto MP Registration Agent	Disabled	Enabled, Disabled	C220 M7, C240 M7, X210c M7	Changed
SProcessor Epoch 0	0	Between 7-0	C220 M7, C240 M7,X210c M7	Changed
Pubkey Hash 0	0	Between 7-0	C220 M7, C240 M7, X210c M7	Changed
SGX Pubkey Hash 1	0	Between 15-8	C220 M7, C240 M7, X210c M7	Changed
NUMA	Disabled	Enabled, Disabled	C220 M7, C240 M7, X210cM7	Changed
Select Memory RAS Configuration	ADDDC Sparing	Mirror Mode 1LM, Partial Mirror mode 1LM, Maximum Performance, ADDDC Sparing	C220 M7, C240 M7, X210c M7	Changed
Select PPR type	Hard PPR	Disabled, Hard PPR	C220 M7, C240 M7, X210c M7	Changed
Partial Cache Line Sparing	Disabled	Enabled, Disabled	C220 M7, C240 M7, X210c M7	Changed

Name	Default Value	M7 Server Supported Values	Platform	New/Changed
BME DMA Mitigation	Disabled	Enabled, Disabled	C220 M7, C240 M7, X210c M7	Changed
Partial Memory Mirror Mode	Disabled	Percentage, Value in GB, Disabled	C220 M7, C240 M7, X210c M7	Changed
Partial Mirror Percentage	0	Between 0-50	C220 M7, C240 M7, X210cM7	Changed
Intel Virtualization Technology	Enabled	Enabled, Disabled	C220 M7, C240 M7, X210c M7	Changed
Memory size limit in GB	0	Between 0-65535	C220 M7, C240 M7, X210c M7	Changed
CR QoS	Disabled	Profile 1, Disabled	C220 M7, C240 M7, X210c M7	Changed
NVM Performance Setting	BW Optimized	BW Optimized, Balanced Profile	C220 M7, C240 M7, X210cM7	Changed
CR FastGo Config	Auto	Enable optimization, Disable Optimization	C220 M7, C240 M7, X210c M7	Changed
Snoopy mode for AD	Disabled	Enabled, Disabled	C220 M7, C240 M7, X210c M7	Changed
Snoopy for 2LM	Disabled	Enabled, Disabled	C220 M7, C240 M7, X210c M7	Changed
Memory refresh rate	1x Refresh	1x Refresh, 2x Refresh	C220 M7, C240 M7, X210c M7	Changed
Panic and High Watermark	Low	High, Low	C220 M7, C240 M7, X210c M7	Changed
Memory Thermal Throttling Mode	CLTT with PECI	CLTT with PECI, Disabled	C220 M7, C240 M7, X210c M7	Changed
Enhanced Memory Test	Auto	Enabled, Disabled, Auto	C220 M7, C240 M7, X210c M7	Changed
UMA	Quadrant(4-clusters)	Quadrant(4-clusters), Hemisphere(2-clusters), Disabled	C220 M7, C240 M7, X210c M7	Changed
Volatile Memory Mode	1LM	1LM, 2LM	C220 M7, C240 M7, X210c M7	Changed
eADR	Disabled	Enabled, Disabled, Auto	C220 M7, C240 M7, X210c M7	Changed

Name	Default Value	M7 Server Supported Values	Platform	New/Changed
Memory Bandwidth Boost	Enabled	Enabled, Disabled	C220 M7, C240 M7, X210c M7	Changed
Virtual NUMA	Disabled	Enabled, Disabled	C220 M7, C240 M7, X210c M7	Changed
XPT remote prefetch	Auto	Enabled, Disabled, Auto	C220 M7, C240 M7, X210cM7	Changed
LLC Dead Line	Enabled	Enabled, Disabled, Auto	C220 M7, C240 M7, X210c M7	Changed
Extended APIC	Enabled	Enabled, Disabled	C220 M7, C240 M7, X210c M7	Changed
Hardware Prefetcher	Enabled	Enabled, Disabled	C220 M7, C240 M7, X210c M7	Changed
Adjacent Cache Line Prefetcher	Enabled	Enabled, Disabled	C220 M7, C240 M7, X210c M7	Changed
DCU Streamer Prefetch	Enabled	Enabled, Disabled	C220 M7, C240 M7, X210c M7	Changed
DCU IP Prefetcher	Enabled	Enabled, Disabled	C220 M7, C240 M7, X210cM7	Changed
Processor C1E	Disabled	Enabled, Disabled	C220 M7, C240 M7, X210c M7	Changed
Processor C6 Report	Enabled	Enabled, Disabled	C220 M7, C240 M7, X210cM7	Changed
Turbo Mode	Enabled	Enabled, Disabled	C220 M7, C240 M7, X210c M7	Changed
EIST PSD Function	HW All	HW all, SW all	C220 M7, C240 M7, X210c M7	Changed
Boot Performance Mode	Max Performance	Max Efficient, Max Performance,	C220 M7, C240 M7, X210c M7	Changed
Uncore Frequency Scaling	Enabled	Enabled, Disabled	C220 M7, C240 M7, X210c M7	Changed
SpeedStep (Pstates)	Enabled	Enabled, Disabled	C220 M7, C240 M7, X210c M7	Changed
Configurable TDP Level	Normal	Level 1, Level 2, Normal	C220 M7, C240 M7, X210c M7	Changed

Name	Default Value	M7 Server Supported Values	Platform	New/Changed
Intel HyperThreading Tech	Enabled	Enabled, Disabled	C220 M7, C240 M7, X210c M7	Changed
CPU Performance	Custom	Enterprise, High Throughput, HPC, Custom	C220 M7, C240 M7, ,X210c M7	Changed
Processor CMCI	Enabled	Enabled, Disabled	C220 M7, C240 M7, X210c M7	Changed
Cores Enabled	Enabled	All, 1–64	C220 M7, C240 M7, X210c M7	Changed
Workload Configuration	IO Sensitive	Balanced, IO Sensitive	C220 M7, C240 M7, X210c M7	Changed
Sub NUMA Clustering	Disabled	Auto, Disabled, SNC 2, SNC 4	C220 M7, C240 M7, X210c M7	Changed
UPI Prefetch	Auto	Enabled, Disabled, Auto	C220 M7, C240 M7, X210c M7	Changed
XPT Prefetch	Auto	Enabled, Disabled, Auto	C220 M7, C240 M7, X210c M7	Changed
Power Performance Tuning	OS	OS, BIOS, PECI	C220 M7, C240 M7, X210c M7	Changed
Energy/Performance Bias Config	Balanced Performance	Performance, Balanced Performance, Power, Balanced Power	C220 M7, C240 M7, X210c M7	Changed
Package C State	C0 C1 State	No limit, Auto, C0 C1 State, C2, C6 Non Retension, C6 Retention	C220 M7, C240 M7, X210c M7	Changed
LLC Prefetch	Enabled	Enabled, Disabled	C220 M7, C240 M7, X210c M7	Changed
Hardware P-States	HWPM Native Mode	HWPM Native Mode, HWPM OOB Mode, Native Mode with no Legacy, Disabled	C220 M7, C240 M7, X210c M7	Changed
Energy Efficient Turbo	Disabled	Enabled, Disabled	C220 M7, C240 M7, X210c M7	Changed
Autonomous Core C-state	Disabled	Enabled, Disabled	C220 M7, C240 M7, X210c M7	Changed

Name	Default Value	M7 Server Supported Values	Platform	New/Changed
Processor EPP Profile	Balanced Performance	Performance, Balanced Performance, Power, Balanced Power	C220 M7, C240 M7, X210c M7	Changed
Patrol Scrub	Enable at End of POST	Enable at End of POST, Disabled	C220 M7, C240 M7, X210c M7	Changed
Intel Dynamic Speed Select	Disabled	Enabled, Disabled	C220 M7, C240 M7, X210c M7	Changed
DCPMM Firmware Downgrade	Disabled	Enabled, Disabled	C220 M7, C240 M7, X210c M7	Changed
Enhanced CPU Performance	Disabled	Auto, Disabled	C220 M7, C240 M7, X210c M7	Changed
UPI Power Management	Disabled	Enabled, Disabled	C220 M7, C240 M7, X210c M7	Changed
UPI Link Speed	Auto	12.8GT/s, 14.4GT/s, 16.0GT/s, Auto	C220 M7, C240 M7, X210c M7	Changed
LIMIT CPU PA to 46 Bit	Enabled	Enabled, Disabled	C220 M7, C240 M7, X210c M7	Changed
X2APIC Opt Out	Disabled	Enabled, Disabled	C220 M7, C240 M7, X210c M7	Changed
PCIe Slots CDN Control	Enabled	Enabled, Disabled	C220 M7, C240 M7, C220 M6, C240 M6, C225 M6, C245M6	Changed