Release Notes for Cisco UCS Rack Server Software, Release 4.2(1)

First Published: 2021-09-01

Last Modified: 2022-08-01

Cisco UCS C-Series Servers

Cisco UCS C-Series Servers deliver unified computing in an industry-standard form factor to reduce total cost of ownership and increase agility. Each product addresses varying workload challenges through a balance of processing, memory, I/O, and internal storage resources.

About the Release Notes

This document describes the new features, system requirements, open caveats and known behaviors for C-Series software release 4.2(1) including Cisco Integrated Management Controller (Cisco IMC) software and any related BIOS, firmware, or drivers. Use this document in conjunction with the documents listed in the Related Documentation, on page 31 section.

Note We sometimes update the documentation after original publication. Therefore, you should also refer to the documentation on Cisco.com for any updates.

Revision History

Revision	Date	Description
H0	August 1, 2022	Created release notes for 4.2(1j) for Cisco UCS C220 M6, C225 M6, C240 M6 and C245 M6 Servers. The firmware files in Cisco Host Upgrade Utility for individual releases are available at: Cisco UCS C-Series Integrated Management Controller Firmware Files, Release 4.2
G1	July 12, 2022	Updated Known Behaviors and Limitations for release 4.2(1i).

Revision	Date	Description
G0	May 16, 2022	Created release notes for 4.2(1i) for Cisco UCS C220 M6, C225 M6, C240 M6 and C245 M6 Servers. The firmware files in Cisco Host Upgrade Utility for individual releases are available at: Cisco UCS C-Series Integrated Management Controller Firmware Files, Release 4.2
F0	March 22, 2022	Created release notes for 4.2(1g) for Cisco UCS C225 M6 and C245 M6 Servers. The firmware files in Cisco Host Upgrade Utility for individual releases are available at: Cisco UCS C-Series Integrated Management Controller Firmware Files, Release 4.2 Updated Known Behaviors and Limitations in Release 4.2(1f).
E0	February 07, 2022	Created release notes for 4.2(1f) for Cisco UCS C220 M6, C225 M6, C240 M6 and C245 M6 Servers. The firmware files in Cisco Host Upgrade Utility for individual releases are available at: Cisco UCS C-Series Integrated Management Controller Firmware Files, Release 4.2 Updated Security Fixes for release 4.2(1b).
D0	October 26, 2021	Created release notes for 4.2(1e) for Cisco UCS C220 M6, C225 M6, C240 M6 and C245 M6 Servers. The firmware files in Cisco Host Upgrade Utility for individual releases are available at: Cisco UCS C-Series Integrated Management Controller Firmware Files, Release 4.2
C1	September 09, 2021	Updated Open Caveats for release 4.2(1c).

Revision	Date	Description
C0	September 1, 2021	Created release notes for 4.2(1c) for Cisco UCS C225 M6 and Cisco UCS C245 M6 Servers. The firmware files in Cisco Host Upgrade Utility for individual releases are available at: Cisco UCS C-Series Integrated Management Controller Firmware Files, Release 4.2
B0	August 17, 2021	Created release notes for 4.2(1b) for Cisco UCS C220 M6 and Cisco UCS C240 M6 Servers. The firmware files in Cisco Host Upgrade Utility for individual releases are available at: Cisco UCS C-Series Integrated Management Controller Firmware Files, Release 4.2
A0	June 24, 2021	Created release notes for 4.2(1a) for Cisco UCS C220 M6, Cisco UCS C240 M6, and Cisco UCS C245 M6 Servers. The firmware files in Cisco Host Upgrade Utility for individual releases are available at: Cisco UCS C-Series Integrated Management Controller Firmware Files, Release 4.2

Supported Platforms and Release Compatibility Matrix

Supported Platforms in this Release

The following servers are supported in this release:

- Cisco UCS C220 M6
- Cisco UCS C240 M6
- Cisco UCS C245 M6
- Cisco UCS C225 M6

For information about these servers, see Overview of Servers.

Cisco IMC and Cisco UCS Manager Release Compatibility Matrix

Cisco UCS C-Series Rack-Mount Servers are managed by built-in standalone software —Cisco IMC. However, when a Rack-Mount Server is integrated with Cisco UCS Manager, the Cisco IMC does not manage the server anymore.

The following table lists the supported platforms, Cisco IMC releases, and Cisco UCS Manager releases for Rack-Mount Servers:

Table 1: Cisco IMC and UCS Manager Software Releases for Rack Mount Servers for Cisco IMC 4.2(1) Release

Cisco IMC Release	Cisco UCS Manager Release	Rack Mount Servers
4.2(1j)	4.2(1n)	Cisco UCS C220 M6, C225 M6, C240 M6, and C245 M6 servers
4.2(1i)	4.2(1m)	Cisco UCS C220 M6, C225 M6, C240 M6, and C245 M6 servers
4.2(1g)	No Support	Cisco UCS C225 M6 and C245 M6 servers
4.2(1f)	4.2(1k)	Cisco UCS C220 M6, C225 M6, C240 M6, and C245 M6 servers
4.2(1e)	4.2(1i)	Cisco UCS C220 M6, C225 M6, C240 M6, and C245 M6 servers
4.2(1c)	No Support	Cisco UCS C225 M6 and C245 M6 servers
4.2(1b)	4.2(1f)	Cisco UCS C220 M6 and C240 M6 servers
4.2(1a)	4.2(1d)	Cisco UCS C220 M6, C240 M6, and C245 M6 servers **Note** Cisco UCS Manager does not support Cisco UCS C245 M6 servers.

Table 2: Cisco IMC and UCS Manager Software Releases for Rack Mount Servers for Cisco IMC 4.1(3) Release

Cisco IMC Release	Cisco UCS Manager Release	Rack Mount Servers
4.1(3i)	4.1(3j)	Cisco UCS C220 M5, C240 M5, C480 M5, S3260 M4, S3260 M5, C125 M5 servers
4.1(3h)	4.1(3i)	Cisco UCS C220 M5, C240 M5, C480 M5, S3260 M4, S3260 M5, C125 M5 servers

Cisco IMC Release	Cisco UCS Manager Release	Rack Mount Servers
4.1(3g)	No Support	Cisco UCS S3260 M4 and S3260 M5 servers
4.1(3f)	4.1(3h)	Cisco UCS C220 M5, C240 M5, C480 M5, S3260 M4, S3260 M4, S3260 M5, and C125 M5 servers
4.1(3d)	4.1(3e)	Cisco UCS C220 M5, C240 SD M5, C240 M5, C480 M5, C480 ML M5, S3260 M4, S3260 M5, and C125 M5 servers
4.1(3c)	4.1(3d)	Cisco UCS C220 M5, C240 SD M5, C240 M5, C480 M5, C480 ML M5, S3260 M4, S3260 M5 and C125 M5 servers
4.1(3b)	4.1(3a)	Cisco UCS C220 M5, C240 SD M5, C240 M5, C480 M5, C480 ML M5, S3260 M4, S3260 M5 and C125 M5 servers

Table 3: Cisco IMC and UCS Manager Software Releases for Rack Mount Servers for Cisco IMC 4.1(2) Release

Cisco IMC Release	Cisco UCS Manager Release	Rack Mount Servers
4.1(2k)	No Support	Cisco UCS C220 M4, C240 M4, and C460 M4 servers
4.1(2j)	No Support	Cisco UCS C220 M4, C240 M4, and C460 M4 servers
4.1(2h)	No Support	Cisco UCS C220 M4, C240 M4, and C460 M4 servers
4.1(2g)	No Support	Cisco UCS C220 M4, C240 M4, and C460 M4 servers
4.1(2f)	4.1(2c)	Cisco UCS C220 M5, C240 SD M5, C240 M5, C480 M5, C480 ML M5, S3260 M5, C220 M4, C240 M4, C460 M4, and S3260 M4 servers
4.1(2e)	No Support	Cisco UCS C125 M5 servers
4.1(2d)	No Support	Cisco UCS C240 M5 and C240 SD M5 servers

Cisco IMC Release	Cisco UCS Manager Release	Rack Mount Servers
4.1(2b)	4.1(2b)	Cisco UCS C220 M5, C240 SD M5, C240 M5, C480 M5, C480 ML M5, S3260 M5, C125 M5, C220 M4, C240 M4, C460 M4, and S3260 M4 servers
4.1(2a)	4.1(2a)	Cisco UCS C220 M5, C240 SD M5, C240 M5, C480 M5, C480 ML M5, S3260 M5, C125 M5, C220 M4, C240 M4, C460 M4, and S3260 M4 servers

Table 4: Cisco IMC and UCS Manager Software Releases for Rack Mount Servers for Cisco IMC 4.1(1) Release

Cisco IMC Release	Cisco UCS Manager Release	Rack Mount Servers
4.1(1h)	4.1(1e)	Cisco UCS C220 M5, C240 M5, C480 M5, C480 ML M5, S3260 M5, C125 M5, C220 M4, C240 M4, C460 M4, and S3260 M4 servers
4.1(1g)	4.1(1d)	Cisco UCS C220 M5, C240 M5, C480 M5, C480 ML M5, S3260 M5, C125 M5, C220 M4, C240 M4, C460 M4, and S3260 M4 servers
4.1(1f)	4.1(1c)	Cisco UCS C220 M5, C240 M5, C480 M5, C480 ML M5, S3260 M5, C125 M5, C220 M4, C240 M4, C460 M4, and S3260 M4 servers
4.1(1d)	4.1(1b)	Cisco UCS C220 M5, C240 M5, C480 M5, and C480 ML M5 servers
4.1(1c)	4.1(1a)	Cisco UCS C220 M5, C240 M5, C480 M5, C480 ML M5, S3260 M5, C125 M5, C220 M4, C240 M4, C460 M4, and S3260 M4 servers

Table 5: Cisco IMC and UCS Manager Software Releases for Rack Mount Servers for Cisco IMC 4.0(4) Release

Cisco IMC Release	Cisco UCS Manager Release	Rack Mount Servers
4.0(4n)	4.0(4l)	Cisco UCS C220 M5, C240 M5, C480 M5, and S3260 M5 servers
4.0(4m)	4.0(4j)	Cisco UCS C220 M5, C240 M5, C480 M5, and S3260 M5 servers
4.0(4l)	4.0(4i)	Cisco UCS C220 M5, C240 M5, C480 M5, and S3260 M5 servers

Cisco IMC Release	Cisco UCS Manager Release	Rack Mount Servers
4.0(4k)	4.0(4h)	Cisco UCS C220 M5, C240 M5, and S3260 M5 servers
4.0(4j)	No Support	Cisco UCS S3260 M5 servers
4.0(4i)	4.0(4g)	Cisco UCS C220 M5, C240 M5, C480 M5 and S3260 M5 servers
4.0(4h)	4.0(4e)	Cisco UCS C220 M5, C240 M5, C480 M5 and S3260 M5 servers
4.0(4f)	4.0(4d)	Cisco UCS C220 M5, C240 M5, C480 M5, S3260 M5 and C480 ML M5 servers
4.0(4e)	4.0(4c)	Cisco UCS C220 M5, C240 M5, C480 M5, S3260 M5 and C480 ML M5 servers
4.0(4d)	No Support	Cisco UCS C220 M5, C240 M5, C480 M5 and S3260 M5 servers
4.0(4b)	4.0(4a)	Cisco UCS C220 M5, C240 M5, C480 M5, S3260 M5 and C480 ML M5 servers

Table 6: Cisco IMC and UCS Manager Software Releases for Rack Mount Servers for Cisco IMC 4.0(3) Release

Cisco IMC Release	Cisco UCS Manager Release	Rack Mount Servers
4.0(3b)	4.0(3a)	Cisco UCS C220 M5 and C240 M5 servers

Table 7: Cisco IMC and UCS Manager Software Releases for Rack Mount Servers for Cisco IMC 4.0(2) Release

Cisco IMC Release	Cisco UCS Manager Release	Rack Mount Servers
4.0(2r)	No support	Cisco UCS C220 M4, C240 M4, and C460 M4 servers.
4.0(2q)	4.0(4l)	Cisco UCS C220 M4, C240 M4, C460 M4, and S3260 M4 servers
4.0(2p)	No support.	Cisco UCS C125 M5 servers
4.0(2o)	4.0(4j)	Cisco UCS C220 M4, C240 M4, C460 M4, and S3260 M4 servers

Cisco IMC Release	Cisco UCS Manager Release	Rack Mount Servers
4.0(2n)	No support.	Cisco UCS C220 M5, C240 M5, C480 M5, C480 ML M5, S3260 M5, C125 M5, C220 M4, C240 M4, C460 M4, and S3260 M4 servers
4.0(2m)	No support.	Cisco UCS S3260 M4 and M5 servers
4.0(2l)	No support.	Cisco UCS C220 M5, C240 M5, C480 M5, C480 ML M5, S3260 M5, C220 M4, C240 M4, C460 M4, and S3260 M4 servers
4.0(2k)	No support.	Cisco UCS S3260 M4 and M5 servers
4.0(2i)	No support.	Cisco UCS C460 M4, S3260 M4, and S3260 M5 servers
4.0(2h)	4.0(2e)	Cisco UCS C220 M5, C240 M5, C480 M5, C480 ML M5, S3260 M5, C125 M5, C220 M4, C240 M4, C460 M4, and S3260 M4 servers
4.0(2f)	4.0(2d)	Cisco UCS C220 M5, C240 M5, C480 M5, C480 ML M5, S3260 M5, C125 M5, C220 M4, C240 M4, C460 M4, and S3260 M4 servers
4.0(2d)	4.0(2b)	Cisco UCS C220 M5, C240 M5, C480 M5, C480 ML M5, S3260 M5, C125 M5, C220 M4, C240 M4, C460 M4, and S3260 M4 servers
4.0(2c)	4.0(2a)	Cisco UCS C220 M5, C240 M5, C480 M5, C480 ML M5, S3260 M5, C125 M5, C220 M4, C240 M4, C460 M4, and S3260 M4 servers

Table 8: Cisco IMC and UCS Manager Software Releases for Rack Mount Servers for Cisco IMC 4.0(1) Release

Cisco IMC Release	Cisco UCS Manager Release	Rack Mount Servers
4.0(1h)	No support.	Cisco UCS C220 M4, C240 M4, C460 M4, C220 M5, C240 M5, C480 M5 servers and C125 M5
4.0(1g)	No support.	Cisco UCS C220 M4, C240 M4, C460 M4, C220 M5, C480 M5 servers and C125 M5
4.0(1e)	No support.	Cisco UCS M4, M5 servers and C125 M5

Cisco IMC Release	Cisco UCS Manager Release	Rack Mount Servers
4.0(1d)	4.0(1d)	Cisco UCS M4, M5 servers and C125 M5
4.0(1c)	4.0(1c)	Cisco UCS M4, M5 servers and C125 M5
4.0(1b)	4.0(1b)	Cisco UCS M4, M5 servers and C125 M5
4.0(1a)	4.0(1a)	Cisco UCS M4, M5 servers and C125 M5

Table 9: Cisco IMC and UCS Manager Software Releases for Rack Mount Servers for Cisco IMC 3.1(3) Release

Cisco IMC Release	Cisco UCS Manager Release	Rack Mount Servers
3.1(3k)	3.2(3p)	Cisco UCS C480 M5, C220 M5, C240 M5, and S3260 M5 servers
3.1(3j)	No Support **Note** We support discovery and upgrade or downgrade functions with Cisco UCS Manager.	Cisco UCS C480 M5, C220 M5, C240 M5, and S3260 M5 servers
3.1(3i)	3.2(3i)	Cisco UCS C480 M5, C220 M5, C240 M5, and S3260 M5 servers
3.1(3h)	3.2(3h)	Cisco UCS C480 M5, C220 M5, C240 M5, and S3260 M5 servers
3.1(3g)	3.2(3g)	Cisco UCS C480 M5, C220 M5, C240 M5, and S3260 M5 servers
3.1(3d)	3.2(3e)	Cisco UCS C480 M5, C220 M5, C240 M5, and S3260 M5 servers
3.1(3c)	3.2(3d)	Cisco UCS C480 M5, C220 M5, C240 M5, and S3260 M5 servers
3.1(3b)	3.2(3b)	Cisco UCS C480 M5, C220 M5, and C240 M5 servers
3.1(3a)	3.2(3a)	Cisco UCS C480 M5, C220 M5, C240 M5, and S3260 M5 servers

Table 10: Cisco IMC and UCS Manager Software Releases for Rack Mount Servers for Cisco IMC 3.1(2) Release

Cisco IMC Release	Cisco UCS Manager Release	Rack Mount Servers
3.1(2d)	3.2(2d)	Cisco UCS C480 M5, C220 M5, and C240 M5
3.1(2c)	3.2(2c)	Cisco UCS C480 M5, C220 M5, and C240 M5
3.1(2b)	3.2(2b)	Cisco UCS C480 M5, C220 M5, and C240 M5

Table 11: Cisco IMC and UCS Manager Software Releases for Rack Mount Servers for Cisco IMC 3.1(1) Release

C-Series Standalone Release	Cisco UCS Manager Release	C-Series Servers
3.1(1d)	3.2(1d)	Cisco UCS C220 M5/C2540 M5

Table 12: Cisco IMC and UCS Manager Software Releases for Rack Mount Servers for Cisco IMC 3.0(4) Release

Cisco IMC Release	Cisco UCS Manager Release	Rack-Mount Servers
3.0(4s)	No support	Cisco UCS C220 M3, C240 M3, C3160 M3, S3260 M4
3.0(4r)	No support	Cisco UCS C220 M4, C240 M4, C460 M4, S3260 M4, C22 M3, C24 M3, C220 M3, C240 M3, C3160 M3, S3260 M3
3.0(4q)	No support	Cisco UCS C220 M4, C240 M4, C460 M4, S3260 M4, C22 M3, C24 M3, C220 M3, C240 M3, C3160 M3, S3260 M3
3.0(4p)	3.2(3o)	Cisco UCS C220 M4, C240 M4, C460 M4, S3260 M4, C22 M3, C24 M3, C220 M3, C240 M3, C3160 M3, S3260 M3
3.0(4o)	No support	Cisco UCS C220 M4, C240 M4, C460 M4, S3260 M4, C22 M3, C24 M3, C220 M3, C240 M3, C3160 M3, S3260 M3
3.0(4n)	No support.	Cisco UCS C220 M4, C240 M4, C460 M4, S3260 M4, C22 M3, C24 M3, C220 M3, C240 M3, C3160 M3, S3260 M3

Cisco IMC Release	Cisco UCS Manager Release	Rack-Mount Servers
3.0(4m)	No support.	Cisco UCS C220 M4, C240 M4, C460 M4, S3260 M4, C22 M3, C24 M3, C220 M3, C240 M3, C3160 M3, S3260 M3
3.0(4l)	No support.	Cisco UCS C220 M4, C240 M4, C460 M4, S3260 M4, C22 M3, C24 M3, C220 M3, C240 M3, C3160 M3, S3260 M3
3.0(4k)	No support.	Cisco UCS C220 M4, C240 M4, C460 M4, S3260 M4, C22 M3, C24 M3, C220 M3, C240 M3, C3160 M3, S3260 M3
3.0(4j)	3.1(3k)	Cisco UCS C220 M4, C240 M4, C460 M4, S3260 M4, C22 M3, C24 M3, C220 M3, C240 M3, C3160 M3, S3260 M3
3.0(4i)	3.1(3j)	Cisco UCS C220 M4, C240 M4, C460 M4, S3260 M4, C22 M3, C24 M3, C220 M3, C240 M3, C3160 M3, S3260 M3
3.0(4e)	No support	Cisco UCS C220 M4, C240 M4, C460 M4, S3260 M4, C22 M3, C24 M3, C220 M3, C240 M3, C3160 M3, S3260 M3
3.0(4d)	3.1(3h)	Cisco UCS C220 M4, C240 M4, C460 M4, S3260 M4, C22 M3, C24 M3, C220 M3, C240 M3, C3160 M3, S3260 M3
3.0(4a)	3.1(3f)	Cisco UCS C220 M4, C240 M4, C460 M4, S3260 M4, C22 M3, C24 M3, C220 M3, C240 M3, C3160 M3, S3260 M3

Table 13: Cisco IMC and UCS Manager Software Releases for Rack Mount Servers for Cisco IMC 3.0(3) Release

Cisco IMC Release	Cisco UCS Manager Release	Rack-Mount Servers
3.0(3f)	-	Cisco UCS C240 M4, and C220 M4
3.0(3e)	3.0(3e)	Cisco UCS C22 M3, C24 M3, C220 M3, C240 M3, C220 M4, C240 M4, C460 M4, C3160 M3, S3260 M4 and S3260 M3 servers

Cisco IMC Release	Cisco UCS Manager Release	Rack-Mount Servers
3.0(3c)	3.0(3c)	Cisco UCS C240 M4, and C220 M4
3.0(3b)	3.0(3b)	Cisco UCS S3260 M3, C3160 M3, C460 M4, C240 M4, and C220 M4
3.0(3a)	3.1(3a)	Cisco UCS C22 M3, C24 M3, C220 M3, C240 M3, C220 M4, C240 M4, C460 M4, C3160 M3, S3260 M4 and S3260 M3 servers

Table 14: Cisco IMC and UCS Manager Software Releases for Rack Mount Servers for Cisco IMC 3.0(2) Release

Cisco IMC Release	Cisco UCS Manager Release	Rack-Mount Servers
3.0(2b)	No Support **Note** We support discovery and upgrade or downgrade functions with Cisco UCS Manager.	C220 M4/C240 M4 only

Table 15: Cisco IMC and UCS Manager Software Releases for Rack Mount Servers for Cisco IMC 3.0(1) Release

Cisco IMC Release	Cisco UCS Manager Release	Rack-Mount Servers
3.0(1d)	No Support **Note** We support discovery and upgrade or downgrade functions with Cisco UCS Manager.	All M3/M4 except C420 M3
3.0(1c)	No Support	All M3/M4 except C420 M3

Cisco IMC Release	UCS Manager Release	Rack Mount Servers
2.0(13e)	3.1(2b)	All M3/M4 except C420 M3
2.0(10b)	3.1(1g)	C220 M4/C240 M4 only
2.0(9c)	3.1(1e)	All other M3/M4
2.0(9f)	2.2(7b)	For all other M3/M4
2.0(10b)	2.2(7b)	C220 M4/C240 M4 only
1.5(9d)	2.2(7b)	C420-M3, C260-M2, C460-M2 only

Cisco IMC Release	UCS Manager Release	Rack Mount Servers
1.5(9d)	2.2(8f)	C420-M3, C260-M2, C460-M2 only
2.0(9c)	2.2(8f)	For all other M3/M4
2.0(10b)	2.2(8f)	C220 M4/C240 M4 only
2.0(12b)	2.2(8f)	C460 M4 only
1.5(8a)	2.2(6g)	C420 M3, C260 M2, C460 M2 only
2.0(8d)	2.2(6c)	For all other M3/M4
1.5(7f)	2.2(5b)	C420 M3, C260 M2, C460 M2 only
2.0(6d)	2.2(5a)	For all other M3/M4
1.5(7a)2	2.2(4b)	C420 M3, C260 M2, C460 M2 only
2.0(4c)	2.2(4b)	For all other M3/M4
1.5(7c)1	2.2(3b)	C420 M3, C260 M2, C460 M2 only
2.0(3d)1	2.2(3a)	For all other M3/M4

Operating System and Browser Requirements

For detailed information about supported Operating System, see the interactive UCS Hardware and Software Compatibility matrix.

Cisco recommends the following browsers for Cisco UCS Rack Server Software, Release 4.2(1):

Recommended Browser	Browser Version	Recommended Operating System
Microsoft Edge	87.0.664.47 (Official build) (64-bit)	Windows 10 x64
Google Chrome	87.0.4280.66 (Official Build) (64-bit)	Windows 10 x64
	86.0.4240.183 (Official Build) (64-bit)	Windows server 2012 R2 standard
	89.0.4389.128 (64-bit)	Windows 2019 Datacenter (64-bit)
	89.0.4389.114 (64-bit)	
	89.0.4389.114 (64-bit)	RHEL 7.6

Recommended Browser	Browser Version	Recommended Operating System
Mozilla Firefox	81.0.2(64 bit)	MacOS Catelina 10.15.7
	81.0.1(64 bit)	Windows 2016 Datacenter (64-bit)
	66.0.2 (64-bit)	Windows server 2012 R2 Standard
	68.6 (64-bit)	RHEL 8.2
	86.0.1 (64-bit)	Windows 2019 Datacenter (64-bit)
Safari	14.0.1	MacOS Catelina 10.15.7

Note If the management client is launched using an unsupported browser, check the help information from the `For best results use supported browsers` option available in the login window for the supported browser versions.

Transport Layer Security (TLS) version 1.2.

Hardware and Software Interoperability

For detailed information about storage switch, operating system and adapter, see the *Hardware and Software Interoperability Matrix* for your release located at:

http://www.cisco.com/en/US/products/ps10477/prod_technical_reference_list.html

Note Connectivity is tested between the server and the first connected device. Further connections, such as to storage arrays after a switch are not listed in the Cisco UCS Hardware Compatibility List though they may be highlighted in the vendor support matrix for those devices.

For details about transceivers and cables that are supported on VIC cards, see the Cisco Optics-to-Device Compatibility Matrix

You can also see the VIC data sheets for more compatibility information: Cisco UCS Virtual Interface Card Data Sheets

Upgrade Paths to Release 4.2

Cisco IMC 4.2(1a) release supports only Cisco UCS C220, C240 M6, and C245 M6 servers. Upgrade from any previous release is not applicable.

Cisco UCS C225 M6 servers are shipped with Cisco IMC 4.2(1c) release. Upgrade from any previous release is not applicable.

Refer to the table for upgrade options from Cisco IMC 4.2(1a) release:

Table 16: Upgrade Paths to Release 4.2

Server	Upgrade from Release	Upgrade to Release
Cisco UCS C220 M6	4.2(1a)	4.2(1b), 4.2(1e), 4.2(1f), and 4.2(1i)
Cisco UCS C240 M6	4.2(1a)	4.2(1b), 4.2(1e), 4.2(1f) and 4.2(1i)
Cisco UCS C245 M6	4.2(1a)	4.2(1g), 4.2(1c), 4.2(1e), 4.2(1f), 4.2(1g) and 4.2(1i)
Cisco UCS C225 M6	4.2(1c)	4.2(1e), 4.2(1f), 4.2(1g) and 4.2(1i)

Firmware Upgrade Details

Firmware Files

The C-Series software release 4.2(1) includes the following software files:

CCO Software Type	File name(s)	Comment
Unified Computing System (UCS) Server Firmware	ucs-c220m6-huu-4.2.1a.iso ucs-c240m6-huu-4.2.1a.iso ucs-c245m6-huu-4.2.1a.iso ucs-c225m6-huu-4.2.1c.iso For release specific ISO versions, see Cisco UCS C-Series Integrated Management Controller Firmware Files, Release 4.2	Host Upgrade Utility
Unified Computing System (UCS) Drivers	ucs-cxxx-drivers.4.2.1a.iso	Drivers
Unified Computing System (UCS) Utilities	ucs-cxxx-utils-efi.4.2.1a.iso ucs-cxxx-utils-linux.4.2.1a.iso ucs-cxxx-utils-vmware.4.2.1a.iso ucs-cxxx-utils-windows.4.2.1a.iso	Utilities

Note Always upgrade the BIOS, the Cisco IMC and CMC from the HUU ISO. Do not upgrade individual components (only BIOS or only Cisco IMC), since this could lead to unexpected behavior. If you choose to upgrade BIOS, and the Cisco IMC individually and not from the HUU ISO, make sure to upgrade both Cisco IMC, and BIOS to the same container release. If the BIOS and the Cisco IMC versions are from different container releases, it could result in unexpected behavior. Cisco recommends that you use the Update All option from the Host Upgrade Utility to update the firmware versions of Cisco IMC, BIOS, and all other server components (VIC, RAID Controllers, PCI devices, and LOM) together.

Host Upgrade Utility

The Cisco Host Upgrade Utility (HUU) is a tool that upgrades the Cisco UCS C-Series firmware.

The image file for the firmware is embedded in the ISO. The utility displays a menu that allows you to choose which firmware components to upgrade. For more information on this utility, see http://www.cisco.com/en/US/products/ps10493/products_user_guide_list.html.

For details of firmware files in Cisco Host Upgrade Utility for individual releases, see Cisco UCS C-Series Integrated Management Controller Firmware Files, Release 4.2.

Updating the Firmware

Use the Host Upgrade Utility to upgrade the C-Series firmware. Host Upgrade Utility can upgrade the following software components:

- BIOS
- Cisco IMC
- CMC
- Cisco VIC Adapters
- LSI Adapters
- LAN on Motherboard
- PCIe adapter firmware
- HDD firmware
- SAS Expander firmware
- DCPMM Memory

All firmware should be upgraded together to ensure proper operation of your server.

Note We recommend that you use the select all and **Update** or **Update & Activate All** option from the Host Upgrade Utility to update the firmware versions of Cisco IMC, BIOS and all other server components (VIC, RAID Controllers, PCI devices, and LOM) together. Click **Exit** once you deploy the firmware.

For more information on how to upgrade the firmware using the utility, see:

http://www.cisco.com/c/en/us/support/servers-unified-computing/ucs-c-series-rack-servers/products-user-guide-list.html

Software Utilities

The following standard utilities are available:

- Host Update Utility (HUU)
- BIOS and Cisco IMC Firmware Update utilities
- Server Configuration Utility (SCU)

- Server Diagnostic Utility (SDU)

The utilities features are as follows:

- Availability of HUU, SCU on the USB as bootable images. The USB also contains driver ISO, and can be accessed from the host operating system.

SNMP

The supported MIB definition for this release and later releases can be found at the following link:

ftp://ftp.cisco.com/pub/mibs/supportlists/ucs/ucs-C-supportlist.html

Note The above link is incompatible with IE 9.0.

New Software Features in Release 4.2

New Software Features in 4.2(1c)

The following new software features are supported in Release 4.2(1a):

- New BIOS tokens support for Cisco UCS C225 M6 servers
- **Shared OCP** and **Shared OCP Extended** NIC mode support.

New Software Features in 4.2(1b)

New BIOS token support for Cisco UCS C220 and C240 M6 servers:

- Enhanced CPU Performance (Default value - **Disabled**)
- Virtual Numa (Default value - **Disabled**)
- LLC Dead Line (Default value - **Enabled**)
- XPT Remote Refresh (Default value - **Auto**)
- UPI Link Enablement (Number of UPI Links Enabled) (Default value - **Auto**)
- UPI Power Management (Default value - **Disabled**)
- C1 Auto Demotion (Default value - **Enabled**)
- C1 Auto UnDemotion (Default value - **Enabled**)

New Software Features in 4.2(1a)

New Software Features in Release 4.2(1a)

The following new software features are supported in Release 4.2(1a):

- Release 4.2 introduces a new enhanced vKVM console for M6 platforms. For more details, see Cisco UCS C-Series Integrated Management Controller GUI Configuration Guide, Release 4.2 or Cisco UCS C-Series Servers Integrated Management Controller CLI Configuration Guide, Release 4.2.
- FlexMMC—Cisco UCS M6 servers support on-board 16GB hardware device attached to the BMC through eMMC bus interface. For more details, see Cisco UCS C-Series Integrated Management Controller GUI Configuration Guide, Release 4.2 or Cisco UCS C-Series Servers Integrated Management Controller CLI Configuration Guide, Release 4.2.
- Personality—Beginning with release 4.2(1a), users can configure personality of Cisco UCS M6 C-Series servers for use in HyperFlex (HX) using XML and Redfish API.
- Management Component Transport Protocol (MCTP) Security Protocol and Data Model (SPDM)—Cisco UCS M6 Servers might contain mutable components that could provide vectors for attack against a device itself or use of a device to attack another device within the system. To defend against these attacks, SPDM specification defines messages, data objects, and sequences for performing message exchanges between devices over a variety of transport and physical media. It orchestrates message exchanges between management controllers and end-point devices over MCTP. Message exchanges include authentication of hardware identities accessing the controller. The SPDM enables access to low-level security capabilities and operations by specifying a managed level for device authentication and certificate management.
- Autoconfiguration feature enables you to change the physical drive status auto config mode in the controller to any of the following values: **Unconfigured Good** - When the server is used for RAID volume and mixed JBOD.
  - RAID-0 Write Back - When the server is used for per drive R0 WB.
  - JBOD - When the server is used for JBOD only.

Note All the status of the unused physical drives changes when you select the appropriate option in the Auto Config mode.

- SNMP user can be created using the following authentication protocols:
  - HMAC_SHA96
  - HMAC128_SHA224
  - HMAC192_SHA256
  - HMAC256_SHA384
  - HMAC384_SHA512

  For more details see, Cisco UCS C-Series Servers REST API Programmer's Guide, Release 4.2

New Hardware Features in Release 4.2

New Hardware in Release 4.2(1g)

- Nvidia A16 PCIe FHFL (UCSC-GPU-A16) GPU support on Cisco UCS C245 M6 servers.

New Hardware Features in 4.2(1f)

- Intel X710-DA4 4x10GbE (UCSC-PCIE-IQ10GF) adapter support on Cisco UCS C245 M6 and UCS C225 M6 servers.

New Hardware Features in 4.2(1c)

- Cisco UCS C225 M6 Server—The Cisco UCS® C225 M6 Rack Server is the most versatile general-purpose infrastructure and application server in the industry. This high-density, 1RU, 2-socket rack server delivers industry-leading performance and efficiency for a wide range of workloads, including virtualization, EDA, SDS, big data, and edge-centric workloads. You can deploy the Cisco UCS C-Series rack servers as standalone servers or as part of the Cisco Unified Computing System™ with the Cisco Intersight Infrastructure Service cloud-based management platform.

  The Cisco UCS C225 M6 Rack Server has 3rd Gen AMD EPYC CPUs for the most cores per socket. Combined with PCIe 4.0 for peripherals and 3200 MHz DDR4 memory, you have significant performance and efficiency gains that will improve your application performance. Cisco UCS C225 M6 Rack Server is shipped with AMD Platform Secure Boot (PSB) feature that implements hardware-rooted boot integrity.

New Hardware in Release 4.2(1a)

- Cisco UCS C245 M6 Server—Cisco UCS C245 M6 Rack Server is well-suited for a wide range of storage and I/O-intensive applications such as big data analytics, databases, collaboration, virtualization, and server consolidation. The Cisco UCS C245 M6 Rack Server has 3rd Gen AMD EPYC CPUs for the most cores per socket. Combined with PCIe 4.0 for peripherals and 3200 MHz DDR4 memory, you have significant performance and efficiency gains that will improve your application performance. You can deploy the Cisco UCS C-Series rack servers as standalone servers or as part of the Cisco Unified Computing System™ with the Cisco Intersight Infrastructure Service cloud-based management platform. These computing innovations help reduce Total Cost of Ownership (TCO) and increase their business agility. These improvements deliver significant performance and efficiency gains that improve your application performance. The Cisco UCS C245 M6 Rack Server delivers outstanding levels of expandability, performance, and is shipped with AMD Platform Secure Boot (PSB) feature that implements hardware-rooted boot integrity.
- Cisco UCS C220 M6 Server—Cisco UCS C220 M6 Rack Server is the most versatile general-purpose infrastructure and application server in the industry. This high-density, 1RU, 2-socket rack server delivers industry-leading performance and efficiency for a wide range of workloads, including virtualization, collaboration, and bare-metal applications. You can deploy the Cisco UCS C-Series Rack Servers as standalone servers or as part of the Cisco Unified Computing System managed by Cisco Intersight, Cisco UCS Manager, or Intersight Managed Mode.
- Cisco UCS C240 M6 Server—Cisco UCS C240 M6 Rack Server is well-suited for a wide range of storage and I/O-intensive applications such as big data analytics, databases, collaboration, virtualization, consolidation, and high-performance computing in its two-socket, 2RU form factor. The Cisco UCS C240 M6 Server extends the capabilities of the Cisco UCS rack server portfolio with 3rd Gen Intel Xeon Scalable Processors supporting more than 43 percent more cores per socket and 33 percent more memory when compared with the previous generation. This provides up to 40 percent more performance than the M5 generation for your most demanding applications. You can deploy the Cisco UCS C-Series rack servers as standalone servers or as part of the Cisco Unified Computing System managed by Cisco Intersight, Cisco UCS Manager, or Intersight Managed Mode.
- Support for the following new UCS VIC 14xx Series adapters on Cisco UCS C220 M6 Server and Cisco UCS C240 M6 Server:

- VIC 1467 10/25G MLOM
- VIC 1477 40/100G MLOM

- SFP-10G-T-X transceiver is supported with VIC 1455/1457/1467 on ports 2 and 4 when in standby-power. When the server is fully powered-on, SFP-10G-T-X transceiver is enabled for all 4 ports. If user intents to mix cable types on a 1455/1457/1467 VIC card along with SFP-10G-T-X, ports 1 and 3 can support only passive copper cables (10/25G).

Security Fixes

Security Fixes in Release 4.2(1j)

Defect ID - CSCwb67205

Cisco UCS M6 servers are affected by vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) IDs:

- **CVE-2022-0005**—Sensitive information accessible by physical probing of JTAG interface for some Intel® Processors with SGX may allow an unprivileged user to potentially enable information disclosure through physical access.
- **CVE-2022-21136**—Improper input validation for some Intel® Xeon® Processors may allow a privileged user to potentially enable denial of service through local access.
- **CVE-2022-21151**—Processor optimization removal or modification of security-critical code for some Intel® Processors may allow an authenticated user to potentially enable information disclosure through local access.

Security Fixes in Release 4.2(1e)

The following Security Fixes were added in Release 4.2(1e):

Defect ID - CSCvz48570

Cisco UCS C-Series M6 servers, are affected by vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) IDs:

- CVE-2021-3711—Implementation of the SM2 decryption code that can lead to a buffer overflow when calling the API function to decrypt SM2 encrypted data. An attacker presenting a specially crafted SM2 content may be able to exploit the vulnerability and change application behavior or cause the application to crash.

  An attacker exploiting the vulnerability may be able to disclose private memory contents or perform a Denial of Service (DoS) attack.

This release includes SSL revisions for Cisco UCS M6 rack servers. These revisions include update for Cisco UCS M6 rack servers, which is a required part of the mitigation for these vulnerabilities.

Security Fixes in Release 4.2(1b)

The following Security Fixes were added in Release 4.2(1b):

Defect ID - CSCvy91321

Cisco Integrated Management Controller (IMC) Software are affected by vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) IDs:

- **CVE-2021-34736**—A vulnerability in the web-based management interface of Cisco Integrated Management Controller (IMC) Software could allow an unauthenticated, remote attacker to cause the web-based management interface to unexpectedly restart.

  The vulnerability is due to insufficient input validation on the web-based management interface. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause the interface to restart, resulting in a denial of service (DoS) condition.

  Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.

Resolved Caveats

The following section lists resolved caveats.

Resolved Caveats in 4.2(1i)

The following defect was resolved in Release 4.2(1i):

Table 17: Firmware Upgrade

Defect ID	Symptom	First Release Affected	Resolved in Release
CSCwb21128	Under certain conditions, the hard drive might experience long latency times, leading to undesirable results while working with latency-sensitive applications. This issue might happen with small block size and sequential writes. This issue is now resolved.	4.1(3d)	4.2(1i)

Table 18: BMC

Defect ID	Symptom	First Release Affected	Resolved in Release
CSCwb33753	During IMM deployment, auto-update of the device connector on a server might fail with the following error message: `Stderr: mount: can't setup loop device: No such file or directory` This issue is now resolved.	4.1(3f)	4.2(1i)

Resolved Caveats in 4.2(1f)

The following defect was resolved in Release 4.2(1f):

Table 19: BMC

Defect ID	Symptom	First Release Affected	Resolved in Release
CSCvz77885	In Cisco UCS M6 servers, Cisco IMC reboots unexpectedly due to Watchdog service reset. This issue is now resolved.	4.1(3d)	4.2(1f)

Resolved Caveats in 4.2(1e)

The following defect was resolved in Release 4.2(1e):

Table 20: BIOS

Defect ID	Symptom	First Release Affected	Resolved in Release
CSCvz36957	Server UUID set in the Server Profile of a Cisco UCS C-Series server is not displayed under the server inventory page. This issue is now resolved.	4.1(3d)	4.2(1e)

Resolved Caveats in 4.2(1c)

The following defect was resolved in Release 4.2(1c):

Table 21: BIOS

Defect ID	Symptom	First Release Affected	Resolved in Release
CSCvy45243	Guest VMs do not power on when there are more than 8 NVMe drives as pass-through. This issue is now resolved.	4.2(1c)	4.2(1c)

Resolved Caveats in 4.2(1b)

The following defect was resolved in Release 4.2(1b):

Table 22: BIOS

Defect ID	Symptom	First Release Affected	Resolved in Release
CSCvy22974	Cisco UCS M6 servers do not boot to Server Diagnostic Utility image while F7 option under the following conditions: • Boot mode is set to Legacy mode. • Image is mapped to vMedia. • SDU image is mapped with vKVM. This issue is now resolved	4.2(1a)	4.2(1b)
CSCvy53138	TME does not get enabled through UCSM BIOS policy. This issue is now resolved	4.2(1a)	4.2(1b)

Table 23: BMC

Defect ID	Symptom	First Release Affected	Resolved in Release
CSCvy50012	Redfish API fails to configure NTP with IPv6 address. This issue is now resolved	4.1(3b)	4.2(1b)

Defect ID	Symptom	First Release Affected	Resolved in Release
CSCvy87338	Deleting or terminating Redfish API session fails when performed using **logout()** method from the Redfish Python library. HTTP response code 404 is seen. This issue is now resolved	4.2(1a)	4.2(1b)

Open Caveats

The following section lists open caveats.

Open Caveats in Release 4.2(1g)

The following defects are open in Release 4.2(1g):

Table 24: CPU

Defect ID	Symptom	Workaround	First Affected Release
CSCwa58957	Intel X710-DA2 Dual Port 10Gb SFP+ adapters placed in slots 4, 5, or 6 connected to CPU 2 of the Cisco UCS C245 M6 servers start operating at lower speeds (2.5 GT/s) with partial loss of functionality after multiple server reboots. This issue is encountered infrequently. It is not observed on slots 1,2, or 3 connected to CPU 1.	Perform one of the following: • Reboot the server. • Move the adapter to slot 1, 2 or 3, if available.	4.2(1g)

Open Caveats in Release 4.2(1c)

The following defects are open in Release 4.2(1c):

Table 25: BIOS

Defect ID	Symptom	Workaround	First Affected Release
CSCvz11112	In Cisco UCS C225 M6 servers, under certain conditions, when the OS ISO image file is large, it slows the packet transfer through HTTP boot and results in **Dracut** error. This results in OS installation failure.	You may try a different environment to successfully install the OS or choose installation for specific flavor, which has lower OS ISO image size.	4.2(1c)
CSCvz28553	In Cisco UCS C245 M6 servers equipped with Cisco VIC 1495 in slot 4 and running RHEL OS, Consistent Device Naming (CDN) name from Cisco IMC does not get correctly reported and appears differently in the OS.	You may use Cisco VIC 1455 card Riser 1, slot 1.	4.2(1c)
CSCvy17163	In Cisco UCS C245 M6 servers, NVMe drives do not come back online automatically after being removed using the **Devices and Printers** icon option.	Remove the drive after ejecting from Windows desktop bottom task bar.	4.2(1c)
CSCvz22293	In Cisco UCS C225 M6 servers, NVMe drives discovery takes a long time after hot plug.	There is no functionality impact. Discovery does happen correctly.	4.2(1c)

Defect ID	Symptom	Workaround	First Affected Release
CSCvz11112	Dracut error is observed while installing RHEL OS release 7.x and 8.x on Cisco UCS C225 M6 servers.	Use the following as an example to point to the HTTP URL of the DVD ISO image: When the ISO is mounted into `/var/www/html/rhel8` directory on the HTTP server: inst.stage2=http://<SERVER_IP>/rhel8; the same option can also be added to the installation specific steps for HTTP boot/install on Cisco UCS C226 M6 servers. In RHEL GUI interface, while selecting the software to install, ensure that you give the path of the HTTP extracted ISO as the installation source. For example: `Http://<SERVER_IP>/rhel8/`	4.2(1c)

Open Caveats in Release 4.2(1b)

The following defects are open in Release 4.2(1b):

Table 26: BMC

Defect ID	Symptom	Workaround	First Affected Release
CSCvy51101	In Cisco UCS C-Series M6 servers, when the OS .ISO file name is longer than 48 characters, un-mapping the .iso file from Ciso IMC GUI or using Redfish API request (**VirtualMedia.EjectMedia**) fails with the following error message: `No such volume` This issue has no impact on OS installation process.	Un-map the OS .ISO file using KVM. On the KVM window, from the left vertical panel, hover the cursor over **Virtual Media** and click the volume name which you wish to un-map.	4.2(1b)

Open Caveats in Release 4.2(1a)

The following defects are open in Release 4.2(1a):

Table 27: BMC

Defect ID	Symptom	Workaround	First Affected Release
CSCvy51101	When the ISO file name is longer than 48 characters, un-mapping the ISO fails from Cisco IMC GUI or Redfish request (VirtualMedia.EjectMedia) with the following error: `No such volume` This issue is seen in Cisco UCS M6 servers when OS installation is invoked using Redfish request (CiscoUCSExtensions. PrepareOSInstall). This issue does not impact OS installation process.	Un-map OS ISO from KVM. On KVM Window, from the left panel, hover the cursor over **Virtual Media** and click the volume name to un-map.	4.2(1a)

Table 28: BMC Storage

Defect ID	Symptom	Workaround	First Affected Release
CSCvy27706	In Cisco UCS C240 M6 server, Cisco IMC displays drives 1-12 under MRAID2 and drives 13-24 under MRAID1.	This issue has no functional impact. Slot numbers automatically get refresh on next reboot.	4.2(1a)

Table 29: External LSI SAS Controller

Defect ID	Symptom	Workaround	First Affected Release
CSCvv80103	In Cisco UCS C240 M6 servers, un-configured drives change to un-configured bad when they are used to create a RAID volume.	Perform one of the following: • Use **storcli** and restart the controller online. • Reboot the host. • Hot remove and insert the drive.	4.2(1a)
CSCvy51539	In Cisco UCS C220 M6 servers, storage controller fail to respond to CLI and LSA initiated commands after being idle for a certain period of time.	Reboot the host.	4.2(1a)
CSCvy26147	In a Cisco UCS C240 M6 server with dual UCSC-SAS-M6T card configured in legacy boot mode, drives in MRAID1 are not listed in Legacy OPROM dispatch after the link is disabled.	After replacing the adapters, ensure that the host is powered off and on. Reboot only with both the controller inserted.	4.2(1a)

Known Behaviors and Limitations

Known Behaviors and Limitations in Release 4.2(1i)

The following caveats are known limitations in release 4.2(1i):

Table 30: BMC

Defect ID	Symptom	Workaround	First Affected Release
CSCwb01860	In Cisco UCS M6 servers, storage firmware downgrade fails with the following message: `Failed: flash image not supported` This issue occurs in Cisco UCS M6 servers equipped with the following: • Adaptors with PCIe vendor id 1000h and device id 10E2h • Firmware: MR 7.20 and above in the system and downgraded to 7.19 or below	Upgrade to the latest patch that contains the storage firmware version 7.20.	4.2(1i)

Known Behaviors and Limitations in Release 4.2(1f)

The following caveats are known limitations in release 4.2(1f):

Table 31: BIOS

Defect ID	Symptom	Workaround	First Affected Release
CSCwb11720	In Cisco UCS C245 M6 servers, Cisco IMC shows the following alarm after upgrading from 4.2(1a) release to 4.2(1f) release: `BIOS_IMAGE_CORRUPTED [F1935][major][BIOS-Image-Corrupted][sys/rack-unit-1/board] BIOS FD0 Verification Failed. Please update and reactivate BIOS` This alarm has no functionality impact and gets cleared.	No known workaround. This issue has no functionality impact.	4.2(1f)

Known Behaviors and Limitations in Release 4.2(1c)

The following caveats are known limitations in release 4.2(1c):

Table 32: BMC

Defect ID	Symptom	Workaround	First Affected Release
CSCvy89810	In Cisco UCS C245 M6 servers, if **NIC Mode** is configured as **Shared OCP Extended**, then BMC becomes inaccessible after downgrading to release 4.2(1a).	Perform the following steps to recover the Cisco IMC network: **1.** Connect the local monitor to VGA port. **2.** Reboot the host using the power button. **3.** During the boot up, enter the **F8** (Cisco IMC Configuration Utility) and choose **Factory Defaults** option. **4.** Press **F10** to save. Cisco IMC reboots to factory default settings. If VIC is populated in the supported riser slots, **NIC Mode** switches to **Cisco Card** mode. If there is no VIC, **NIC mode**switches to **Dedicated** mode. Reboot the host again and enter the **F8** utility to configure the network settings.	4.2(1c)

Known Behaviors and Limitations in Release 4.2(1a)

The following caveats are known limitations in release 4.2(1a):

Table 33: BMC

Defect ID	Symptom	Workaround	First Affected Release
CSCvw20909	Mixed mode configuration is not allowed for Intel Persistent Memory in all Cisco UCS M6 servers.	No known workaround	4.2(1a)

Defect ID	Symptom	Workaround	First Affected Release
CSCvu99928	In Cisco UCS M6 servers, Old SSH client fails to connect to Cisco IMC when FIPS is enabled.	Upgrade SSH client from Version 5.3 to Version 5.7 or above.	4.1(3b)

Related Documentation

For configuration information for this release, refer to the following:

- Cisco UCS C-Series Servers Integrated Management Controller CLI Configuration Guide
- Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide
- Cisco UCS Rack-Mount Servers Cisco IMC API Programmer's Guide

For information about installation of the C-Series servers, refer to the following:

- Cisco UCS C-Series Rack Servers Install and Upgrade Guides

The following related documentation is available for the Cisco Unified Computing System:

- Regulatory Compliance and Safety Information for Cisco UCS
- For information about 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.

Refer to the release notes for Cisco UCS Manager software and the *Cisco UCS C Series Server Integration with Cisco UCS Manager Guide* at the following locations:

- Cisco UCS Manager Release Notes
- Cisco UCS C Series Server Integration with Cisco UCS Manager Guides