Release Notes for Cisco UCS Rack Server Software, Release 4.3(4)

First Published: 2024-06-05

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 4.3(4) 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 22 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
A0	June 05, 2024	Created release notes for 4.3.4.240152 for the following servers: • Cisco UCS C220 M7 and C240 M7 servers • Cisco UCS C220 M6, C240 M6, C225 M6, C245 M6 servers and S3260 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 4.3

Cisco IMC Release Number and .ISO Image Names

Beginning with the release 4.3, Cisco is updating the release number naming convention to align with the .ISO images.

Example: **4.3.1.YYXXXX**

- **4.3**—Represents the main release.
- **.1**—Represents the first release.

  For the current 4.3 main release, **.1** represents the first release number.

  For subsequent maintenance releases, this number will represent the related maintenance release number.
- **YY**—Represents the year of release.

  For the current 4.3 main release, **23** is derived from the year 2023.
- **XXXX**—The final 4 digits represent the increasing sequence of build numbers every year.

  For the first 4.3 main release, the number is **0097**.

Supported Platforms and Release Compatibility Matrix

Supported Platforms in this Release

The following servers are supported in this release:

- Cisco UCS C220 M7
- Cisco UCS C240 M7
- Cisco UCS C220 M6
- Cisco UCS C240 M6
- Cisco UCS C245 M6
- Cisco UCS C225 M6
- Cisco UCS S3260 M5

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, 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 4.3(4) Release

Cisco IMC Release	Cisco UCS Manager Release	Rack Mount Servers
4.3.4.240152	4.3(4a)	• Cisco UCS C220 M7 and C240 M7 servers • Cisco UCS C220 M6, C240 M6, C225 M6 and C245 M6 and S3260 M5 servers

Table 2: Cisco IMC and UCS Manager Software Releases for Rack Mount Servers for Cisco IMC 4.3(3) Release

Cisco IMC Release	Cisco UCS Manager Release	Rack Mount Servers
4.3.3.240043	NA	• Cisco UCS C220 M7 and C240 M7 servers • Cisco UCS C220 M6, C240 M6, C225 M6 and C245 M6 servers
4.3.3.240041	NA	• Cisco UCS S3260 M5 servers
4.3.3.240022	4.3(3a)	• Cisco UCS C220 M7 and C240 M7 servers • Cisco UCS C220 M6, C240 M6, C225 M6 and C245 M6 and S3260 M5 servers

Table 3: Cisco IMC and UCS Manager Software Releases for Rack Mount Servers for Cisco IMC 4.3(2) Release

Cisco IMC Release	Cisco UCS Manager Release	Rack Mount Servers
4.3.2.240053	NA	Cisco UCS C220 M5, C240 M5, C480 M5, C125 M5 and S3260 M5 servers
4.3.2.240037	NA	• Cisco UCS C225 M6 and C245 M6 servers
4.3.2.240009	NA	• Cisco UCS C220 M6, C240 M6, C225 M6 and C245 M6 servers • Cisco UCS C220 M5, C240 M5, C480 M5, C125 M5 and S3260 M5 servers

Cisco IMC Release	Cisco UCS Manager Release	Rack Mount Servers
4.3.2.240002	4.3(2)	• Cisco UCS C220 M7 and C240 M7 servers • Cisco UCS C220 M6, C240 M6, C225 M6 and C245 M6 servers • Cisco UCS C220 M5, C240 M5, C480 M5, C125 M5 and S3260 M5 servers
4.3.2.230270	4.3(2)	• Cisco UCS C220 M7 and C240 M7 servers • Cisco UCS C220 M6, C240 M6, C225 M6 and C245 M6 servers • Cisco UCS C220 M5, C240 M5, C480 M5, C125 M5 and S3260 M5 servers
4.3.2.230207	4.3(2)	• Cisco UCS C220 M7 and C240 M7 servers • Cisco UCS C220 M6, C240 M6, C225 M6 and C245 M6 servers • Cisco UCS C220 M5, C240 M5, C480 M5, C125 M5 and S3260 M5 servers

Table 4: Cisco IMC and UCS Manager Software Releases for Rack Mount Servers for Cisco IMC 4.3(1) Release

Cisco IMC Release	Cisco UCS Manager Release	Rack Mount Servers
4.3.1.230138	No Support	Cisco UCS C220 M7 and C240 M7 servers
4.3.1.230124	No Support	Cisco UCS C220 M7 and C240 M7 servers
4.3.1.230097	No Support	Cisco UCS C220 M7 and C240 M7 servers

Table 5: 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

Cisco IMC Release	Cisco UCS Manager Release	Rack Mount 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
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 6: 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 7: 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

Table 8: 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
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 9: 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.

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
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 10: 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

Cisco IMC Release	Cisco UCS Manager Release	Rack Mount 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

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 4.3(4):

Recommended Browser	Minimum Recommended Browser Version	Minimum Recommended Operating System
Google Chrome	Version 122.0.6261.129 (Official Build) (x86_64)	Mac OS 14.2.1 (23C71)
	Version 122.0.6261.131 (Official Build) (64-bit)	Microsoft Windows 11 Enterprise
	Version 123.0.6312.59 (Official Build) (64-bit)	Microsoft Windows 11 Enterprise
	Version 123.0.6312.58 [(Official Build) (64-bit)]	Microsoft Windows 11 Enterprise
Safari	Version 17.2.1 (19617.1.17.11.12)	Mac OS 14.2.1 (23C71)
Mozilla Firefox	123.0.1	
	124.0.1 (64-bit)	Microsoft Windows 11 Enterprise
	24.0.1	

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.

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
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.

Downgrade Limitation for Release 4.3.4.240152:

See Cisco UCS Rack Server Upgrade Support Matrix to view your server upgrade path.

Downgrade Limitation for Release 4.3.3.240022:

In the release 4.3.3.240022, you cannot downgrade the Cisco UCS M7 servers with 5th Gen Intel® Xeon® processors.

When you try to downgrade Cisco IMC, the following error message is displayed on CLI, GUI, Redfish API and XML API user interfaces:

Error message during BMC downgrade with different interfaces like CLI/WEBUI/Redfish/XML =

“Update aborted. INCOMPATIBLE_IMAGE”

When you try to downgrade BIOS, the following error message is displayed on CLI, GUI, Redfish API and XML API user interfaces:

CPU ID mismatch between uploaded image and the platform.

Note You can downgrade Cisco UCS M7 servers with 4th Generation Intel® Xeon® Scalable Processors.

Infrastructure Upgrade and Downgrade to Release 4.3(2):

- Cisco UCS M4 servers are not supported by 4.3.2.230207 and later releases.
- You must perform firmware update after adding any new hardware component to the system.
- If you are planning to install Cisco UCS VIC 15237 or 15427 in a server, then upgrade the server to 4.3.2.230270 or later versions and then insert the adapter into the server.

  If you insert Cisco UCS VIC 15237 or 15427 into the server that is running earlier versions than 4.3.2.230270, then upgrade the server to 4.3.2.230270 or later versions and power cycle the server to recognize the adapter.
- If you are planning to install Cisco UCS VIC 15235 or 15425 in a server, then upgrade the server to 4.3.2.230207 or later versions and then insert the adapter into the server.

  If you insert Cisco UCS VIC 15235 or 15425 into the server that is running earlier versions than 4.3.2.230207, then upgrade the server to 4.3.2.230207 or later versions and power cycle the server to recognize the adapter.

Support for Cisco UCS M7 Servers

Cisco UCS M7 servers are supported from the release 4.3.1.230097 onwards.

The following releases are for Cisco UCS M7 servers only:

- 4.3.1.230138
- 4.3.1.230124
- 4.3.1.230097

Upgrade Paths to Release 4.3.4

The section provides information on the upgrade paths to release 4.3.4.

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

Table 12: Upgrade Paths to Release 4.3(4x)

Upgrade From Release	Upgrade To Release	Recommended Upgrade Path
Following Cisco UCS servers from the release 4.3.1.230097 • Cisco UCS C220 M7 • Cisco UCS C240 M7	• 4.3.4.240152 • 4.3.3.240043 • 4.3.3.240022 • 4.3.2.240002 • 4.3.2.230270 • 4.3.2.230207 • 4.3.1.230138 • 4.3.1.230124	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 4.3.4.240152. • 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 the release 4.2(3b) • 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	• 4.3.4.240152 • 4.3.3.240043 • 4.3.3.240022 • 4.3.2.230270 • 4.3.2.230207 • 4.2(3g) • 4.2(3e) • 4.2(3d) **Note** For Cisco UCS M5 servers, the following releases support only Cisco UCS S3260 M5 servers: 4.3.3.240022	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 4.3.2.230207. • 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 the release 4.2(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	• 4.3.2.240002 • 4.3.2.230270 • 4.3.2.230207 • 4.2(3g) • 4.2(3e) • 4.2(3d) • 4.2(3b) **Note** For Cisco UCS M5 servers, the following releases support only Cisco UCS S3260 M5 servers: 4.3.4.240152 4.3.3.240022	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 16.	• 4.3.4.240152 • 4.3.3.240043 • 4.3.3.240022 • 4.3.2.240002 • 4.3.2.230270 • 4.3.2.230207	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	• 4.3.2.240002 • 4.3.2.230270 • 4.3.2.230207 • 4.2(3g) • 4.2(3e) • 4.2(3d) • 4.2(3b) **Note** For Cisco UCS M5 servers, the following releases support only Cisco UCS S3260 M5 servers: 4.3.4.240152 4.3.3.240022	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	• 4.3.2.240002 • 4.3.2.230270 • 4.3.2.230207 • 4.2(3g) • 4.2(3e) • 4.2(3d) • 4.2(3b) **Note** For Cisco UCS M5 servers, the following releases support only Cisco UCS S3260 M5 servers: 4.3.4.240152 4.3.3.240022	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	- 4.3.2.240002 - 4.3.2.230270 - 4.3.2.230207 - 4.2(3g) - 4.2(3e) - 4.2(3d) - 4.2(3b) **Note** For Cisco UCS M5 servers, the following releases support only Cisco UCS S3260 M5 servers: 4.3.4.240152 4.3.3.240022	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	- 4.3.2.240002 - 4.3.2.230270 - 4.3.2.230207 - 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	• 4.3.3.240043 • 4.3.3.240022 • 4.3.2.240002 • 4.3.2.230270 • 4.3.2.230207 • 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.
Cisco UCS C240 M6		
Cisco UCS C225 M6		
Cisco UCS C245 M6		

Firmware Files

Firmware Files

The C-Series software release 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 4.3	Host Upgrade Utility
Unified Computing System (UCS) Drivers	ucs-cxxx-drivers.4.3.4.240152.iso	Drivers
Unified Computing System (UCS) Utilities	ucs-cxxx-utils-efi.4.3.4.240152.iso ucs-cxxx-utils-linux.4.3.4.240152.iso ucs-cxxx-utils-vmware.4.3.4.240152.iso ucs-cxxx-utils-windows.4.3.4.240152.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 4.3.

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
- Broadcom Adapters
- LAN on Motherboard
- PCIe adapter firmware
- HDD firmware
- SAS Expander firmware
- DCPMM Memory
- PCI Gen5 retimer

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

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)
- 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 4.3.4

New Hardware in Release 4.3.4.240152

The following new hardware are supported in Release 4.3.4.240152:

- Support for the following RAID controllers:
  - Cisco boot optimized M.2 NVMe RAID controller (UCS-M2-NVRAID) with Cisco UCS C220 M7 and C240 M7 servers.

    This controller supports only RAID0, RAID1, or JBOD (default - JBOD) mode and only UEFI boot mode.
- Support for the UCS-TPM-002D TPM module with Cisco UCS C220 M6, C240 M6, C220 M7, and C240 M7 servers.
- Support for the following GPUs:
  - Intel® Data Center GPU Flex 140, HHHL, 75W PCIe with Cisco UCS C220 M7 and C240 M7 servers
  - Intel® Data Center GPU Flex 170, FH-3/4L, 150W PCIe with Cisco UCS C240 M7 servers
  - NVIDIA® Hopper L4 70W, 24GB, 1-slot HHHL (UCSC-GPU-L4M6) with Cisco UCS C220 and C240 M6 servers

New Software in Release 4.3.4

New Software Features in Release 4.3.4.240152

The following new software features are supported in Release 4.3.4.240152.

- Beginning with 4.3.4.240152 release, Cisco has released a new version of IMC with updated UI and security enhancements.

  The new UI (beta version) includes features like a more intuitive interface, streamlined workflows, and better integration with other management tools.
- Support for Transmit Enhanced Mode on Cisco UCS VIC 15000 series cards on Cisco UCS C-Series servers.

When Transmit Enhanced Mode is enabled, Cisco IMC allows the firmware to optimize traffic forwarding for TCP transmissions across IPv4 networks between 1000-1560 packet sizes

- Release 4.3.4.240152 qualifies the new CipherTrust KMIP server from Thales®, which is set to take over from the old SafeNet and Vormetric servers that are being phased out. The new CipherTrust KMIP server offers enhanced usability and an expanded feature set, but keeps the user experience the same. Support for new CipherTrust in Cisco IMC starts with version 4.3.4.240152. For detailed instructions on the configuration process of the CipherTrust KMIP manager, please refer to the CipherTrust Manager user guide provided by Thales®.

- Beginning with 4.3.4.240152 release, Cisco IMC UI displays the following additional details for third-party adapters:

Table 14: Third-Party Adapter Information

Name	Description
Name	Name of the PCIe adapter.
Vendor	The vendor for the PCIe adapter.
Serial Number	Serial number of the PCIe adapter.
Part Number	Part number of the PCIe adapter.
Manufacturer	PCIe adapter manufacturer.
Firmware Version	Current firmware version of the PCIe adapter.

Table 15: Port Details

Name	Description
Port column	Port used to make external connection to the adapter.
Status column	The status of the PCIe adapter. This can be up or down.
Link Speed column	Displays the speed of an adapter card installed in PCIs slot.
WWPN column	The World Wide Port Name for the adapter.
Factory WWPN column	Factory supplied World Wide Port Name for the adapter.
WWNN column	The World Wide Node Name for the adapter.
Factory WWNN column	The World Wide Node Name for the adapter from factory settings.

For more information, see Cisco UCS C-Series Integrated Management Controller GUI Configuration Guide, Release 4.3 or Cisco UCS C-Series Servers Integrated Management Controller CLI Configuration Guide, Release 4.3.

Resolved Caveats

Resolved Caveats in 4.3.4.240152

The following defects were resolved in Release 4.3.4.240152:

Table 16: Host Firmware Upgrade

Defect ID	Symptom	First Release Affected	Resolved in Release
CSCwj49647	Cisco UCS servers has faulty drive notfications in Cisco IMC Web UI. If the data sanitization fails for any drives, then check the drive state. If the storage driver is in fault state, then the failure is expected. In some case, the storage drives might be in moderate fault. For those drives, data sanitization might pass in case the drive is visible to host. This issue is now resolved.	4.2(3d)	4.3.4.240152

Open Caveats

Open Caveats in Release 4.3.4.240152

The following defects are open in Release 4.3.4.240152:

Defect ID	Symptom	Workaround	First Affected Release
CSCwi60571	In Cisco UCS M6 servers, the network speed of the port is not available for few Mellanox third party adapters. In Cisco IMC user interfaces, the value displayed for the **Network Port Speed** field is **NA**.	You can check the network speed of the port using Host Operating system.	4.3.4.240152

Known Behaviors and Limitations

Known Behaviors and Limitations in Release 4.3.4.240152

New Cisco IMC UI Limitations

Beginning with the release 4.3.4.240152, Cisco has released a new version of Cisco IMC with updated UI and security enhancements.

The following are the limitations in the new Cisco IMC UI (beta version):

- Device Connector configuration page is not available in the new Cisco IMC UI.
- Features supporting browser-based local upload or downloads are not available in the new Cisco IMC UI.
- There can be maximum four sessions across old and new Cisco IMC UI.
- You cannot terminate any active sessions in the new Cisco IMC UI from other Cisco IMC interfaces.
- No impact on logged out and inactive timed-out sessions.

Known Behaviors and Limitations

The following caveats are known limitations in release 4.3.4.240152:

Defect ID	Symptom	Workaround	First Affected Release
CSCwi67637	In Cisco UCS M6 and M7 servers, the Cisco PID is not listed. Third Party Adapter FRU Name is not aligned with Cisco Product name (PID Catalog Product name).	You can refer **Cisco PID** / **Product name information** available in **Product ID Catalog** to order any third-party adapter. You can view the **PID Catalog** in Cisco IMC to identify the Cisco PID and Product name for any third-party adapter or hardware component.	4.3.4.240152

Defect ID	Symptom	Workaround	First Affected Release
CSCwi73879	The following fields are not displayed in Cisco IMC interfaces for third party adapters: • Adapter Temperature • Port Status • FRU Information	Use Host Upgrade Utility (HUU) to update and activate all the firmware components (including third party adapter firmware) to latest firmware and enable MCTP. If third party management features are not working after HUU Update, perform Force Update - update specific third-party adapter component from the list of third-party adapter firmware.	4.3.4.240152

Security Fixes in Release 4.3.4

Security Fixes in Release 4.3.4.240152

Defect ID - CSCwi59840

Cisco IMC includes Third-party Software that is affected by the vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) IDs:

- CVE-2023-48795—The SSH transport protocol with certain OpenSSH extensions, found in OpenSSH before 9.6 and other products, allows remote attackers to bypass integrity checks, such that some packets are omitted (from the extension negotiation message), and a client and server may consequently end up with a connection for which some security features have been downgraded or disabled, also known as Terrapin attack.

  This occurs because the SSH Binary Packet Protocol (BPP), implemented by these extensions, mishandles the handshake phase and use of sequence numbers. For example, when there is an effective attack against SSH's use of ChaCha20-Poly1305 (and CBC with Encrypt-then-MAC), the bypass occurs in chacha20-poly1305@openssh.com, (and if CBC is used, then the -etm@openssh.com MAC algorithms).

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