Release Notes for Cisco UCS Rack Server Software, Release 4.2(3)

First Published: 2023-01-06

Last Modified: 2024-04-16

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(3) 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 29 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	April 16, 2024	Created release notes for 4.2(3k) for the following servers: Cisco UCS S3260 M5 servers This patch contains fixes and firmware updates for Cisco UCS S3260 M5 server.

Revision	Date	Description
G0	February 21, 2024	Created release notes for 4.2(3j) for the following servers: Cisco UCS C220 M6, C225 M6, C240 M6, and C245 M6 servers Cisco UCS C220 M5, C240 M5, C480 M5, C480 ML M5, S3260 M4, S3260 M5, and C125 M5 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	November 06, 2023	Created release notes for 4.2(3i) for the following servers: Cisco UCS C220 M6, C225 M6, C240 M6, and C245 M6 servers Cisco UCS C220 M5, C240 M5, C480 M5, C480 ML M5, S3260 M4, S3260 M5, and C125 M5 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
A1	October 20, 2023	Updated the **Open Caveats** section for the release 4.2(3b).

Revision	Date	Description
E0	September 28, 2023	Created release notes for 4.2(3h) for the following servers: Cisco UCS C220 M6, C225 M6, C240 M6, and C245 M6 servers Cisco UCS C220 M5, C240 M5, C480 M5, C480 ML M5, S3260 M4, S3260 M5, and C125 M5 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
D0	July 17, 2023	Created release notes for 4.2(3g) for the following servers: Cisco UCS C220 M6, C225 M6, C240 M6, and C245 M6 servers Cisco UCS C220 M5, C240 M5, C480 M5, C480 ML M5, S3260 M4, S3260 M5, and C125 M5 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
C0	May 15, 2023	Created release notes for 4.2(3e) for the following servers: Cisco UCS C220 M6, C225 M6, C240 M6, and C245 M6 servers Cisco UCS C220 M5, C240 M5, C480 M5, C480 ML M5, S3260 M4, S3260 M5, and C125 M5 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

Revision	Date	Description
B0	March 20, 2023	Created release notes for 4.2(3d) for the following servers: Cisco UCS C220 M6, C225 M6, C240 M6, and C245 M6 servers Cisco UCS C220 M5, C240 M5, C480 M5, C480 ML M5, S3260 M4, S3260 M5, and C125 M5 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	January 6, 2023	Created release notes for 4.2(3b) for the following servers: Cisco UCS C220 M6, C225 M6, C240 M6, and C245 M6 servers Cisco UCS C220 M5, C240 M5, C480 M5, C480 ML M5, S3260 M4, S3260 M5, and C125 M5 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
- Cisco UCS C220 M5
- Cisco UCS C240 M5
- Cisco UCS C240 SD M5

- Cisco UCS S3260 M5
- Cisco UCS C480 M5
- Cisco UCS C480 M5 ML
- Cisco UCS C125 M5
- Cisco UCS S3260 M4

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, UCSM end-user interface is used to manage the server.

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(3) Release

Cisco IMC Release	Cisco UCS Manager Release	Rack Mount Servers
4.2(3k)	NA	Cisco UCS S3260 M5 servers
4.2(3j)	4.2(3j)	Cisco UCS C220 M6, C225 M6, C240 M6, and C245 M6 servers Cisco UCS C220 M5, C240 M5, C240 SD M5, C480 M5, C480 ML M5, S3260 M4, S3260 M5, and C125 M5 servers
4.2(3i)	4.2(3i)	Cisco UCS C220 M6, C225 M6, C240 M6, and C245 M6 servers Cisco UCS C220 M5, C240 M5, C240 SD M5, C480 M5, C480 ML M5, S3260 M4, S3260 M5, and C125 M5 servers
4.2(3g)	4.2(3g)	Cisco UCS C220 M6, C225 M6, C240 M6, and C245 M6 servers Cisco UCS C220 M5, C240 M5, C240 SD M5, C480 M5, C480 ML M5, S3260 M4, S3260 M5, and C125 M5 servers
4.2(3e)	4.2(3e)	Cisco UCS C220 M6, C225 M6, C240 M6, and C245 M6 servers Cisco UCS C220 M5, C240 M5, C240 SD M5, C480 M5, C480 ML M5, S3260 M4, S3260 M5, and C125 M5 servers

Cisco IMC Release	Cisco UCS Manager Release	Rack Mount Servers
4.2(3d)	4.2(3d)	Cisco UCS C220 M6, C225 M6, C240 M6, and C245 M6 servers Cisco UCS C220 M5, C240 M5, C240 SD M5, C480 M5, C480 ML M5, S3260 M4, S3260 M5, and C125 M5 servers
4.2(3b)	4.2(3b)	Cisco UCS C220 M6, C225 M6, C240 M6, and C245 M6 servers Cisco UCS C220 M5, C240 M5, C240 SD M5, C480 M5, C480 ML M5, S3260 M4, S3260 M5, and C125 M5 servers

Table 2: Cisco IMC and UCS Manager Software Releases for Rack Mount Servers for Cisco IMC 4.2(2) Release

Cisco IMC Release	Cisco UCS Manager Release	Rack Mount Servers
4.2(2g)	4.2(2d)	Cisco UCS C220 M6, C225 M6, C240 M6, and C245 M6 servers Cisco UCS C220 M5, C240 M5, C240 SD M5, C480 M5, C480 ML M5, S3260 M4, S3260 M5, and C125 M5 servers
4.2(2f)	4.2(2c)	Cisco UCS C220 M6, C225 M6, C240 M6, and C245 M6 servers Cisco UCS C220 M5, C240 M5, C240 SD M5, C480 M5, C480 ML M5, S3260 M4, S3260 M5, and C125 M5 servers
4.2(2a)	4.2(2a)	Cisco UCS C220 M6, C225 M6, C240 M6, and C245 M6 servers Cisco UCS C220 M5, C240 M5, C240 SD 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 4.2(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

Cisco IMC Release	Cisco UCS Manager Release	Rack Mount 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

Table 4: 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(3n)	NA	Cisco UCS C220 M5, C240 M5, C480 M5, S3260 M5 and S3260 M4 servers
4.1(3m)	4.1(3m)	Cisco UCS C220 M5, C240 M5, C480 M5, S3260 M5 and S3260 M4 servers
4.1(3l)	4.1(3k)	Cisco UCS C480 M5, C220 M5, C240 M5 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
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

Cisco IMC Release	Cisco UCS Manager Release	Rack Mount 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 5: 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(2m)	No Support	Cisco UCS C220 M4, C240 M4 and C460 M4 servers.
4.1(2l)	No Support	Cisco UCS C220 M4 and C240 M4 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 6: 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 7: 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 8: 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 9: 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 10: 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

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(3):

Recommended Browser	Minimum Recommended Browser Version	Minimum Recommended Operating System
Microsoft Edge	95.0.1020.53(Official Build) (64-bit)	Microsoft Windows 10 x64
	98.0.1108.50 (Official build) (64-bit)	Microsoft Windows 10 x64
Google Chrome	96.0.4664.45	
	96.0.4664.45 (Official Build) (64-bit)	
	94.0.4606.71 (Official Build) (64-bit)	
Mozilla Firefox	94.0.2 Build ID: 20211119140621	MAC Monterey v.12.0.1
	97.0.1	Microsoft Windows 10 x64
	78.9.0 ESR (64-bit)	RHEL 8.4
Safari	14.1.2 (16611.3.10.1.6)	MAC Monterey v.12.0.1
	15.1 (17612.2.9.1.20)	

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

Default Ports

Following is a list of server ports and their default port numbers:

Table 11: Server Ports

Port Name	Port Number
LDAP Port 1	389
LDAP Port 2	389
LDAP Port 3	389
LDAP Port 4	3268
LDAP Port 5	3268
LDAP Port 6	3268
SSH Port	22
HTTP Port	80
HTTPS Port	443
SMTP Port	25
KVM Port	2068
Intersight Management Port	8889
Intersight Cloud Port	8888

Port Name	Port Number
SOL SSH Port	2400
SNMP Port	161
SNMP Traps	162
External Syslog	514

Upgrade and Downgrade Guidelines

To get a complete overview of all the possible upgrade paths in Cisco IMC, see Cisco UCS Rack Server Upgrade Support Matrix.

Note Before downgrading from release 4.2(3d), ensure to change the LUNs per target configuration to [1-1024].

Upgrade Paths to Release 4.2

The section provides information on the upgrade paths to release 4.2.

Refer to the table for upgrade paths for various Cisco UCS C-series IMC versions.

Table 12: Upgrade Paths to Release 4.2(3x)

Upgrade From Release	Upgrade To Release	Recommended Upgrade Path
4.2(3b)	• 4.2(3j) • 4.2(3i) • 4.2(3h) • 4.2(3h) • 4.2(3g) • 4.2(3e) • 4.2(3d)	Follow below upgrade path: • You can use Interactive HUU or Non-Interactive HUU (NIHUU) script to update the server. • While updating the firmware using the NIHUU tool, use the Python scripts that are released with version 4.2(3b). • Use OpenSSL 1.0.1e-fips on the client side (where the NIHUU python scripts are running). • Download HUU iso from here. • Download NIHUU script from here.

Upgrade From Release	Upgrade To Release	Recommended Upgrade Path
• Cisco UCS C220 M6 • Cisco UCS C240 M6 • Cisco UCS C245 M6 • Cisco UCS C225 M6 • 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 • Cisco UCS S3260 M4	• 4.2(3j) • 4.2(3i) • 4.2(3h) • 4.2(3g) • 4.2(3e) • 4.2(3d) • 4.2(3b)	Follow below upgrade path: • You can use Interactive HUU or Non-Interactive HUU (NIHUU) script to update the server. • While updating the firmware using the NIHUU tool, use the Python scripts that are released with version 4.2(2). • Use OpenSSL 1.0.1e-fips on the client side (where the NIHUU python scripts are running). • Download HUU iso from here. • Download NIHUU script from here.
All Cisco UCS M6 Servers from 4.2(1). For the list of supported platforms, see Table 13: Upgrade Paths to Release 4.2(1a), on page 17.	• 4.2(3j) • 4.2(3i) • 4.2(3h) • 4.2(3g) • 4.2(3e) • 4.2(3d) • 4.2(3b)	Follow below upgrade path: • You can use Interactive HUU or Non-Interactive HUU (NIHUU) script to update the server. • While updating the firmware using the NIHUU tool, use the Python scripts that are released with version 4.2(1). • Use OpenSSL 1.0.1e-fips on the client side (where the NIHUU python scripts are running). • Download HUU iso from here. • Download NIHUU script from here.

Upgrade From Release	Upgrade To Release	Recommended Upgrade Path
Following Cisco UCS Servers from 4.1(3): • 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 • Cisco UCS S3260 M4	• 4.2(3j) • 4.2(3i) • 4.2(3h) • 4.2(3g) • 4.2(3e) • 4.2(3d) • 4.2(3b)	Follow below upgrade path: • You can use Interactive HUU or NIHUU script to update the server. • While updating the firmware using the NIHUU tool, use the Python scripts that are released with version 4.1(3). • Use OpenSSL 1.0.1e-fips on the client side (where the NIHUU python scripts are running). • Download HUU iso from here. • Download NIHUU script from here.
Following Cisco UCS Servers from 4.1(2): • 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 • Cisco UCS S3260 M4	• 4.2(3j) • 4.2(3i) • 4.2(3h) • 4.2(3g) • 4.2(3e) • 4.2(3d) • 4.2(3b)	Follow below upgrade path: • You can use Interactive HUU or Non-Interactive HUU (NIHUU) script to update the server. • While updating the firmware using the NIHUU tool, use the Python scripts that are released with version 4.1(2). • Use OpenSSL 1.0.1e-fips on the client side (where the NIHUU python scripts are running). • Download HUU iso from here. • Download NIHUU script from here.

Upgrade From Release	Upgrade To Release	Recommended Upgrade Path
Following Cisco UCS Servers from 4.1(1): • Cisco UCS C220 M5 • Cisco UCS C240 M5 • Cisco UCS C480 M5 • Cisco UCS C480 M5 ML • Cisco UCS S3260 M5 • Cisco UCS C125 M5 • Cisco UCS S3260 M4	• 4.2(3j) • 4.2(3i) • 4.2(3h) • 4.2(3g) • 4.2(3e) • 4.2(3d) • 4.2(3b)	Follow below upgrade path: • You can use Interactive HUU or Non-Interactive HUU (NIHUU) script to update the server. • While updating the firmware using the NIHUU tool, use the Python scripts that are released with version 4.1(1). • Use OpenSSL 1.0.1e-fips on the client side (where the NIHUU python scripts are running). • Download HUU iso from here. • Download NIHUU script from here.
Following Cisco UCS Servers from 4.0(4): • Cisco UCS C220 M5 • Cisco UCS C240 M5 • Cisco UCS C480 M5 • Cisco UCS C480 M5 ML • Cisco UCS S3260 M4	• 4.2(3j) • 4.2(3i) • 4.2(3h) • 4.2(3g) • 4.2(3e) • 4.2(3d) • 4.2(3b)	Follow below upgrade path: • You can use Interactive HUU or Non-Interactive HUU (NIHUU) script to update the server. • While updating the firmware using the NIHUU tool, use the Python scripts that are released with version 4.0(4). • Use OpenSSL 1.0.1e-fips on the client side (where the NIHUU python scripts are running). • Download HUU iso from here. • Download NIHUU script from here.

Table 13: Upgrade Paths to Release 4.2(1a)

Upgrade From Release	Upgrade To Release	Recommended Upgrade Path
Cisco UCS C220 M6	4.2(1a)	4.2(1b), 4.2(1e), and 4.2(1f)
Cisco UCS C240 M6	4.2(1a)	4.2(1b), 4.2(1e), and 4.2(1f)
Cisco UCS C225 M6	4.2(1a)	4.2(1c), 4.2(1e), 4.2(1f), and 4.2(1g)
Cisco UCS C245 M6	4.2(1c)	4.2(1e), 4.2(1f), and 4.2(1g)

Firmware Upgrade Details

Firmware Files

The C-Series software release 4.2(3) includes the following software files:

CCO Software Type	File name(s)	Comment
Unified Computing System (UCS) Server Firmware	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.4.2.3b.iso	Drivers
Unified Computing System (UCS) Utilities	ucs-cxxx-utils-efi.4.2.3b.iso ucs-cxxx-utils-linux.4.2.3b.iso ucs-cxxx-utils-vmware.4.2.3b.iso ucs-cxxx-utils-windows.4.2.3b.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
- Storage controller firmware

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

Note We recommend that you use **Update & Activate** 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. To force update the component, toggle **Advance mode** and select the required firmware component and click **Update & Activate**. Click **Power Cycle** icon 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

SNMP

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

https://cisco.github.io/cisco-mibs/

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.

New Hardware in Release 4.2

New Hardware in Release 4.2(3k)

There are no new hardware features introduced for this release.

New Hardware in Release 4.2(3j)

There are no new hardware features introduced for this release.

New Hardware in Release 4.2(3i)

There are no new hardware features introduced for this release.

New Hardware in Release 4.2(3h)

There are no new hardware features introduced for this release.

New Hardware in Release 4.2(3g)

There are no new hardware features introduced for this release.

New Hardware in Release 4.2(3e)

Support for the following on Cisco UCS M6 servers:

- Cisco-NVDA MCX631432AC-ADAB CX6 Lx 2x25G SFP28 x8 OCP NIC
- Cisco-NVDA MCX623436AC-CDAB CX6 Dx 2x100G QSFP56 x16 OCP NIC

New Hardware in Release 4.2(3d)

Peripherals

Support for the following:

- Support for 1200W Artesyn and Lite-On Power Supply Units on Cisco UCS M6 servers.

New Hardware in Release 4.2(3b)

Peripherals

Support for the following:

- Support for UCS VIC 15238 on Cisco UCS M6 servers.
- Solidigm (Formerly Intel) P5520 and P5620 QLC 15TB

New Software Features in Release 4.2

New Software Features in Release 4.2(3k)

There are no new software features introduced for this release.

New Software Features in Release 4.2(3j)

There are no new software features introduced for this release.

New Software Features in Release 4.2(3i)

There are no new software features introduced for this release.

New Software Features in Release 4.2(3h)

There are no new software features introduced for this release.

New Software Features in Release 4.2(3g)

There are no new software features introduced for this release.

New Software Features in Release 4.2(3d)

The following new software features are supported in Release 4.2(3d):

- Data Sanitization - Beginning with release 4.2(3d), Cisco IMC supports data sanitization feature. Using the data sanitization process, Cisco IMC erases all sensitive data, thus making extraction or recovery of customer data impossible. As Cisco IMC progresses through the erase process, the status report is updated. You can check the status and progress of the data sanitization process for each individual device erase from the report, identify and rectify any issues, if required.

  Erase process for data sanitization is performed in the following order on the server components:

  - Storage
  - VIC
  - BIOS
  - Cisco IMC

  You can choose to either perform data sanitization on all the server components or select only VIC and Storage components for data sanitization.

  Cisco IMC reboots when the data sanitization process is completed and generates a report.

  For more details, see Cisco UCS C-Series Servers REST API Programmer's Guide, Release 4.3.

Note

- This feature is supported only on Redfish API interface.
- This feature is supported on Cisco UCS C-series M5 and M6 servers.

- Maximum LUNs per target has increased from [1-1024] to [1-4096] for Linux and ESX OS for 13xx, 14xx, 15xxx VIC adapters.

  This change is applicable to vHBA type FC Initiator only. ESX 7.x and ESX 8.0 supports a total of 1024 LUNs per host.

Note Before downgrading from release 4.2(3d), ensure to change the LUNs per target configuration to [1-1024].

Security Fixes in Release 4.2

Security Fixes in Release 4.2(3j)

Defect ID - CSCwh68315

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

- **CVE-2023-23583**—Sequence of processor instructions leads to unexpected behavior in some Intel(R) processors and may allow an authenticated user to potentially enable escalation of privilege and information disclosure and denial of service through local access.

Security Fixes in Release 4.2(3h)

Defect ID - CSCwf30460

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

- **CVE-2022-41804**—Unauthorized error injection in Intel(R) SGX or Intel(R) TDX for some Intel(R) Xeon(R) Processors which may allow a privileged user to potentially enable escalation of privilege through local access.
- **CVE-2022-40982**—Information exposure through microarchitectural state after transient execution in certain vector execution units for some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure through local access.
- **CVE-2023-23908**—Improper access control in some 3rd Generation Intel(R) Xeon(R) Scalable processors may allow a privileged user to potentially enable information disclosure through local access.
- **CVE-2022-37343**— Improper access control in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege through local access.

Defect ID - CSCwf30468

Cisco UCS M5 C-series servers are affected by vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) IDs:

- **CVE-2022-40982**—Information exposure through microarchitectural state after transient execution in certain vector execution units for some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure through local access.
- **CVE-2022-43505**—Insufficient control flow management in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable denial of service through local access.

Security Fixes in Release 4.2(3d)

Defect ID - CSCwc73237

Cisco UCS C-series M6 servers based on Intel® Whitley Processors (Ice Lake), are affected by vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) IDs:

- **CVE-2022-21216**—Insufficient granularity of access control in out-of-band management in some Intel® Atom and Intel Xeon Scalable Processors may allow a privileged user to potentially enable escalation of privilege through adjacent network access.
- **CVE-2022-33196**— Incorrect default permissions in some memory controller configurations for some Intel® Xeon® Processors when using Intel® Software Guard Extensions which may allow a privileged user to potentially enable escalation of privilege through local access.
- **CVE-2022-38090**—Improper isolation of shared resources in some Intel® Processors when using Intel® Software Guard Extensions may allow a privileged user to potentially enable information disclosure through local access.
- **CVE-2022-33972**—Incorrect calculation in microcode keying mechanism for some 3rd Generation Intel® Xeon® Scalable Processors may allow a privileged user to potentially enable information disclosure through local access.
- **CVE-2022-32231**— Improper initialization in the BIOS firmware for some Intel® Processors may allow a privileged user to potentially enable escalation of privilege through local access.
- **CVE-2021-0187**—Improper access control in the BIOS firmware for some Intel® Processors may allow a privileged user to potentially enable an escalation of privilege through local access.
- **CVE-2022-26837**— Improper input validation in the BIOS firmware for some Intel® Processors may allow a privileged user to potentially enable escalation of privilege through local access.
- **CVE-2022-36348**—Active debug code in some Intel® SPS firmware before version SPS_E5_04.04.04.300.0 might allow an authenticated user to potentially enable escalation of privilege through local access.

Defect ID - CSCwd61013

Cisco UCS C-series M5 servers based on Intel® Purley Processors are affected by vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) IDs:

- **CVE-2022-26343**—Improper access control in the BIOS firmware for some Intel® Processors may allow a privileged user to potentially enable escalation of privilege through local access.
- **CVE-2022-32231**— Improper initialization in the BIOS firmware for some Intel® Processors may allow a privileged user to potentially enable escalation of privilege through local access.

Open Caveats in Release 4.2

Open Caveats in 4.2(3e)

The following defects are open in Release 4.2(3e):

Table 14: BMC

Defect ID	Symptom	Workaround	First Affected Release
CSCwe64856	In Cisco UCS S3260 M5 servers, resetting VIC adapters to factory default using CLI fails and the process remains in pending state.	Use Cisco IMC GUI or perform AC cycle in CLI to recover the process.	4.2(3e)

Open Caveats in 4.2(3b)

The following defect is open in Release 4.2(3b):

Table 15: VIC Firmware

Defect ID	Symptom	Workaround	First Affected Release
CSCwh06536	The links with SFP-10G-T-X are up on VIC 14xx series adapters from the VIC firmware version 5.2(2b). However, the links with SFP-10G-T-X on VIC 14xx series adapters are down after upgrading the VIC firmware version to 5.2(3b) or later from the version 5.2(2b).	Use the firmware version 5.2(2b).	4.2(3b)

Resolved Caveats

Resolved Caveats in Release 4.2(3j)

The following defect was resolved in Release 4.2(3j):

Defect ID	Symptom	First Release Affected	Resolved in Release
CSCwf93621	In Cisco UCS C240 M5SX and UCS HX240c M5SX servers, when the firmware is upgraded to the release 4.2(3d), discovery or association is failing with a faulty drive in the system. This issue is now resolved.	4.2(3d)	4.2(3j)

Resolved Caveats in Release 4.2(3i)

The following defects were resolved in Release 4.2(3i):

Table 16: VIC Firmware

Defect ID	Symptom	First Release Affected	Resolved in Release
CSCwb82433	Cisco UCS C220 M5 servers, equipped with Cisco UCS VIC 1400 series adapter and have **Geneve** feature enabled, go offline after the Cisco UCS VIC adapters fail to respond. This issue is now resolved.	4.2(1d)	4.2(3i)

Resolved Caveats in Release 4.2(3h)

The following defect was resolved in Release 4.2(3h):

Table 17: BMC

Defect ID	Symptom	First Release Affected	Resolved in Release
CSCwe92151	When some specific model of HDDs are inserted or the drives are initialized during any operation in a Cisco UCS C-series M6 or M7 server, the server automatically powers ON from OFF state. This causes low level firmware update failure. This issue is now resolved.	4.3.2.230207	4.2(3h)

Resolved Caveats in Release 4.2(3g)

The following defects were resolved in Release 4.2(3g):

Table 18: BMC

Defect ID	Symptom	First Release Affected	Resolved in Release
CSCwd46043	During regular operation of the Cisco UCS C240 M5 server, Cisco IMC might lose management plane connectivity. There might not be impact on the data plane as the Cisco IMC (management plane) is the affected component and the connectivity is restored on its own. This issue is now resolved.	4.2(2a)	4.2(3g)
CSCwe33951	In Cisco UCS M5 servers managed by Cisco UCS Manager or Intersight, sudden critical alerts for inventory mismatch (listed below) are displayed: • DIMM inventory mismatch • CPU inventory mismatch • Server hardware inventory mismatch These critical alerts are cosmetic in nature and do not impact the operation of the server. This issue is now resolved.	4.2(2a)	4.2(3g)

Defect ID	Symptom	First Release Affected	Resolved in Release
CSCwe61589	In Cisco UCS C220 M5 servers, Intelligent Platform Management Interface (IPMI) goes into a constant restart loop after application stall messages, causing IPMI management to fail. This issue is now resolved.	4.1(3c)	4.2(3g)
CSCwe64856	In Cisco UCS S3260 M5 servers, reset factory default of VIC adapter fails and and is hung in pending state. This issue is now resolved.	4.2(3d)	4.2(3g)

Resolved Caveats in Release 4.2(3d)

The following defects were resolved in Release 4.2(3d):

Table 19: BMC

Defect ID	Symptom	First Release Affected	Resolved in Release
CSCwd90347	On hot removal or insertion of NVMe drive, the Redfish PCI inventory does not get updated. The sameinventory is updated in other Cisco IMC interfaces (GUI or CLI). This issue is now resolved.	4.2(3b)	4.2(3d)
CSCwc12006	In Cisco UCS S3260 servers, Cisco UCS Manager generates error in power state when chassis 2 is redundancy-degraded and auto clears. This issue is now resolved.	4.0(4a)	4.2(3d)

Table 20: ext-intel-cntrlr

Defect ID	Symptom	First Release Affected	Resolved in Release
CSCwd49108	NIC card does not detect the ports after updating the firmware version from 4.2(1b) to 4.2(2a). Intel has removed the support for "FC-FEC" from the Intel E810-XXVDA2 firmware in 4.2(2a) release. You might run into link down issue if the switches do not support "RS-FEC", recommended for 25G/s ethernet connections. This issue is now resolved.	4.2(3b)	4.2(3d)

Resolved Caveats in Release 4.2(3b)

The following defects were resolved in Release 4.2(3b):

Table 21: Host Firmware Upgrade

Defect ID	Symptom	First Release Affected	Resolved in Release
CSCwc44412	Activity LED on Solidigm (Formerly Intel) P5520, P5620 and P5316 QLC drives is off when it is plugged in and the server is idle. The LED does not blink on the drive even though the drive is running. This issue is now resolved.	4.2(2a)	4.2(3b)

Known Behaviors and Limitations

Known Behaviors and Limitations in Release 4.2(3h)

The following caveats are known limitations in release 4.2(3h):

Table 22: External PSU

Defect ID	Symptom	Workaround	First Affected Release
CSCwc10053	In Cisco UCS C-series M5 and M6 servers, PSU firmware update fails for 1600 Liteon PSU when the AC cable is not connected to the PSU. In some cases, the 1600 Liteon PSU firmware might get corrupted when the AC cable is not connected to the PSU.	Connect the AC power cable to all the PSUs present in the server. If the PSU firmware is corrupted, then re-insert the PSU.	4.2(3h)

Known Behaviors and Limitations in Release 4.2(3b)

The following caveats are known limitations in release 4.2(3b):

Table 23: Host Firmware Upgrade

Defect ID	Symptom	Workaround	First Affected Release
CSCwc64817	In Cisco UCS S3260 M5 servers, the Redfish API user interface does not populate the drive list under **SimpleStorage** resource.	Use the resources under **Storage** resource. The resources under **SimpleStorage** resource are deprecated.	4.1(3g)
CSCwd15480	In Cisco UCS S3260 M5 servers, firmware update fails when there are no VIC cards in SIOC1 or SIOC2.	Add the appropriate VIC cards in SIOC1 or SIOC2.	4.2(2f)

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