Release Notes for Cisco UCS Manager, Release 4.2

First Published: 2021-06-24

Last Modified: 2026-08-05

Cisco UCS Manager

Cisco UCS™ Manager, Release 4.2 provides unified, embedded management of all software and hardware components of the Cisco Unified Computing System™ (Cisco UCS) across multiple chassis, Cisco UCS servers, and thousands of virtual machines. Cisco UCS Manager manages Cisco UCS as a single entity through an intuitive GUI, a command-line interface (CLI), or an XML API for comprehensive access to all Cisco UCS Manager functions. For more information on Cisco UCS Manager, see Cisco UCS Manager on Cisco.com.

This document contains information on new features, resolved caveats, open caveats, and workarounds for Cisco UCS Manager, Release 4.2. This document also includes the following:

- Current information that became available after the technical documentation was published
- Related firmware and BIOSes on blade and rack servers and other Cisco Unified Computing System (UCS) components associated with the release

Deprecation Notice

Deprecated UCS B-Series Blade Software Release 4.2(2a)

Release 4.2(2a) is deprecated and firmware files are no longer available for Cisco UCS B-Series Blade Server Software.

Do not upgrade B-Series servers directly to the 4.2(2a) release from a release of 4.0(4m) or earlier. There is no possibility of recovery from this upgrade failure. The blade will need to be replaced via a hardware RMA.

For more information, refer to the Deferral Notice:

https://software.cisco.com/download/advisories?fileName=ucs-k9-bundle-b-series.4.2.2a.B.bin&mdfid=283853163

Deprecated Release 4.2(1k) and 4.2(1l)

Releases 4.2(1k) and 4.2(1l) are deprecated and firmware files are no longer available.

Cisco recommends that you upgrade to release 4.2(1m) or later. For more information, refer to the Deferral Notices:

- https://software.cisco.com/download/advisories?fileName=ucs-k9-bundle-b-series.4.2.1k.B.bin&mdfid=283853163

- https://software.cisco.com/download/advisories?fileName=ucs-k9-bundle-b-series.4.2.1l.B.bin&mdfid=283853163

Revision History

Table 1: Release 4.2(3)

Release	Date	Description
4.2(3s)	August 05, 2026	Created release notes for Cisco UCS Manager Release 4.2(3s).
4.2(3r)	April 14, 2026	Created release notes for Cisco UCS Manager Release 4.2(3r).
4.2(3p)	September 23, 2025	Created release notes for Cisco UCS Manager Release 4.2(3p).
4.2(3o)	February 21, 2025	Created release notes for Cisco UCS Manager Release 4.2(3o).
4.2(3n)	December 19, 2024	Created release notes for Cisco UCS Manager Release 4.2(3n).
4.2(3m)	October 23, 2024	Created release notes for Cisco UCS Manager Release 4.2(3m).
4.2(3l)	September 30, 2024	Created release notes for Cisco UCS Manager Release 4.2(3l).
4.2(3k)	July 05, 2024	Added CSCwd35712 under Resolved Caveats in Release 4.2(3k), on page 119.
4.2(3k)	June 14, 2022	Created release notes for Cisco UCS Manager Release 4.2(3k).
4.2(3j)	March 20, 2024	Updated Upgrade and Downgrade Guidelines, on page 8.
4.2(3j)	February 21, 2024	Created release notes for Cisco UCS Manager Release 4.2(3j).
4.2(3i)	November 06, 2023	Created release notes for Cisco UCS Manager Release 4.2(3i).
4.2(3h)	September 28, 2023	Created release notes for Cisco UCS Manager Release 4.2(3h).
4.2(3g)	August 21, 2023	Updated Open Caveats in Release 4.2(3g).
4.2(3g)	July 17, 2023	Created release notes for Cisco UCS Manager Release 4.2(3g).

Release	Date	Description
4.2(3e)	May 15, 2023	Created release notes for Cisco UCS Manager Release 4.2(3e).
4.2(3d)	March 20, 2023	Created release notes for Cisco UCS Manager Release 4.2(3d).
4.2(3b) and 4.2(2e)	March 15, 2023	Updated Cross-Version Firmware Support table for the following: • 4.2(2) A Infrastructure bundle supports 4.2(3) B and C server firmware bundles • 4.2(1) A infrastructure bundle supports 4.2(3) B and C server bundles • 4.2(1) A infrastructure bundle supports 4.2(2) B and C server bundles
4.2(3b)	January 06, 2023	Created release notes for Cisco UCS Manager Release 4.2(3b).

Table 2: Release 4.2(2)

Release	Date	Description
4.2(2a)	March 14, 2024	Updated Behavior Changes and Known Limitations section.
4.2(2a)	May 24, 2023	Updated Security Fixes for 4.2(2a).
4.2(2e)	March 03, 2023	Created release notes for Cisco UCS Manager Release 4.2(2e).
4.2(2d)	November 23, 2022	Created release notes for Cisco UCS Manager Release 4.2(2d).
4.2(2c)	September 20, 2022	Created release notes for Cisco UCS Manager Release 4.2(2c).
4.2(2a)	August 19, 2022	Deprecated UCS B-Series Blade Software Release 4.2(2a).
4.2(2a)	July 08, 2022	Created release notes for Cisco UCS Manager Release 4.2(2a).

Table 3: Release 4.2(1)

Release	Date	Description
4.2(1n)	August 01, 2022	Created release notes for Cisco UCS Manager Release 4.2(1n).
4.2(1m)	May 16, 2022	Created release notes for Cisco UCS Manager Release 4.2(1m).
4.2(1i)	October 26, 2021	Created release notes for Cisco UCS Manager Release 4.2(1i).
4.2(1f)	August 17, 2021	Created release notes for Cisco UCS Manager Release 4.2(1f).
4.2(1d)	June 24, 2021	Created release notes for Cisco UCS Manager Release 4.2(1d).

Top Reasons to Move to Cisco UCS Manager Release 4.2

Release 4.2(3)

- 6500 Series Fabric Interconnect—Cisco UCS Manager introduces support for fifth generation of Cisco UCS 6536 Fabric Interconnect (UCS FI 6536). The Cisco 6536 Fabric Interconnects are a core part of the Cisco Unified Computing System, providing both network connectivity and management capabilities for the system. The Cisco 6536 offer line-rate, low-latency, lossless 10/25/40/100 Gigabit Ethernet, Fibre Channel over Ethernet (FCoE), and Fibre Channel functions.
- Support for Cisco UCS VIC 15411 – 4 x 10G mLOM adapter on Cisco UCS B-series M6 servers
- Support of Cisco UCS VIC 15238 – 2 x 40G/100G/200G mLOM adapter on Cisco UCS C-series M6 rack servers
- Authenticated SMTP support for UCS Call Home
- QinQ forwarding feature
- **Password Encryption Key** to enhance security for backup configuration files.

Release 4.2(2)

- Support of Cisco VIC 15428 mLOM 4-port adapter on Cisco UCS C-series M6 rack servers

Release 4.2(1)

- Support for Cisco UCS C220 M6 ServerCisco UCS C240 M6 Server, Cisco UCS C225 M6 Server, and Cisco UCS C245 M6 Server
- Support for Cisco UCS B200 M6 Server.
- Support for new peripherals and optics.

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 B200 M6
- Cisco UCS B200 M5
- Cisco UCS B480 M5
- Cisco UCS C220 M5
- Cisco UCS C240 M5
- Cisco UCS C240 SD M5
- Cisco UCS C480 M5
- Cisco UCS C480 M5 ML
- Cisco UCS S3260 M5
- Cisco UCS C125 M5
- Cisco UCS C220 M4
- Cisco UCS C240 M4
- Cisco UCS C460 M4
- Cisco UCS S3260 M4
- Cisco UCS B200 M4
- Cisco UCS B260 M4
- Cisco UCS B420 M4
- Cisco UCS B460 M4

Cisco UCS Manager and Cisco UCS C-Series Release Compatibility Matrix for C-Series Rack-Mount Servers

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

Each Cisco UCS Manager release incorporates its corresponding C-Series Standalone release. For example, Cisco UCS Manager Release 4.2(1) is integrated with C-Series Standalone Release 4.2(1) for the M6 servers, Release 4.1(1) for the M4 and M5 servers, Release 4.0(2) for all the M4 and M5 servers. Hence, it supports all the M6, M5 and M4 servers supported by C-Series Standalone releases.

The following table lists the Cisco UCS Manager and C-Series software standalone releases for C-Series Rack-Mount Servers:

Table 4: Cisco UCS Manager and C-Series Software releases for C-Series Servers

Cisco UCS Manager Release	C-Series Standalone Releases Included	C-Series Servers Supported by the C-Series Standalone Releases
4.2(3)	4.2(3)	All M6, M5, and S3260 M4
	4.1(3)	All M5 and S3260 M4
	4.1(2)	C220 M4, C240 M4, and C460 M4
4.2(2)	4.2(2)	All M6, M5, and S3260 M4
	4.1(3)	S3260 M4, All M5
	4.1(2)	C220 M4, C240 M4, C460 M4
4.2(1)	4.2(1)	All M6
	4.1(3)	S3260 M4, All M5
	4.1(2)	C220 M4, C240 M4, C460 M4
4.1(3)	4.1(3)	S3260 M4, All M5
	4.1(2)	C220 M4, C240 M4, C460 M4
	3.0(4)	All M3
4.1(2)	4.1(2)	C220 M5, C240 M5, C240 SD M5, C480 M5, S3260 M5, C480 M5 ML, C125 M5, C220 M4, C240 M4, C460 M4, S3260 M4
	3.0(4)	All M3
4.1(1)	4.1(1)	C220 M5, C240 M5, C480 M5, S3260 M5, C125 M5, C480 M5 ML only
	4.0(2)	C220 M4, C240 M4, C460 M4, S3260 M4, C125 M5 only
	3.0(4)	All M3
4.0(4)	4.0(4)	C220 M5, C240 M5, C480 M5, S3260 M5, C480 M5 ML only
	4.0(2)	C220 M4, C240 M4, C460 M4, S3260 M4, C125 M5 only
	3.0(4)	All M3

Cisco UCS Manager Release	C-Series Standalone Releases Included	C-Series Servers Supported by the C-Series Standalone Releases
4.0(2)	4.0(2)	C220 M4, C240 M4, C460 M4, C220 M5, C240 M5, C480 M5, S3260 M4, S3260 M5, C125 M5, C480 M5 ML only
	3.0(4)	All M3
4.0(1)	4.0(1)	C220 M4, C240 M4, C460 M4, C220 M5, C240 M5, C480 M5, S3260 M4, S3260 M5, C125 M5 only
	3.0(4)	All M3
3.2(3)	3.1(3)	C220 M5, C240 M5, C480 M5, S3260 M5 only
	3.0(4)	All M3/M4
3.2(2)	3.1(2)	C220 M5, C240 M5, C480 M5 only
	3.0(3)	All M3/M4
3.2(1)	3.1(1)	C220 M5, C240 M5 only
	3.0(3)	All M3/M4
3.1(3)	3.0(3)	All M3/M4
3.1(2)	2.0(13)	All M3/M4
3.1(1)	2.0(10)	C220 M4, C240 M4 only
	2.0(9)	All other M3/M4
2.2(8)	2.0(12)	C460 M4 only
	2.0(10)	C220 M4, C240 M4 only
	1.5(9)	C420-M3, C260-M2, C460-M2 only
	2.0(9)	For all other M3/M4

System Requirements

Supported Operating Systems

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

Supported Web Browsers

Cisco UCS Manager GUI	Web Browsers
HTML5	Apple Safari 16.2 (18614.3.7.1.5) Google Chrome 109.0.5414.75 Microsoft Internet Explorer 11.0.9600.18739 (Microsoft Internet Explorer is Retired. Support is available only until Windows 8.1 and Windows2008 R2) Microsoft Edge 109.0.1518.55 Mozilla Firefox 108.0.2 Opera 94.0.4606.76

Note HTML-5 UI supports one user session per browser.

Network Requirements

The *Cisco UCS Manager Administration Management Guide, Release 4.2* provides detailed information about configuring the Intersight Device Connector.

Cisco UCS Central Integration

Cisco UCS Manager Release 4.2 can only be registered with Cisco UCS Central, Release 2.0(1n) or later releases.

Note For the complete list of compatible versions of Cisco UCS Central and Cisco UCS Manager, refer Release Notes for Cisco UCS Central.

Upgrade and Downgrade Guidelines

To get a complete overview of all the possible upgrade paths in Cisco UCS Manager, see Cisco UCS Manager Upgrade/Downgrade Support Matrix.

Infrastructure Upgrade and Downgrade to Release 4.2(3)

1. Once you upgrade Cisco UCS 6400 or 64108 FI to release 4.2(3) or later and enable Q-in-Q feature from Cisco UCS Manager GUI, then you cannot downgrade to any previous release. To downgrade to any release earlier than 4.2(3), you must first disable Q-in-Q feature from Cisco UCS Manager GUI.
2. Once you upgrade to release 4.2(3) or later and enable **SMTP Authentication** under Call Home in Cisco UCS Manager GUI, then you cannot downgrade to any previous release. To downgrade to any release earlier than 4.2(3), you must first disable **SMTP Authentication** from Cisco UCS Manager GUI.

Table 5: Upgrade Paths to Release 4.2(3)

Upgrade from Release	Recommended Upgrade Path
Upgrade from any 4.2(2) release	Direct upgrade.
Upgrade from any 4.2(1) release	**1.** Upgrade from 4.2(1i)A or later patch—Direct upgrade to release 4.2(3)A. **2.** Upgrade from a patch earlier than 4.2(1i)A— **a.** Upgrade to release 4.2(1i)A bundle and activate. **Note** Do not download release 4.2(3)A bundle before activating release 4.2(1i)A. **b.** Download and upgrade to release 4.2(3)A.
Upgrade from any 4.1(3) release	**1.** Upgrade from 4.1(3h) or later patch—Direct upgrade to release 4.2(3). **2.** Upgrade from a patch earlier than 4.1(3h)— **a.** Upgrade to release 4.1(3h)A bundle and activate. **Note** Do not download release 4.2(3)A bundle before activating release 4.1(3h)A. **b.** Download and upgrade to release 4.2(3).
Upgrade from any 4.1(2) release	**1.** Upgrade to release 4.1(3h)A bundle or later infrastructure bundle in 4.1(3) release version and activate. **Note** Do not download release 4.2(3)A bundle before activating release 4.1(3h)A bundle or later infrastructure bundle in 4.1(3) release version. **2.** Download and upgrade to release 4.2(3)A.

Upgrade from Release	Recommended Upgrade Path
Upgrade from any 4.1(1) release	**1.** Upgrade to release 4.1(3h)A bundle or later infrastructure bundle in 4.1(3) release version and activate. **Note** Do not download release 4.2(3)A bundle before activating release 4.1(3h)A bundle or later infrastructure bundle in 4.1(3) release version. **2.** Download and upgrade to release 4.2(3)A.
Upgrade from any 4.0(4) release	**1.** Upgrade from 4.0(4n)A or later infrastructure bundle in 4.0(4) release version —Direct upgrade to release 4.2(3)A. **2.** Upgrade from a patch earlier than 4.0(4n)A— **a.** Upgrade to release 4.0(4n)A bundle and activate. **Note** Do not download release 4.2(3)A bundle before activating release 4.0(4n)A or later infrastructure bundle. **b.** Download and upgrade to release 4.2(3)A.

Upgrade Cisco UCS M5 B-Series Servers to Release 4.2(2)

While upgrading any Cisco UCS M5 B-Series server from 4.0(4m) or an earlier release, perform a two-step upgrade.

1. First upgrade the server to any 4.1 release. Cisco recommends latest 4.1(3) patch.
2. Once the server is running the 4.1 release, upgrade to 4.2(2) release.

Infrastructure Upgrade and Downgrade to Release 4.2(2)

The section provides information on the upgrade paths to release 4.2(2) and downgrade limitations.



Note You should upgrade the entire infrastructure A bundle.

Refer to the table for upgrade paths for Cisco UCS Manager:

Table 6: Upgrade Paths to Release 4.2(2)

Upgrade from Release	Recommended Upgrade Path
Upgrade from any 4.2(1) release	**1.** Upgrade from 4.2(1i)A or later patch—Direct upgrade to release 4.2(2)A. **2.** Upgrade from a patch earlier than 4.2(1i)A— **a.** Upgrade to release 4.2(1i)A bundle and activate. **Note** Do not download release 4.2(2)A bundle before activating release 4.2(1i)A. **b.** Download and upgrade to release 4.2(2)A.
Upgrade from any 4.1(3) release	**1.** Upgrade to release 4.1(3h)A bundle or later infrastructure bundle in 4.1(3) release version and activate. **Note** Do not download release 4.2(2)A bundle before activating release 4.1(3h)A bundle or later infrastructure bundle in 4.1(3) release version. **2.** Download and upgrade to release 4.2(2)A.
Upgrade from any 4.1(2) release	**1.** Upgrade to release 4.1(3h)A bundle or later infrastructure bundle in 4.1(3) release version and activate. **Note** Do not download release 4.2(2)A bundle before activating release 4.1(3h)A bundle or later infrastructure bundle in 4.1(3) release version. **2.** Download and upgrade to release 4.2(2)A.
Upgrade from any 4.1(1) release	**1.** Upgrade to release 4.1(3h)A bundle or later infrastructure bundle in 4.1(3) release version and activate. **Note** Do not download release 4.2(2)A bundle before activating release 4.1(3h)A bundle or later infrastructure bundle in 4.1(3) release version. **2.** Download and upgrade to release 4.2(2)A.

Upgrade from Release	Recommended Upgrade Path
Upgrade from any 4.0(4) release	1. Upgrade from 4.0(4n)A or later infrastructure bundle in 4.0(4) release version —Direct upgrade to release 4.2(2)A. 2. Upgrade from a patch earlier than 4.0(4n)A— a. Upgrade to release 4.0(4n)A bundle and activate. **Note** Do not download release 4.2(2)A bundle before activating release 4.0(4n)A or later infrastructure bundle. b. Download and upgrade to release 4.2(2)A.

CSCwa39877

In a setup equipped with Cisco UCS VIC 15428 adapter, you cannot downgrade to any release earlier than 4.2(2a).

Infrastructure Upgrade and Downgrade to Release 4.2(1)

Table 7: Upgrade Paths to Release 4.2(1)

Upgrade from Release	Recommended Upgrade Path
Upgrade from any 4.1(3) release	1. Upgrade from 4.1(3h)A or later patch—Direct upgrade to release 4.2(1)A. 2. Upgrade from a patch earlier than 4.1(3h)— a. Upgrade to release 4.1(3h)A bundle and activate. **Note** Do not download release 4.2(1)A bundle before activating release 4.1(3h)A. b. Download and upgrade to release 4.2(1)A.
Upgrade from any 4.1(2) release	1. Upgrade to release 4.1(3h)A bundle or later infrastructure bundle in 4.1(3) release version and activate. **Note** Do not download release 4.2(1)A bundle before activating release 4.1(3h)A bundle or later infrastructure bundle in 4.1(3) release version. 2. Download and upgrade to release 4.2(1)A.

Upgrade from Release	Recommended Upgrade Path
Upgrade from any 4.1(1) release	**1.** Upgrade to release 4.1(3h)A bundle or later infrastructure bundle in 4.1(3) release version and activate. **Note** Do not download release 4.2(1)A bundle before activating release 4.1(3h)A bundle or later infrastructure bundle in 4.1(3) release version. **2.** Download and upgrade to release 4.2(1)A.
Upgrade from any 4.0(4) release	**1.** Upgrade from 4.0(4n)A or later infrastructure bundle in 4.0(4) release version —Direct upgrade to release 4.2(1)A. **2.** Upgrade from a patch earlier than 4.0(4n)A— **a.** Upgrade to release 4.0(4n)A bundle and activate. **Note** Do not download release 4.2(1)A bundle before activating release 4.0(4n)A or later infrastructure bundle. **b.** Download and upgrade to release 4.2(1)A.

Upgrade and Downgrade to Release 4.2(1)

If Cisco UCS Manager upgrade to release 4.2(1l) fails with `Unable to open downloaded image` error message, refer Open Caveats for Release 4.2(1l), on page 152 for a workaround.

Upgrade Limitation

In general, capability catalog can be upgraded within the same major release version. For example, Cisco UCS 3.2(2) release can use a capability catalog with the same major release version like 3.2(1) and cannot use a capability catalog with the release version 3.0(1). However, the Capability Catalog upgrade from 4.2(1) to 4.2(2) can lead to upgrade failure. Cisco UCS release 4.2(1) release version can be used only with 4.2(1) release version of capability catalog.

Default Open Ports

The following table lists the default open ports used in Cisco UCS Manager Release 4.2.

Port	Interface	Protocol	Traffic Type	Fabric Interconnect	Usage
22	CLI	SSH	TCP	UCS 6300 Series UCS 6400 Series UCS 6536	Cisco UCS Manager CLI access
80	XML	HTTP	TCP	UCS 6300 Series UCS 6400 Series UCS 6536	Cisco UCS Manager GUI and third party management stations. Client download
443	XML	HTTP	TCP	UCS 6300 Series UCS 6400 Series UCS 6536	Cisco UCS Manager login page access Cisco UCS Manager XML API access
743	KVM	HTTP	TCP	UCS 6300 Series UCS 6400 Series UCS 6536	CIMC Web Service / Direct KVM
7546	CFS	CFSD	TCP	UCS 6400 Series UCS 6536	Cisco Fabric Service

Cisco UCS Manager Network Management Guide, Release 4.2 provides a complete list of open TCP and UDP ports.

New Features in Release 4.2

Cisco UCS Manager, Release 4.2 is a unified software release for all supported UCS hardware platforms.

New Hardware Features

- New Hardware in Release 4.2(3s), on page 16
- New Hardware in Release 4.2(3r), on page 16
- New Hardware in Release 4.2(3p), on page 16
- New Hardware in Release 4.2(3o), on page 16
- New Hardware in Release 4.2(3n), on page 16

- New Hardware in Release 4.2(3m), on page 16
- New Hardware in Release 4.2(3l), on page 16
- New Hardware in Release 4.2(3k), on page 17
- New Hardware in Release 4.2(3j), on page 17
- New Hardware in Release 4.2(3i), on page 17
- New Hardware in Release 4.2(3h), on page 17
- New Hardware in Release 4.2(3g), on page 17
- New Hardware in Release 4.2(3e), on page 17
- New Hardware in Release 4.2(3d), on page 17
- New Hardware in Release 4.2(3b), on page 17
- New Hardware in Release 4.2(2e), on page 18
- New Hardware in Release 4.2(2d), on page 18
- New Hardware in Release 4.2(2c), on page 18
- New Hardware in Release 4.2(2a), on page 18
- New Hardware in Release 4.2(1n), on page 19
- New Hardware in Release 4.2(1m), on page 19
- New Hardware in Release 4.2(1l) (Deprecated Release), on page 19
- New Hardware in Release 4.2(1i), on page 20
- New Hardware in Release 4.2(1f), on page 20
- New Hardware in Release 4.2(1d), on page 21

New Software Features

- New Software Features in Release 4.2(3s), on page 25
- New Software Features in Release 4.2(3r), on page 25
- New Software Features in Release 4.2(3p), on page 25
- New Software Features in Release 4.2(3o), on page 25
- New Software Features in Release 4.2(3n), on page 25
- New Software Features in Release 4.2(3m), on page 25
- New Software Features in Release 4.2(3l), on page 25
- New Software Features in Release 4.2(3k), on page 25
- New Software Features in Release 4.2(3j), on page 25
- New Software Features in Release 4.2(3i), on page 25

- New Software Features in Release 4.2(3h), on page 25
- New Software Features in Release 4.2(3g), on page 26
- New Software Features in Release 4.2(3e), on page 26
- New Software Features in Release 4.2(3d), on page 26
- New Software Features in Release 4.2(3b), on page 26
- New Software Features in Release 4.2(2e), on page 27
- New Software Features in Release 4.2(2d), on page 27
- New Software Features in Release 4.2(2a), on page 27
- New Software Features in Release 4.2(1n), on page 29
- New Software Features in Release 4.2(1m), on page 29
- New Software Features in Release 4.2(1l) (Deprecated Release), on page 29
- New Software Features in Release 4.2(1i), on page 29
- New Software Features in Release 4.2(1f), on page 29
- New Software Features in Release 4.2(1d), on page 30

New Hardware in Release 4.2

New Hardware in Release 4.2(3s)

None

New Hardware in Release 4.2(3r)

None

New Hardware in Release 4.2(3p)

None

New Hardware in Release 4.2(3o)

None

New Hardware in Release 4.2(3n)

None

New Hardware in Release 4.2(3m)

None

New Hardware in Release 4.2(3l)

None

New Hardware in Release 4.2(3k)

None

New Hardware in Release 4.2(3k)

None

New Hardware in Release 4.2(3j)

None

New Hardware in Release 4.2(3i)

None

New Hardware in Release 4.2(3h)

None

New Hardware in Release 4.2(3g)

None

New Hardware in Release 4.2(3e)

Peripherals

The following are supported on Cisco UCS C-series M6 servers:

- UCSC-O-N6CD100GF (Cisco-NVDA MCX623436AC-CDAB CX6Dx 2x100G QSFP56 x16 OCP NIC)
- UCSC-O-N6CD25GF (Cisco-NVDA MCX631432AC-ADAB CX6 Lx 2x25G SFP28 x8 OCP NIC)

New Hardware in Release 4.2(3d)

None

New Hardware in Release 4.2(3b)

- 6500 Series Fabric Interconnect—Beginning with Release 4.2(3b), Cisco UCS Manager introduces support for fifth generation of Cisco UCS 6536 Fabric Interconnect (UCS FI 6536). The Cisco 6536 Fabric Interconnects are a core part of the Cisco Unified Computing System, providing both network connectivity and management capabilities for the system. The Cisco 6536 offer line-rate, low-latency, lossless 10/25/40/100 Gigabit Ethernet, Fibre Channel over Ethernet (FCoE), and Fibre Channel functions.

  The Cisco UCS 6536 Fabric Interconnect provide the management and communication backbone for UCS B-Series Blade Servers, UCS 5108 B-Series Server Chassis, and UCS C-Series Rack Servers. All servers attached to a Cisco UCS 6536 Fabric Interconnect become part of a single, highly available management domain. In addition, by supporting a unified fabric, Cisco UCS 6536 Fabric Interconnect provides both the LAN and SAN connectivity for all servers within its domain.

- You can migrate the following Fabric Interconnects to UCS 6536 Fabric Interconnect:
  - UCS 6200 Series Fabric Interconnects
  - UCS 6300 Series Fabric Interconnects

Cisco recommends that once you migrate to UCS 6536 Fabric Interconnect, do not migrate back to UCS 6300 Series Fabric Interconnect or UCS 6200 Series Fabric Interconnect.

- Peripherals—
  - Support for Cisco UCS VIC 15411 – 4 x 10G mLOM adapter on Cisco UCS B-series M6 servers



Note Cisco UCS VIC 15411 cannot be combined with Cisco UCS VIC 1400 series within the same server.

  - Support of Cisco UCS VIC 15238 (UCSC-M-V5D200G)– 2 x 40G/100G/200G mLOM adapter on Cisco UCS C-series M6 rack servers with Cisco UCS 6300 and 6536 Fabric Interconnects.
  - Support for NVIDIA UCSC-GPU-A100-80G with Cisco UCS C240 and C480 M5 servers.
  - Support for Cisco Nexus 2348UPQ with Cisco UCS 6500 Series Fabric Interconnects.

New Hardware in Release 4.2(2e)

None

New Hardware in Release 4.2(2d)

None

New Hardware in Release 4.2(2c)

Support for Nvidia GPU-A100-80 GPU (UCSC-GPU-A100-80) for Cisco UCS M5 servers.

New Hardware in Release 4.2(2a)

Peripherals

Support for the following:

- Support for Cisco UCS VIC 1440+PE with Cisco UCS 6300/6400 fabric interconnects and 22xx series IOMs.
- Support of Cisco UCS VIC 15428 MLOM 4-port adapter on Cisco UCS C-series M6 rack servers



Note Release 4.2(2a) does not support Cisco UCS 5th Gen FI (UCS-FI-6536).

- QSFP-40/100-SRBD Network Interface Card at 40G on Cisco VIC 1300 and 1400.
- Intel X710T4LG 4x10 GbE RJ45 PCIe NIC (Carlsville ASIC) with Cisco UCS C220 M6, C240 M6, C225 M6, and C245 M6 servers.
- Qlogic QLE 2772 Fibre Channel Adapter with Cisco UCS C125 M5 servers.
- Qlogic QLE 2772 or QLE 2742 Fibre Channel Adapter with Cisco UCS S3260 servers.

- QLogic QLE2772 2x32GFC Gen 6 Enhanced PCIe HBA) with Cisco UCS C225 M6 and C245 M6 servers.
- MLNX MCX623106AS-CDAT, 2x100 GbE QSFP56 PCIe (non-Crypto/TLS) with Cisco UCS C225 M6 and C245 M6 servers.
- UCSC-P-B7D32GF (Cisco-Emulex LPe35002-M2-2x32GFC Gen 7 PCIe HBA)

New Hardware in Release 4.2(1n)

None

New Hardware in Release 4.2(1m)

None

New Hardware in Release 4.2(1l) (Deprecated Release)

Cisco UCS C225 M6 Server

Cisco UCS C225 M6 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 Cisco UCS Manager and the Cisco Intersight Infrastructure Service cloud-based management platform.

Cisco UCS C225 M6 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 Manager supports C225 M6 servers with Rome and Milan Processors

The C225 M6 servers are supported only with Cisco UCS 6454, 64108, and 6300 Fabric Interconnects.

The server supports the following features:

- A maximum of two 3rd Gen AMD EPYC CPUs.
- 16 DIMM slots per CPU for 3200-MHz DDR4 DIMMs with individual DIMM capacity points up to 256 GB. The maximum memory capacity for 2 CPUs is 8 TB (for 32 x 256 GB DDR4 DIMMs.
- Up to 10 x 2.5-inch 12-Gbps Front load HDDs or SSDs or up to 10 x 2.5-inch (U.2) PCIe Gen 4x2 NVMe SSDs
- The server provides internal slots for one Cisco 12G SAS RAID controllers with 4 GB cache backup to control SAS/SATA drives, or Up to two Cisco 12G SAS HBAs to control SAS/SATA drives.
- Two power supplies with support for N and N+1 power redundancy modes.
- Network connectivity through either a Serial port (RJ-45 connector) COM 1, BMC or Host Serial access or RJ45 BMC Dedicated Management Port.
- Support for the following new UCS VIC 1400 Series adapters:
  - VIC 1467 10/25G MLOM for C-Series (Cisco UCS VIC 1467 MLOM)
  - VIC 1477 40/100G MLOM for C-Series (Cisco UCS VIC 1477 MLOM)

Cisco UCS C245 M6 Server

Cisco UCS Manager now supports Cisco UCS C245 M6 servers with Rome Processors.

Intel MR6

Support for Intel MR6 for M6 server platforms.

New Hardware in Release 4.2(1i)

Cisco UCS C245 M6 Server

Cisco UCS C245 M6 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. Cisco UCS C245 M6 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 Manager supports only Cisco UCS C245 M6 servers with Milan Processors only.

Cisco UCS C245 M6 servers are supported only with Cisco UCS 6454, 64108, and 6300 Fabric Interconnects.

The server supports the following features:

- A maximum of two 3rd Gen AMD EPYC CPUs.
- 16 DIMM slots per CPU for 3200-MHz DDR4 DIMMs with individual DIMM capacity points up to 256 GB. The maximum memory capacity for 2 CPUs is 8 TB (for 32 x 256 GB DDR4 DIMMs.
- Up to 24 front SFF SAS/SATA HDDs or SSDs (optionally up to 4 of the drives can be NVMe).
- Up to 8 PCie slots using three rear risers, or Storage-centric option provides three rear risers with a total of up to 4 NVMe SFF drives and 3 PCIe slots.
- The server provides internal slots for one Cisco 12G SAS RAID controllers with 4 GB cache backup to control SAS/SATA drives, or Up to two Cisco 12G SAS HBAs to control SAS/SATA drives.
- Two power supplies with support for N and N+1 power redundancy modes.
- Network connectivity through either a Serial port (RJ-45 connector) COM 1, BMC or Host Serial access or RJ45 BMC Dedicated Management Port.
- Support for the following new UCS VIC 1400 Series adapters:
  - VIC 1467 10/25G MLOM for C-Series (Cisco UCS VIC 1467 MLOM)
  - VIC 1477 40/100G MLOM for C-Series (Cisco UCS VIC 1477 MLOM)

New Hardware in Release 4.2(1f)

Peripherals

- Support for NVIDIA A10 GPU (PCIe FHFL SS 24GB 150W) in Cisco UCS C240 and C245 M6 servers along with NVIDIA A100 GPU.
- Support for NVIDIA T4 PCIe 16GB 70W (T4 GPU) in Cisco UCS C220 and C225 M6 servers.

New Hardware in Release 4.2(1d)

Cisco UCS B200 M6 Server

Cisco UCS B200 M6 Server is a half-width blade server that is designed for the Cisco UCS 5108 Blade Server Chassis. You can install up to eight UCS B200 M6 blade servers in a UCS 5108 chassis, mixing with other models of Cisco UCS blade servers in the chassis if desired.

The server supports the following features:

- Two CPU sockets for Third Generation Intel Xeon Scalable family of CPUs support one or two CPU blade configurations.
- Up to 32 DDR4 DIMMs (16 sockets/8 channels per CPU). 32 DIMM slots for industry-standard DDR4 memory at speeds up to 3200 MHz, with up to 8 TB of total memory when using 256 GB DIMMs. Up to 16 DIMM slots ready for Intel Optane DC PMem to accommodate up to 12 TB of Intel Optane DC persistent memory.
- One front mezzanine storage module with the following options:
  - Cisco FlexStorage module supporting two 7 mm SATA SSDs. A 12G SAS controller chip is included on the module to provide hardware RAID for the two drives.
  - Cisco FlexStorage module supporting two mini-storage modules, module "1" and module "2." Each mini-storage module is a SATA M.2 dual-SSD mini-storage module that includes an on-board SATA RAID controller chip. Each RAID controller chip manages two SATA M.2 dual SSD modules.
  - Rear mLOM, which is required for blade discovery. This mLOM VIC card (for example, a Cisco VIC 1440) can provide per fabric connectivity of 20 G or 40 G when used with the pass-through Cisco UCS Port Expander Card in the rear mezzanine slot. Cisco UCS B200 M6 server supports NVMe Drive with pass-through adapter module supporting two 7 mm NVME SSDs.
  - Optionally, the rear mezzanine slot can have a Cisco VIC Card (for example, a Cisco VIC 1480) or the pass-through Cisco UCS Port Expander Card.



Note Component support is subject to chassis power configuration restrictions.

Cisco UCS B200 M6 Servers are not supported with Cisco UCS 6200 series Fabric Interconnect.

Cisco UCS C220 M6 Server

Cisco UCS C220 M6 Server is a one-rack unit server that can be used standalone, or as part of the Cisco Unified Computing System, which unifies computing, networking, management, virtualization, and storage access into a single integrated architecture.

The server supports the following features:

- A maximum of two 3rd Generation Intel Xeon processors.
- 32 DD4 DIMMs (16 per CPU) for a total system memory of either 8 TB (32 x 256 GB DDR4 DIMMs) or 12 TB (16 x 256 GB DDR4 DIMMs1 and 16 x 512 GB Intel® Optane™ Persistent Memory Module (PMEMs)).
- 3 PCI Express riser connectors, which provide slots for “full height” and “half height” PCI-e adapters.

- Two Titanium (80 PLUS rated) power supplies with support for N and N+1 power redundancy modes.
- 2 x 10GBase-T Ethernet LAN over Motherboard (LOM) ports for network connectivity, plus one 1 Gb Ethernet dedicated management port.
- One mLOM card provides 2 x 100 Gig Ethernet ports. Cisco UCS 220 M6 server supports 2 x 100 G [Cisco UCS VIC 1477] and 4 x 25 G [Cisco UCS VIC 1467] MLOM adapters.
- One KVM port on the front of the server.
- Two different front-loading hardware configurations are available:
  - UCSC-C220-M6S
  - UCSC-C220-M6N
- Rear PCI risers are supported as one to three half-height PCIe risers, or one to two full-height PCIe risers.
- The server provides an internal slot for one of the following:
  - SATA Interposer to control SATA drives from the PCH (AHCI), or
  - Cisco 12 G RAID controller with cache backup to control SAS/SATA drives, or
  - Cisco 12 G SAS pass-through HBA to control SAS/SATA drives.



Note Cisco UCS C220 M6 Servers are not supported with Cisco UCS 6200 series Fabric Interconnect.

Cisco UCS C240 M6 Server

Cisco UCS C240 M6 Server is a 2 rack-unit, rack server chassis that can operate in both standalone environments and as part of the Cisco Unified Computing System (Cisco UCS). Cisco UCS C240 M6 Servers support a maximum of two 3rd Gen Intel® Xeon® Scalable Processors, in either one or two CPU configurations.

The server supports the following features:

- 16 DIMM slots per CPU for 3200-MHz DDR4 DIMMs in capacities up to 256 GB DIMMs.
- A maximum of 8 TB of memory is supported for a dual CPU configuration populated with either:
  - DIMM memory configurations of either 32 256 GB DDR DIMMs, or
  - 16 x 256 GB DDR4 DIMMs plus 16 x 256 GB Intel® Optane™ Persistent Memory Modules (PMEMs).
- The servers have different supported drive configurations depending on whether they are configured with large form factor (LFF) or small form factor (SFF) front-loading drives.
- Internal slot for a 12 G SAS RAID controller with SuperCap for write cache backup, or for a SAS HBA.
- Network connectivity through either a dedicated modular LAN over motherboard card (mLOM) that accepts a series 14xx Cisco virtual interface card (VIC) or a third-party NIC. These options are in addition to Intel x550 10Gbase-T mLOM ports built into the server motherboard.
- Two power supplies (PSUs) that support N+1 power configuration.

- Six modular, hot swappable fans.
- Five different front-loading hardware configurations are available:
  - UCSC-C240-M6S
  - UCSC-C240-M6L
  - UCSC-C240-M6SX
  - UCSC-C240-M6N
  - UCSC-C240-M6SN



Note Cisco UCS C240 M6 Servers are not supported with Cisco UCS 6200 series Fabric Interconnect.

Peripherals

- Support for Key Management Interoperability Protocol (KMIP) Profiles Version 2.0 on UCS clients.
- Support for Cisco UCS M4 and M5 servers with Cisco UCS 6248, 6296, 6300, 6454, and 64108 Fabric Interconnect series.
- Support for NVIDIA A-100 GPU cards (UCSC-GPU-A100) on UCS C240 M6 servers.
- Support for Nexus 93180YC-FX3 at 25G connection with UCS VIC 1455, 1457, and 1467
- Support for UCS-M2-HWRAID on Cisco UCS C220 M6 Server and Cisco UCS C240 M6 Server
- Support for UCSB-RAID12G-M6 on Cisco UCS B200 M6 Server
- **UCS VIC 1400 Series Adapters**

  Support for the following new UCS VIC 1400 Series adapters on Cisco UCS C220 M6 Server and Cisco UCS C240 M6 Server:
  - VIC 1467 10/25G MLOM for C-Series (Cisco UCS VIC 1467 MLOM)
  - VIC 1477 40/100G MLOM for C-Series (Cisco UCS VIC 1477 MLOM)
- Support for Cisco UCS-MP-128GS-B0, UCS-MP-256GS-B0, and UCS-MP-512GS-B0 DIMMs.
- Support for the following plan of record (POR) and capacity for all namespaces in App Direct Mode and App Direct Non Interleaved memory type:

Table 8: Minimum and Maximum capacity values in App Direct memory type:

	Minimum Capacity			**Maximum Capacity**			
POR	4+4	8+4	8+8	4+4	8+1	8+4	8+8
128GB	4	4	8	504	126	504	1008
256GB	4	4	8	1012	253	1012	2024

	Minimum Capacity			Maximum Capacity			
512GB	4	4	8	2028	507	2028	4056

Table 9: Minimum and Maximum capacity values for App Direct Non Interleaved memory type :

	Minimum Capacity				Maximum Capacity			
POR	4+4	8+1	8+4	8+8	4+4	8+1	8+4	8+8
128GB	1	1	1	1	126	126	126	126
256GB	1	1	1	1	253	253	253	253
512GB	1	1	1	1	507	507	507	507

Table 10: Namespace capacity and Intel MPN

Capacity	Intel MPN
128 GB	NMB1XXD128GPSU4
128GB	NMB1XXD128GPSUF
256GB	NMB1XXD256GPSU4
256GB	NMB1XXD256GPSUF
512GB	NMB1XXD512GPSU4
512GB	NMB1XXD512GPSUF

Feature Enhancements

- Added support for Intel® Optane™ Data Center persistent memory 100 series.

Third-party Adapters Support

From Cisco UCS Manager Release 4.2.1, the following third-party adapters are supported:

- Intel E810CQDA2 2 x 100 GbE QSFP28 PCIe Network Interface Card on C220 M6 and C240 M6 servers (UCSC-P-I8D100GF)
- Intel E810XXVDA2 2 x 25/10 GbE SFP28 PCIe Network Interface Card on C220 M6 and C240 M6 servers (UCSC-P-I8D25GF)
- Intel E810XXVDA4L 4 x 25/10 GbE SFP28 PCIe Network Interface Card on C220 M6 and C240 M6 servers (UCSC-P-I8Q25GF)
- Intel E810CQDA1 1 x 100 GbE QSFP28 PCIe Network Interface Card on C220 M6 and C240 M6 servers (UCSC-P-I8S100GF)
- Mellanox ConnectX-6 MCX623106AC-CDAT 2 x 100 GbE QSFP56 PCIe Network Interface Card on C220 M6 and C240 M6 servers (UCSC-P-M6CD100GF)

- Mellanox ConnectX-6 MCX623106AS-CDAT 2 x 100 GbE QSFP56 PCIe Network Interface Card on C220 M6 and C240 M6 servers (UCSC-P-M6DD100GF)
- Intel XL710 T2 LG Dual port
- Emulex LPe35002 Gen 7 PCIe 4.0 Fibre Channel (FC) Host Bus Adapters (HBAs)
- Dell QLogic 2772 Dual Port 32GbE Fibre Channel Host Bus Adapter (HBA)

New Software in Release 4.2

New Software Features in Release 4.2(3s)

None

New Software Features in Release 4.2(3r)

None

New Software Features in Release 4.2(3p)

None

New Software Features in Release 4.2(3o)

Cisco UCS Manager supports TLS 1.3 connection with Cisco UCS Central.

New Software Features in Release 4.2(3n)

None

New Software Features in Release 4.2(3m)

None

New Software Features in Release 4.2(3l)

None

New Software Features in Release 4.2(3k)

None

New Software Features in Release 4.2(3k)

None

New Software Features in Release 4.2(3j)

None

New Software Features in Release 4.2(3i)

None

New Software Features in Release 4.2(3h)

None

New Software Features in Release 4.2(3g)

None

New Software Features in Release 4.2(3e)

None

New Software Features in Release 4.2(3d)

Feature Enhancements

- Beginning with release 4.2(3d), Cisco UCS Manager introduces **Password Encryption Key** to enhance security for backup configuration files. **Password Encryption Key**, by default, is not set once you upgrade to release 4.2(3d). For more information how to set the **Password Encryption Key**, see *Cisco UCS Manager Administration Management Guide 4.2* under Cisco UCS Manager Configuration Guides.
- Maximum data LUNs Per Target is increased from [1-1024] to [1-4096] for Linux and ESX OS for Cisco UCS 13xx, 14xx, 15xxx VIC series adapters.



Note This update is applicable to vHBA type FC Initiator only. Before downgrading from Cisco UCS Manager release 4.2(3d), change the LUNs Per Target configuration to [1-1024]. ESX 7.x and ESX 8.0 supports a total of 1024 LUNs per host.

- MAC limit is increased from 32K to 96K for Cisco UCS 6400 Series, Cisco UCS 64108, and Cisco UCS 6536 FIs.

New Software Features in Release 4.2(3b)

Software Enablement for New Hardware (Listed in the New hardware section)

Feature Enhancements

- Cisco UCS 6536 Fabric Interconnect supports splitting a single 40 Gigabit(G)/100G Quad Small Form-factor Pluggable (QSFP) port into four 10G/25G ports using a supported breakout cable. The switch has 32 40/100-Gbps Ethernet ports and 4 unified ports that can support 40/100-Gbps Ethernet ports or 16 Fiber Channel (FC) ports after breakout at 8/16/32-Gbps FC speeds. Port breakout is supported for Ethernet ports (1-32) and Unified ports (33-36).
- Added the support to configure the Ethernet breakout ports on Cisco UCS 6536 and Cisco UCS 6400 Series Fabric Interconnects (UCS FI 6454 and UCS FI 64108) without leading the Fabric Interconnect to reboot.



Note Cisco UCS Manager releases prior to 4.2(3b) continue to lead the Fabric Interconnect reboot after Ethernet breakout port configuration, on Cisco UCS 6400 Series Fabric Interconnects.

- In Cisco UCS 6536 Fabric Interconnect, all ports are enabled using a term-based subscription license.

License Management tab in the Cisco UCS Manager GUI is deprecated for Cisco UCS 6536 Fabric Interconnect. Scope license command is also deprecated.

- Beginning with release 4.2(3b), UCS Manager supports secured authentication for the transport email with the SMTP server. You can toggle SMTP Authentication between **Off** and **On**.
- Support for NVMe over ROCEv2 with ESXi for Cisco UCS VIC 15000 series adapters.
- Cisco UCS 6536 Fabric Interconnect supports Fibre Channel (FC) breakout port configuration. The FC breakout is supported on ports 36 through 33 when each port is configured with a four-port breakout cable. For example: Four FC breakout ports on the physical port 33 are numbered as 1/33/1, 1/33/2, 1/33/3, and 1/33/4.
- Cisco UCS Manager Release 4.2(3b) supports double-tagged packet forwarding, 802.1Q-in-802.1Q (Q-in-Q), with Cisco UCS 6400 and 6500 Series Fabric Interconnects.
- Beginning with Cisco UCS Manager Release 4.2(3b), UCS Manager supports the firmware management for the following NVIDIA A Series GPUs with and without Crypto-Embedded Controller (CEC):
  - NVIDIA A10
  - NVIDIA A16
  - NVIDIA A30
  - NVIDIA A40
  - NVIDIA A100-80GB

New Software Features in Release 4.2(2e)

None

New Software Features in Release 4.2(2d)

None

New Software Features in Release 4.2(2c)

None

New Software Features in Release 4.2(2a)

Software Enablement for New Hardware (Listed in the New hardware section)

Feature Enhancements

- Support for Cisco UCS VIC 1440+PE with Cisco UCS 6300/6400 fabric interconnects and 22xx series IOMs.
- Support of Cisco VIC 15428 MLOM 4-port adapters on Cisco UCS C-series M6 rack servers.
- Beginning Cisco UCS Manager release 4.2(2a), the Cisco SSL version is upgraded to 1.1.1l-fips on Cisco UCS Mini, UCS 6200 series, UCS 6300 series, and UCS 6400 Series Fabric Interconnects.

Note The updated Cisco SSL version may require updated SSH Clients, which support updated key exchanges.

- Creating a **Certificate Signing Request** (CSR) now supports a maximum of three Domain Name System (DNS).
- Release 4.2(2a) extends support to the enhanced vKVM console on Cisco UCS B200 M5 and B480 M5 servers.
- Added **Reset BIOS Password** option to Server Management actions. This option enables you to reset the BIOS password without using the F2 BIOS configuration prompt.
- Added support for enabling PNuOS with UEFI secure boot when configured in **UEFI Boot Mode** under Boot Policy.
- Port number 443 is now blocked for Cisco IMC OOB KVM IP addresses when Cisco IMC Web Service Admin State is in **Disabled** mode
- Added the ability to clear the **Server Personality** set by the installer and revert the server to **no personality state** in Cisco UCS C220 M6, C240 M6, C245 M6, C225 M6, and B200 M6 servers.
- Support of **Precision Time Protocol** (PTP) with VIC 15428 adapter on all current distributions of the Linux operating system.
- Support for 16K ring size on VIC 15428 adapter with eNIC driver on Linux operating systems, and eNIC driver on Windows and ESX operating systems
- Cisco UCS Manager now supports HDD/SSD and SAS/SATA drive types diagnostic self-test. If the drive fails self test, a major fault is raised. Cisco recommends that you backup the data and replace the drive. For more details, see Cisco UCS Manager Storage Management Guide, Release 4.2 or Cisco UCS Manager Server Management Using the CLI, Release 4.2.

Note This feature does not support NVME JBOD drives. You may use third-party tools to diagnose NVME JBOD disk errors.

- Support for Cisco UCS Mini fabric interconnects with Cisco UCS VIC 14xx series on Cisco UCS M5 rack-mount servers.
- fNIC support for FDMI on ESX 6.7 and 7.0.
- FDMI support for Redhat Enterprise Linux 8.6 and 9.0.
- FDMI is now supported for VIC 15428 adapters on all current Linux releases.
- Added the capability of auto negotiation on Ethernet server, Fabric Interconnects, or Interfaces to determine the optimal speed of the connected device. While configuring server ports, you can enable or disable auto-negotiate option.

Note Auto-negotiate must be disabled for 100Gps server port connected to N9K-C93180YC-FX3 in FEX mode.

- Added the capability to enable/disable RFC 5424 compliance. While configuring the syslog using Cisco UCS Manager, you can click **Enable** to display the syslog messages as per RFC 5424 format.

Note This option is applicable only for Cisco UCS 6400 Series Fabric Interconnects.

New Software Features in Release 4.2(1n)

None

New Software Features in Release 4.2(1m)

None

New Software Features in Release 4.2(1l) (Deprecated Release)

Software Enablement for New Hardware (Listed in the New hardware section)

Feature Enhancements

- Server Personality is now supported on Cisco UCS C225 M6 Server. If configured, Server Personality can be reverted to the unconfigured state via CLI command.

New Software Features in Release 4.2(1i)

Software Enablement for New Hardware (Listed in the New hardware section)

Feature Enhancements

- Added an option to revert a previously configured Server Personality on Cisco UCS C245 M6 Server, Cisco UCS C240 M6 Server, and Cisco UCS C220 M6 Server to a no personality state.

New Software Features in Release 4.2(1f)

Software Enablement for New Hardware (Listed in the New hardware section)

Feature Enhancements

- New property added to create and modify the Internet Group Management Protocol (IGMP) Source IP Proxy State in Multicast Policy.
- Added an option to disable the Lewisburg SATA AHCI controller on Cisco UCS M5 servers.
- Support to display the DIMM manufacturing date/country information in dmidecode's (SMBIOS) Asset Tag field.

- Support mechanism for 6400 series Fabric Interconnets to send the Registered State Change Notification (RSCN) when the Cisco UCS IOM port-channel membership changes.
- BIOS support on M6 servers for new functions for processor, RAS memory, and trusted platform support.

New Software Features in Release 4.2(1d)

Software Enablement for New Hardware (Listed in the New hardware section)

Feature Enhancements

- The Security Protocol and Data Model (SPDM) Specification, which challenges a device to prove its identity according to a specified level of device authentication, is supported on Cisco UCS M6 Servers. Additionally, SPDM allows uploads of up to 40 external security certificates to the BMC.
- Cisco UCS C220M6/C240M6 C-series M6 servers that support Aero PCIe SAS316-port storage controllers for Direct Attached Storage allow creation of an automatic configuration storage profile. Using an an autoconfiguration profile allows you to choose whether to have a newly inserted disk automatically moved to the Unconfigured-good state.
- Cisco UCS Manager now supports the watchdog timer function on Cisco UCS 6400 Series Fabric Interconnects with switch ports that are PFC mode enabled.
- Cisco UCS Manager now supports NVMe over Fibre Channel (FC-NVMe) on UCS 6300 series Fabric Interconnects, UCS 6454, and UCS 64108 Fabric Interconnects with Cisco UCS VIC 14xx series adapters on ESX 7.0, ESX 7.0 U1 and ESX 7.0u2.

  This support is also available on Cisco Standalone rack servers with Cisco UCS 14xx series adapters.
- Cisco UCS Manager now supports NVME over RDMA on Red Hat Enterprise Linux 7.9.
- Cisco UCS Manager now supports NVMe over Fibre Channel for ESX and Linux with Fibre Channel Direct Connect.
- Cisco UCS Manager now supports an Aggressive Cooling option as part of the Power Control policy for Cisco UCS M6 Servers.
- Cisco UCS M6 servers now display a Server Personality field in their General Properties if a server personality was configured for Cisco HyperFlex servers.
- The port VLAN count scale has been increased from 64,000 to 108,000 for Cisco UCS 6400 series Fabric Interconnect.
- The IP multicast group limit with Cisco UCS 6454 Fabric Interconnect and Cisco UCS IOM 2408, has been increased from 4000 entries to 16,000 entries.

Deprecated Hardware and Software in Cisco UCS Manager Release 4.2

The discovery of Cisco UCS B200, C220, and C240 M6 servers on Cisco UCS 6200 Series Fabric Interconnect is not supported.

Beginning with Cisco UCS Manager Release 4.2(1d), all M3 servers (UCS B22 Blade Server, B200 M3 Blade Server, B420 M3 Blade Server, and all C-Series M3 servers) are no longer supported on all platforms (UCS 6200 Series, 6300 Series, and 6400 Series Fabric Interconnects).

Beginning with Cisco UCS Manager Release 4.2(1d), the N2K-C2248TP-1GE FEX is no longer supported.

Cross-Version Firmware Support

The Cisco UCS Manager A bundle software (Cisco UCS Manager, Cisco NX-OS, IOM and FEX firmware) can be mixed with previous B or C bundle releases on the servers (host firmware [FW], BIOS, Cisco IMC, adapter FW and drivers).

The following table lists the mixed A, B, and C bundle versions that are supported on Cisco UCS 6200, 6300, 6400, and 6500 Series Fabric Interconnects:

Table 11: Mixed Cisco UCS Releases Supported on Cisco UCS 6200, 6300, 6400, 6500 Series Fabric Interconnects

	Infrastructure Versions (A Bundles)								
Host FW Versions (B or C Bundles)	4.0(1)	4.0(2)	4.0(4)	4.1(1)	4.1(2)	4.1(3)	4.2(1)	4.2(2)	4.2(3)
4.2(3)	—	—	—	—	—	—	6200, 6332, 6332-16UP, 6454, 64108	6200, 6332, 6332-16UP, 6454, 64108	6200, 6332, 6332-16UP, 6454, 64108, 6536
4.2(2)	—	—	—	—	—	—	6200, 6332, 6332-16UP, 6454, 64108	6200, 6332, 6332-16UP, 6454, 64108	6200, 6332, 6332-16UP, 6454, 64108
4.2(1)	—	—	—	—	—	—	6200, 6332, 6332-16UP, 6454, 64108	6200, 6332, 6332-16UP, 6454, 64108	6200, 6332, 6332-16UP, 6454, 64108
4.1(3)	—	—	—	6200, 6332, 6332-16UP, 6454, 64108	6200, 6332, 6332-16UP, 6454, 64108	6200, 6332, 6332-16UP, 6454, 64108	6200, 6332, 6332-16UP, 6454, 64108	6200, 6332, 6332-16UP, 6454, 64108	6200, 6332, 6332-16UP, 6454, 64108
4.1(2)	—	—	—	6200, 6332, 6332-16UP, 6454, 64108	6200, 6332, 6332-16UP, 6454, 64108	6200, 6332, 6332-16UP, 6454, 64108	6200, 6332, 6332-16UP, 6454, 64108	6200, 6332, 6332-16UP, 6454, 64108	6200, 6332, 6332-16UP, 6454, 64108
4.1(1)	—	—	—	6200, 6332, 6332-16UP, 6454, 64108	6200, 6332, 6332-16UP, 6454, 64108	6200, 6332, 6332-16UP, 6454, 64108	6200, 6332, 6332-16UP, 6454, 64108	6200, 6332, 6332-16UP, 6454, 64108	6200, 6332, 6332-16UP, 6454, 64108
4.0(4)	6200, 6332, 6332-16UP, 6454	6200, 6332, 6332-16UP, 6454	6200, 6332, 6332-16UP, 6454	6200, 6332, 6332-16UP, 6454	6200, 6332, 6332-16UP, 6454	6200, 6332, 6332-16UP, 6454	6200, 6332, 6332-16UP, 6454	6200, 6332, 6332-16UP, 6454	6200, 6332, 6332-16UP, 6454

	Infrastructure Versions (A Bundles)								
4.0(2)	6200, 6332, 6332-16UP, 6454	6200, 6332, 6332-16UP, 6454	6200, 6332, 6332-16UP, 6454	6200, 6332, 6332-16UP, 6454	6200, 6332, 6332-16UP, 6454	6200, 6332, 6332-16UP, 6454	6200, 6332, 6332-16UP, 6454	6200, 6332, 6332-16UP, 6454	6200, 6332, 6332-16UP, 6454
4.0(1)	6200, 6332, 6332-16UP, 6454	6200, 6332, 6332-16UP, 6454	6200, 6332, 6332-16UP, 6454	6200, 6332, 6332-16UP, 6454	6200, 6332, 6332-16UP, 6454	6200, 6332, 6332-16UP, 6454	6200, 6332, 6332-16UP, 6454	6200, 6332, 6332-16UP, 6454	6200, 6332, 6332-16UP, 6454

The following table lists the mixed A, B, and C bundle versions that are supported on Cisco UCS Mini fabric interconnects:

Table 12: Mixed Cisco UCS Releases Supported on Cisco UCS Mini Fabric Interconnects

	Infrastructure Versions (A Bundles)								
Host FW Versions (B or C Bundles)	4.0(1)	4.0(2)	4.0(4)	4.1(1)	4.1(2)	4.1(3)	4.2(1)	4.2(2)	4.2(3)
4.2(3)	—	—	—	—	—	—	6324	6324	6324
4.2(2)	—	—	—	—	—	—	6324	6324	6324
4.2(1)	—	—	—	—	—	—	6324	6324	6324
4.1(3)	—	—	—	6324	6324	6324	6324	6324	6324
4.1(2)	—	—	—	6324	6324	6324	6324	6324	6324
4.1(1)	—	—	—	6324	6324	6324	6324	6324	6324
4.0(4)	6324	6324	6324	6324	6324	6324	6324	6324	6324
4.0(2)	6324	6324	6324	6324	6324	6324	6324	6324	6324
4.0(1)	6324	6324	6324	6324	6324	6324	6324	6324	6324

The following table lists the mixed B, C bundles that are supported on all platforms with the 4.2(3)A bundle:

Table 13: Mixed B, C Bundles Supported on All Platforms with the 4.2(3)A Bundle

	Infrastructure Versions (A Bundles)				
Host FW Versions (B, C Bundles)	4.2(3)				
	6200	6300	6324	6400	6500
	ucs-k9-bundle-infra.4.2.3b.A.bin	ucs-6300-k9-bundle-infra.4.2.3b.A.bin	ucs-mini-k9-bundle-infra.4.2.3b.A.bin	ucs-6400-k9-bundle-infra.4.2.3b.A.bin	ucs-6500-k9-bundle-infra.4.2.3b.A.bin

	Infrastructure Versions (A Bundles)				
4.2(3)	Yes	Yes	Yes	Yes	Yes
4.2(2)	Yes	Yes	Yes	Yes	No
4.2(1)	Yes	Yes	Yes	Yes	No
4.1(3)	Yes	Yes	Yes	Yes	No
4.1(2)	Yes	Yes	Yes	Yes	No
4.1(1)	Yes	Yes	Yes	Yes	No
4.0(1), 4.0(4) (B, C Bundles)	Yes	Yes	Yes	Yes	No



Important If you implement cross-version firmware, you must ensure that the configurations for the Cisco UCS domain are supported by the firmware version on the server endpoints.

Cisco UCS NVMeoF Support Matrix for 3rd Party Storage Vendors

Table 14: Cisco UCS NVMeoF Support Matrix for 3rd Party Storage Vendors

Storage Vendor	Feature	Storage Array	Cisco UCS FI	Cisco UCS VIC	Operating System
NetApp, Inc®	NVMe-FC	ONTAP 9.7 onwards	Cisco UCS 6400 Series Cisco UCS 6536	Cisco UCS 1400 Series Cisco UCS 15000 Series	ESXi 7.0U3+, ESXi 8.0+, RHEL 8.6+, RHEL 9.0+, SLES 15SP3+
	Note Cisco UCS VIC 1300 series is supported Only with RHEL 8.6+				
	NVMe-TCP	ONTAP 9.10 onwards	Cisco UCS 6400 Series Cisco UCS 6536	Cisco UCS 1400 Series Cisco UCS 15000 Series	ESXi 7.0U3 +, ESXi 8.0 +, RHEL 9.0+, SLES 15SP3+

Storage Vendor	Feature	Storage Array	Cisco UCS FI	Cisco UCS VIC	Operating System
Pure Storage, Inc.®	NVMe-FC	Pure //X, //XL (Purity 6.1+)	Cisco UCS 6300 Series Cisco UCS 6400 Series Cisco UCS 6536	Cisco UCS 1300 Series Cisco UCS 1400 Series Cisco UCS 15000 Series	ESXi 7.0U2 +, ESXi 8.0, RHEL 8.4+, RHEL 9.0+, SLES 15SP1+
	Note Cisco UCS VIC 1300 series is supported Only with RHEL 8.6+				
	NVMe-ROCEv2	Pure //X, //XL (Purity 5.2.1+)	Cisco UCS 6300 Series Cisco UCS 6400 Series Cisco UCS 6536	Cisco UCS 1400 Series Cisco UCS 15000 Series	RHEL 7.2 +, RHEL 8.0 +, RHEL 9.0+, SLES 15SP1 +
	NVMe-ROCEv2	Pure //X, //XL (Purity 5.2.1+)	Cisco UCS 6400 Series Cisco UCS 6536	Cisco UCS 1400 Series Cisco UCS 15000 Series	ESXi 7.0U3 and ESXI 8.0
	NVMe-TCP	Pure //X, //XL (purity 6.4+)	Cisco UCS 6300 Series Cisco UCS 6400 Series Cisco UCS 6536	Cisco UCS 1400 Series Cisco UCS 15000 Series	ESXi 7.0U3 +, SLES 15SP3 +
Dell Inc.®	NVMe-FC	PowerStore, PowerMax	Cisco UCS 6300 Series Cisco UCS 6400 Series Cisco UCS 6536	Cisco UCS 1400 Series Cisco UCS 15000 Series	ESXi 7.0U3 +, SLES 15SP3 +
	NVMe-TCP	PowerStore	Cisco UCS 6300 Series Cisco UCS 6400 Series Cisco UCS 6536	Cisco UCS 1400 Series Cisco UCS 15000 Series	ESXi 7.0U3 +

Storage Vendor	Feature	Storage Array	Cisco UCS FI	Cisco UCS VIC	Operating System
IBM® Information Technology	NVMe-FC	IBM FlashSystem 9500 IBM FlashSystem 9200 IBM FlashSystem 9100 IBM FlashSystem 7300 IBM FlashSystem 7200 IBM FlashSystem 5200 IBM FlashSystem 5035 IBM FlashSystem 5015	Cisco UCS 6400 Series	Cisco UCS VIC 1440 Cisco UCS VIC 1480 Cisco UCS VIC 1340 Cisco UCS VIC 1380	ESXi 8.0+, RHEL 8.6+ , SLES 15SP4+, SLES 15SP3+, UEK R6 U3+, Windows 2022+ and Citrix Hypervisor8.2+

Internal Dependencies

The following sections provide information on the interdependencies between Cisco UCS hardware and versions of Cisco UCS Manager.

- Version dependencies for Server FRU items such as DIMMs depend on the server type.
- Chassis items such as fans and power supplies work with all versions of Cisco UCS Manager.

Cisco UCS 6536, 6400, 6300, 6332, and 6200 Series Fabric Interconnects and Components

Blade Servers

Note In a mixed firmware configuration, we recommend that the minimum server bundle corresponds to the Minimum Software Version. The infrastructure must be at or above the Minimum Software Version.

Table 15: Minimum Host Firmware Versions for Blade Servers

Servers	Minimum Software Version UCS 6200 Series FI	Minimum Software Version UCS 6324, UCS 6332, 6332-16UP FI	Minimum Software Version UCS 6324, UCS 6332, 6332-16UP FI		Minimum Software Version UCS 6454 FI	Minimum Software Version UCS 64108 FI	Minimum Software Version UCS 6536 FI	Suggested Software Version UCS 6200 Series FI UCS 6324 Series FI UCS 6332, 6332-16UP FI UCS 6400 Series FI UCS 6536 Series FI
	UCS-IOM- 2204 UCS-IOM- 2208	UCS-IOM- 2204 UCS-IOM- 2208	UCS-IOM- 2304	UCS-IOM-2304V2	UCS-IOM- 2204 UCS-IOM- 2208 UCS-IOM- 2408*	UCS-IOM- 2204 UCS-IOM- 2208 UCS-IOM- 2408*	UCS-IOM-2304V1/V2 UCS-IOM- 2408	UCS-IOM-2204 UCS-IOM-2208 UCS-IOM-2408 UCS-IOM- 2304 UCS-IOM- 2304V2
					UCS-IOM-2408 support on M4 and M5 server is with UCS 1300/1400 series VIC adapters. UCS-IOM-2408 is supported with UCS 6400 Series/UCS 6536 FI UCS IOM-2304v1/v2 is supported with UCS 6300/UCS 6536 FI UCS IOM-220x is supported with UCS 6200 series/UCS 6300 series/UCS 6400 series FI. Cisco UCS M6 servers are not supported with 6200 series FI Cisco UCS 6536 FI supports Cisco UCS M4 servers only with Cisco UCS VIC 1300 Series			
B200 M6	N/A	4.2(1d)	4.2(1d)	4.2(1d)	4.2(1d)	4.2(1d)	4.2(3b)	4.2(3s)
B200 M5	3.2(1d)	3.2(1d)	3.2(1d)	4.0(4o)	4.0(1a)	4.1(1a)	4.2(3b)	4.2(3s)
B480 M5	3.2(2b)	3.2(2b)	3.2(2b)	4.0(4o)	4.0(1a)	4.1(1a)	4.2(3b)	4.2(3s)
B200 M4	2.2(8a)	3.1(3a)	3.1(3a)	4.0(4o)	4.0(1a)	4.1(1a)	4.2(3b)	4.2(3s)
B260 M4 E7-2800 v2 **B260 M4 E7-4800 v2** **B260 M4 E7-8800 v2** **B260 M4 E7-4800 v3** **B260 M4 E7-8800 v3**	2.2(8a) 2.2(8a) 2.2(8a) 2.2(8a) 2.2(8a)	3.1(3a) 3.1(3a) 3.1(3a) 3.1(3a) 3.1(3a)	3.1(3a)	4.0(4o)	4.0(1a)	4.1(1a)	4.2(3b)	4.2(3s)
B260 M4 E7-4800 v4 **B260 M4 E7-8800 v4**	2.2(8b) 2.2(8b)	3.1(3a) 3.1(3a)	3.1(3a) 3.1(3a)	4.0(4o)	4.0(1a)	4.1(1a)	4.2(3b)	4.2(3s)
B420 M4 E5-4600 v3 **B420 M4 E5-4600 v4**	2.2(8a) 2.2(8b)	3.1(3a) 3.1(3a)	3.1(3a) 3.1(3a)	4.0(4o)	4.0(1a)	4.1(1a)	4.2(3b)	4.2(3s)
B460 M4 E7-4800 v2 **B460 M4 E7-8800 v2** **B460 M4 E7-4800 v3** **B460 M4 E7-8800 v3**	2.2(8a) 2.2(8a) 2.2(8a) 2.2(8a)	3.1(3a) 3.1(3a) 3.1(3a) 3.1(3a)	3.1(3a)	4.0(4o)	4.0(1a)	4.1(1a)	4.2(3b)	4.2(3s)
B460 M4 E7-4800 v4 **B460 M4 E7-8800 v4**	2.2(8b) 2.2(8b)	3.1(3a) 3.1(3a)	3.1(3a)	4.0(4o)	4.0(1a)	4.1(1a)	4.2(3b)	4.2(3s)

Rack Servers

Note In a mixed firmware configuration, we recommend that the minimum server bundle corresponds to the Minimum Software Version. The infrastructure must be at or above the Minimum Software Version.

Table 16: Minimum Host Firmware Versions for Rack Servers

Servers	Minimum Software Version UCS 6200 Series FI	Minimum Software Version UCS 6332, 6332-16UP	Minimum Software Version UCS 6454	Minimum Software Version UCS 64108	Minimum Software Version UCS 6536	Suggested Software Version UCS 6200 Series FI UCS 6332, 6332-16UP FI UCS 6400 Series FI
Cisco UCS M6 servers are not supported with 6200 series FI						
C220 M6	N/A	4.2(1d)	4.2(1d)	4.2(1d)	4.2(3b)	4.2(3s)
C240 M6	N/A	4.2(1d)	4.2(1d)	4.2(1d)	4.2(3b)	4.2(3s)
C225 M6	N/A	4.2(1l)	4.2(1l)	4.2(1l)	4.2(3b)	4.2(3s)
C245 M6	N/A	4.2(1i)	4.2(1i)	4.2(1i)	4.2(3b)	4.2(3s)
C220 M5	3.2(1d)	3.2(1d)	4.0(1a)	4.1(1a)	4.2(3b)	4.2(3s)
C240 M5	3.2(1d)	3.2(1d)	4.0(1a)	4.1(1a)	4.2(3b)	4.2(3s)
C125 M5	NA	4.0(1a)	4.0(1a)	4.1(1a)	4.2(3b)	4.2(3s)
S3260 M5	3.2(3a)	3.2(3a)	4.0(1a)	4.1(1a)	4.2(3b)	4.2(3s)
C220 M4	2.2(8a)	3.1(3a)	4.0(1a)	4.1(1a)	4.2(3b)	4.2(3s)
C240 M4	2.2(8a)	3.1(3a)	4.0(1a)	4.1(1a)	4.2(3b)	4.2(3s)
C460 M4 E7-2800 v2 C460 M4 E7-4800 v2 C460 M4 E7-8800 v2 C460 M4 E7-4800 v3 C460 M4 E7-8800 v3	2.2(8a) 2.2(8a) 2.2(8a) 2.2(8a) 2.2(8a)	3.1(3a) 3.1(3a) 3.1(3a) 3.1(3a) 3.1(3a)	4.0(1a)	4.1(1a)	4.2(3b)	4.2(3s)

Servers	Minimum Software Version UCS 6200 Series FI	Minimum Software Version UCS 6332, 6332-16UP	Minimum Software Version UCS 6454	Minimum Software Version UCS 64108	Minimum Software Version UCS 6536	Suggested Software Version UCS 6200 Series FI UCS 6332, 6332-16UP FI UCS 6400 Series FI
Cisco UCS M6 servers are not supported with 6200 series FI						
C460 M4 E7-8800 v4	2.2(8b)	3.1(3a)	4.0(1a)	4.1(1a)	4.2(3b)	4.2(3s)
C480 M5	3.2(2b)	3.2(2b)	4.0(1a)	4.1(1a)	4.2(3b)	4.2(3s)
S3260 M4	3.1(2b)	3.1(3a)	4.0(1a)	4.1(1a)	NA	4.2(3s)

Adapters

Table 17: Minimum Software Versions for Adapters

Adapters	Minimum Software Version UCS 6200 Series FI	Minimum Software Version UCS 6332, 6332-16UP	Minimum Software Version UCS 6332, 6332-16UP	Minimum Software Version UCS 6332, 6332 -16UP	Minimum Software Version UCS 6454	Minimum Software Version UCS 6454	Minimum Software Version UCS 64108	Minimum Software Version UCS 6536	Minimum Software Version UCS 6536	Suggested Software Version UCS 6200 Series FI UCS 6332, 6332-16UP FI UCS 6400 Series FI UCS 6500 Series FI
	UCS-IOM -2204 UCS-IOM -2208	UCS-IOM -2204 UCS-IOM -2208	UCS-IOM-2304 UCS-IOM-2304V2	2232 PP 2348	UCS-IOM- 2204 UCS-IOM -2208 UCS-IOM -2408*	93180YC -FX3 (25G server ports) 2232 PP 2348 UPQ	UCS-IOM -2204 UCS-IOM -2208 UCS-IOM -2408*	UCS-IOM -2304 V1/V2 UCS-IOM -2408	93180YC -FX3 (25G server ports) 2348 UPQ (10G server ports) 2232 PP	UCS-IOM -2204 UCS-IOM -2208 UCS-IOM -2408* UCS-IOM- 2304 UCS-IOM-2304V2
					* UCS-IOM-2408 supported on M4 and M5 only with UCS 6400 Series FI Cisco UCS IOMs are applicable only for Cisco UCS B-Series Servers					
UCSC-M-V5Q50G (Cisco UCS VIC 15428 MLOM 4-port adapter)	-	-	-	4.2(1d)	-	4.2(1d)	-	-	4.2(3b)	4.2(3s)

Adapters	Minimum Software Version UCS 6200 Series FI	Minimum Software Version UCS 6332, 6332-16UP	Minimum Software Version UCS 6332, 6332-16UP	Minimum Software Version UCS 6332, 6332 -16UP	Minimum Software Version UCS 6454	Minimum Software Version UCS 6454	Minimum Software Version UCS 64108	Minimum Software Version UCS 6536	Minimum Software Version UCS 6536	Suggested Software Version UCS 6200 Series FI UCS 6332, 6332-16UP FI UCS 6400 Series FI UCS 6500 Series FI
	UCS-IOM -2204 UCS-IOM -2208	UCS-IOM -2204 UCS-IOM -2208	UCS-IOM-2304 UCS-IOM-2304V2	2232 PP 2348	UCS-IOM-2204 UCS-IOM -2208 UCS-IOM -2408*	93180YC -FX3 (25G server ports) 2232 PP 2348 UPQ	UCS-IOM -2204 UCS-IOM -2208 UCS-IOM -2408*	UCS-IOM -2304 V1/V2 UCS-IOM -2408	93180YC -FX3 (25G server ports) 2348 UPQ (10G server ports) 2232 PP	UCS-IOM -2204 UCS-IOM -2208 UCS-IOM -2408* UCS-IOM- 2304 UCS-IOM-2304V2
					* UCS-IOM-2408 supported on M4 and M5 only with UCS 6400 Series FI Cisco UCS IOMs are applicable only for Cisco UCS B-Series Servers					
UCSC-M-V5D200G (Cisco UCS VIC 15238 MLOM adapter) Direct Attached only	-	4.2(3b) Direct Attached only	4.2(3b) Direct Attached only	4.2(3b) Direct Attached only	-	-	-	4.2(3b) Direct Attached only (40/100G)	4.2(3b) Direct Attached only (40/100G)	4.2(3s)
UCSBMLV5Q 10G (Cisco VIC 15411)	-	4.2(1d)	4.2(1d)	-	4.2(1d)	-	4.2(1d)	4.2(3b)	-	4.2(3s)
UCSC-PCIE-C100 -04 (Cisco UCS VIC 1495)	4.0(2a)	4.0(2a)	4.0(2a)	-	4.0(2a)	-	4.0(2a)	4.2(3b) Direct Attach only (40/100G)	4.2(3b) Direct Attach only (40/100G)	4.2(3s)
UCSC-MLOM-C100 -04 (Cisco UCS VIC 1497)	4.0(2a)	4.0(2a)	4.0(2a)	-	4.0(2a)	-	4.0(2a)	4.2(3b) Direct Attach only (40/100G)	4.2(3b) Direct Attach only (40/100G)	4.2(3s)
UCSB-MLOM-40G-04 (UCS VIC 1440)	4.0(1a)	4.0(1a)	4.0(1a)	-	4.0(1a)	-	4.1(1a)	4.2(3b)	-	4.2(3s)
UCSCM- V25-04 (UCS VIC 1467)	-	-	-	4.2(1l)	-	4.2(1l)	-	-	4.2(3b)	4.2(3s)
UCSC-M-V100-04 (UCS VIC 1477)	-	4.2(1l)Direct Attached only			-	-	-	4.2(3b) Direct Attached only		4.2(3s)

Adapters	Minimum Software Version UCS 6200 Series FI	Minimum Software Version UCS 6332, 6332-16UP	Minimum Software Version UCS 6332, 6332-16UP	Minimum Software Version UCS 6332, 6332 -16UP	Minimum Software Version UCS 6454	Minimum Software Version UCS 6454	Minimum Software Version UCS 64108	Minimum Software Version UCS 6536	Minimum Software Version UCS 6536	Suggested Software Version UCS 6200 Series FI UCS 6332, 6332-16UP FI UCS 6400 Series FI UCS 6500 Series FI
	UCS-IOM -2204 UCS-IOM -2208	UCS-IOM -2204 UCS-IOM -2208	UCS-IOM-2304 UCS-IOM-2304V2	2232 PP 2348	UCS-IOM-2204 UCS-IOM -2208 UCS-IOM -2408*	93180YC -FX3 (25G server ports) 2232 PP 2348 UPQ	UCS-IOM -2204 UCS-IOM -2208 UCS-IOM -2408*	UCS-IOM -2304 V1/V2 UCS-IOM -2408	93180YC -FX3 (25G server ports) 2348 UPQ (10G server ports) 2232 PP	UCS-IOM -2204 UCS-IOM -2208 UCS-IOM -2408* UCS-IOM- 2304 UCS-IOM-2304V2
					* UCS-IOM-2408 supported on M4 and M5 only with UCS 6400 Series FI Cisco UCS IOMs are applicable only for Cisco UCS B-Series Servers					
UCSB-VIC-M84-4P (UCS VIC 1480)	4.0(1a)	4.0(1a)	4.0(1a)	-	4.0(1a)	-	4.1(1a)	4.2(3b)	-	4.2(3s)
UCSC-PCIE-C25Q-04 (UCS VIC 1455)	4.0(1a)	4.0(1a)	4.0(1a)	4.0(1a)	4.0(1a)	4.0(1a)	4.1(1a)	-	4.2(3b)	4.2(3s)
UCSC-MLOM-C25Q-04 (UCS VIC 1457)	4.0(1a)	4.0(1a)	4.0(1a)	4.0(1a)	4.0(1a)	4.0(1a)	4.1(1a)	-	4.2(3b)	4.2(3s)
UCSC-PCIE-C40Q -03 (UCS VIC 1385) UCSC-MLOM-C40Q -03 (UCS VIC 1387)	2.2(8a)	3.1(3a)	3.1(3a)	4.0(1a)	4.0(1a)	4.0(1a)	4.1(1a)	-	4.2(3b)	4.2(3s)
UCSB-MLOM-40G-03 (UCS VIC 1340) UCSB-VIC-M83-8P (UCS VIC 1380) UCSC-MLOM-CSC -02 (UCS VIC 1227)	2.2(8a)	3.1(3a)	3.1(3a)	-	4.0(1a)	-	4.1(1a)	4.2(3b)	-	4.2(3s)
UCSC-PCIE-CSC-02 (UCS VIC 1225)	2.2(8a)	3.1(3a)	3.1(3a)	-	4.0(1a)	-	4.1(1a)	-	-	-

Adapters	Minimum Software Version UCS 6200 Series FI	Minimum Software Version UCS 6332, 6332-16UP	Minimum Software Version UCS 6332, 6332-16UP	Minimum Software Version UCS 6332, 6332 -16UP	Minimum Software Version UCS 6454	Minimum Software Version UCS 6454	Minimum Software Version UCS 64108	Minimum Software Version UCS 6536	Minimum Software Version UCS 6536	Suggested Software Version UCS 6200 Series FI UCS 6332, 6332-16UP FI UCS 6400 Series FI UCS 6500 Series FI
	UCS-IOM -2204 UCS-IOM -2208	UCS-IOM -2204 UCS-IOM -2208	UCS-IOM-2304 UCS-IOM-2304V2	2232 PP 2348	UCS-IOM-2204 UCS-IOM -2208 UCS-IOM -2408*	93180YC -FX3 (25G server ports) 2232 PP 2348 UPQ	UCS-IOM -2204 UCS-IOM -2208 UCS-IOM -2408*	UCS-IOM -2304 V1/V2 UCS-IOM -2408	93180YC -FX3 (25G server ports) 2348 UPQ (10G server ports) 2232 PP	UCS-IOM -2204 UCS-IOM -2208 UCS-IOM -2408* UCS-IOM- 2304 UCS-IOM-2304V2
					* UCS-IOM-2408 supported on M4 and M5 only with UCS 6400 Series FI Cisco UCS IOMs are applicable only for Cisco UCS B-Series Servers					
UCSC-P- M5S100GF (Mellanox ConnectX-5 MCX515A- CCAT 1 x 100GbE QSFP PCI NIC)	4.1(1a)	4.1(1a)	4.1(1a)	-	4.1(1a)	-	4.1(1a)	-	-	4.2(3s)
UCSC-P -M5D25GF (Mellanox ConnectX-5 MCX512A- ACAT 2 x 25Gb/10GbE SFP PCI)	4.1(1a)	4.1(1a)	4.1(1a)	-	4.1(1a)	-	4.1(1a)	-	-	4.2(3s)
UCSC-O- M5S100GF (Mellanox ConnectX-5 MCX545B- ECAN 1 x 100GbE QSFP PCI NIC)	4.1(1a)	4.1(1a)	4.1(1a)	-	4.1(1a)	-	4.1(1a)	-	-	4.2(3s)
UCSC-P -M4D25GF (Mellanox MCX4121A -ACAT Dual Port 10/25G SFP28 NIC)	4.0(4o)	4.0(4o)	4.0(4o)	-	4.0(4o)	-	4.1(1a)	-	-	4.2(3s)
UCSC-PCIE-QS100GF (QLogic QL45611HLCU 100GbE)	4.0(4o)	4.0(4o)	4.0(2a)	-	4.0(4o)	-	4.1(1a)	-	-	4.2(3s)
UCSC-PCIE -BD16GF (Emulex LPe31002 Dual-Port 16G FC HBA)	3.2(3a)	3.2(3a)	3.2(3a)	-	4.0(1a)	-	4.1(1a)	-	-	4.2(3s)

Adapters	Minimum Software Version UCS 6200 Series FI	Minimum Software Version UCS 6332, 6332-16UP	Minimum Software Version UCS 6332, 6332-16UP	Minimum Software Version UCS 6332, 6332 -16UP	Minimum Software Version UCS 6454	Minimum Software Version UCS 6454	Minimum Software Version UCS 64108	Minimum Software Version UCS 6536	Minimum Software Version UCS 6536	Suggested Software Version UCS 6200 Series FI UCS 6332, 6332-16UP FI UCS 6400 Series FI UCS 6500 Series FI
	UCS-IOM -2204 UCS-IOM -2208	UCS-IOM -2204 UCS-IOM -2208	UCS-IOM-2304 UCS-IOM-2304V2	2232 PP 2348	UCS-IOM-2204 UCS-IOM -2208 UCS-IOM -2408*	93180YC -FX3 (25G server ports) 2232 PP 2348 UPQ	UCS-IOM -2204 UCS-IOM -2208 UCS-IOM -2408*	UCS-IOM -2304 V1/V2 UCS-IOM -2408	93180YC -FX3 (25G server ports) 2348 UPQ (10G server ports) 2232 PP	UCS-IOM -2204 UCS-IOM -2208 UCS-IOM -2408* UCS-IOM- 2304 UCS-IOM-2304V2
					* UCS-IOM-2408 supported on M4 and M5 only with UCS 6400 Series FI Cisco UCS IOMs are applicable only for Cisco UCS B-Series Servers					
UCSC-PCIE -ID40GF (Intel XL710 adapter)	3.2(3a)	3.2(3a)	3.2(3a)	-	4.0(1a)	-	4.1(1a)	-	-	4.2(3s)
UCSC-PCIE -IQ10GF (Intel X710-DA4 adapter)	3.2(3a)	3.2(3a)	3.2(3a)	-	4.0(1a)	-	4.1(1a)	-	-	4.2(3s)
UCSC-PCIE -ID10GF (Intel X710-DA2 adapter)	3.2(3a)	3.2(3a)	3.2(3a)	-	4.0(1a)	-	4.1(1a)	-	-	4.2(3s)
UCSC-PCIE -ID25GF (Intel XXV710-DA2 Dual port 25 Gigabit Ethernet PCIe adapter)	3.2(3a)	3.2(3a)	3.2(3a)	-	4.0(1a)	-	4.1(1a)	-	-	4.2(3s)
UCSC-PCIE -ID10GC (Intel X550-T2 adapter)	3.2(3a)	3.2(3a)	3.2(3a)	-	4.0(1a)	-	4.1(1a)	-	-	4.2(3s)
N2XX-AIPCI01 (Intel X520 dual port adapter)	3.2(3a)	3.2(3a)	3.2(3a)	-	4.0(1a)	-	4.1(1a)	-	-	4.2(3s)
UCSC-PCIE -ID25GF (Intel X710 25Gb Dual-port BaseT)	3.2(3a)	3.2(3a)	3.2(3a)	-	4.0(1a)	-	4.1(1a)	-	-	4.2(3s)
UCSC-PCIE -QD40GF (QLogic QL45412H 40GbE)	3.2(2b)	3.2(2b)	3.2(2b)	-	4.0(1a)	-	4.1(1a)	-	-	4.2(3s)

Adapters	Minimum Software Version UCS 6200 Series FI	Minimum Software Version UCS 6332, 6332-16UP	Minimum Software Version UCS 6332, 6332-16UP	Minimum Software Version UCS 6332, 6332 -16UP	Minimum Software Version UCS 6454	Minimum Software Version UCS 6454	Minimum Software Version UCS 64108	Minimum Software Version UCS 6536	Minimum Software Version UCS 6536	Suggested Software Version UCS 6200 Series FI UCS 6332, 6332-16UP FI UCS 6400 Series FI UCS 6500 Series FI
	UCS-IOM -2204 UCS-IOM -2208	UCS-IOM -2204 UCS-IOM -2208	UCS-IOM-2304 UCS-IOM-2304V2	2232 PP 2348	UCS-IOM-2204 UCS-IOM -2208 UCS-IOM -2408*	93180YC -FX3 (25G server ports) 2232 PP 2348 UPQ	UCS-IOM -2204 UCS-IOM -2208 UCS-IOM -2408*	UCS-IOM -2304 V1/V2 UCS-IOM -2408	93180YC -FX3 (25G server ports) 2348 UPQ (10G server ports) 2232 PP	UCS-IOM -2204 UCS-IOM -2208 UCS-IOM -2408* UCS-IOM- 2304 UCS-IOM-2304V2
					* UCS-IOM-2408 supported on M4 and M5 only with UCS 6400 Series FI Cisco UCS IOMs are applicable only for Cisco UCS B-Series Servers					
UCSC-PCIE -IQ10GC (Intel X710-T4)	3.2(2b)	3.2(2b)	3.2(2b)	-	4.0(1a)	-	4.1(1a)	-	-	4.2(3s)
UCSC-PCIE -QD16GF (QLogic QLE2692-CSC)	3.2(1d)	3.2(1d)	3.2(1d)	-	4.0(1a)	-	4.1(1a)	-	-	4.2(3s)
UCS-VIC -M82-8P (UCS VIC 1280) UCSB-MLOM -40G-01 (UCS VIC 1240) UCSB-MLOM-PT-01 (Cisco Port Expander Card)	2.2(8a)	3.1(3a)	3.1(3a)	-	4.0(1a)	-	4.1(1a)	-	-	4.2(3s)

Adapters	Minimum Software Version UCS 6200 Series FI	Minimum Software Version UCS 6332, 6332-16UP	Minimum Software Version UCS 6332, 6332-16UP	Minimum Software Version UCS 6332, 6332 -16UP	Minimum Software Version UCS 6454	Minimum Software Version UCS 6454	Minimum Software Version UCS 64108	Minimum Software Version UCS 6536	Minimum Software Version UCS 6536	Suggested Software Version UCS 6200 Series FI UCS 6332, 6332-16UP FI UCS 6400 Series FI UCS 6500 Series FI
	UCS-IOM -2204 UCS-IOM -2208	UCS-IOM -2204 UCS-IOM -2208	UCS-IOM-2304 UCS-IOM-2304V2	2232 PP 2348	UCS-IOM-2204 UCS-IOM -2208 UCS-IOM -2408*	93180YC -FX3 (25G server ports) 2232 PP 2348 UPQ	UCS-IOM -2204 UCS-IOM -2208 UCS-IOM -2408*	UCS-IOM -2304 V1/V2 UCS-IOM -2408	93180YC -FX3 (25G server ports) 2348 UPQ (10G server ports) 2232 PP	UCS-IOM -2204 UCS-IOM -2208 UCS-IOM -2408* UCS-IOM- 2304 UCS-IOM-2304V2
					* UCS-IOM-2408 supported on M4 and M5 only with UCS 6400 Series FI Cisco UCS IOMs are applicable only for Cisco UCS B-Series Servers					
UCSC-F-FIO -1000MP (Cisco UCS Fusion ioMemory – PX600, 1.0TB) UCSC-F-FIO -1300MP (Cisco UCS Fusion ioMemory – PX600, 1.3TB) UCSC-F-FIO -2600MP (Cisco UCS Fusion ioMemory – PX600, 2.6TB) UCSC-F-FIO -5200MP (Cisco UCS Fusion ioMemory – PX600, 5.2TB)	2.2(8a)	3.1(3a)	3.1(3a)	-	4.0(1a)	-	4.1(1a)	-	-	4.2(3s)
UCSB-FIO -1600MS (Cisco UCS Fusion ioMemory Mezzanine SX300, 1.6TB) UCSB-FIO -1300MS (Cisco UCS Fusion ioMemory Mezzanine PX600, 1.3TB)	2.2(8a)	3.1(3a)	3.1(3a)	-	4.0(1a)	-	4.1(1a)	-	-	4.2(3s)

Adapters	Minimum Software Version UCS 6200 Series FI	Minimum Software Version UCS 6332, 6332-16UP	Minimum Software Version UCS 6332, 6332-16UP	Minimum Software Version UCS 6332, 6332 -16UP	Minimum Software Version UCS 6454	Minimum Software Version UCS 6454	Minimum Software Version UCS 64108	Minimum Software Version UCS 6536	Minimum Software Version UCS 6536	Suggested Software Version UCS 6200 Series FI UCS 6332, 6332-16UP FI UCS 6400 Series FI UCS 6500 Series FI
	UCS-IOM -2204 UCS-IOM -2208	UCS-IOM -2204 UCS-IOM -2208	UCS-IOM-2304 UCS-IOM-2304V2	2232 PP 2348	UCS-IOM- 2204 UCS-IOM -2208 UCS-IOM -2408*	93180YC -FX3 (25G server ports) 2232 PP 2348 UPQ	UCS-IOM -2204 UCS-IOM -2208 UCS-IOM -2408*	UCS-IOM -2304 V1/V2 UCS-IOM -2408	93180YC -FX3 (25G server ports) 2348 UPQ (10G server ports) 2232 PP	UCS-IOM -2204 UCS-IOM -2208 UCS-IOM -2408* UCS-IOM- 2304 UCS-IOM-2304V2
					* UCS-IOM-2408 supported on M4 and M5 only with UCS 6400 Series FI Cisco UCS IOMs are applicable only for Cisco UCS B-Series Servers					
UCSC-INVADER -3108 UCSC-NYTRO -200GB (Cisco Nytro MegaRAID 200GB Controller)	2.2(8a)	3.1(3a)	3.1(3a)	-	4.0(1a)	-	4.1(1a)	-	-	4.2(3s)

Adapters	Minimum Software Version UCS 6200 Series FI	Minimum Software Version UCS 6332, 6332-16UP	Minimum Software Version UCS 6332, 6332-16UP	Minimum Software Version UCS 6332, 6332 -16UP	Minimum Software Version UCS 6454	Minimum Software Version UCS 6454	Minimum Software Version UCS 64108	Minimum Software Version UCS 6536	Minimum Software Version UCS 6536	Suggested Software Version UCS 6200 Series FI UCS 6332, 6332-16UP FI UCS 6400 Series FI UCS 6500 Series FI
	UCS-IOM -2204 UCS-IOM -2208	UCS-IOM -2204 UCS-IOM -2208	UCS-IOM-2304 UCS-IOM-2304V2	2232 PP 2348	UCS-IOM-2204 UCS-IOM -2208 UCS-IOM -2408*	93180YC -FX3 (25G server ports) 2232 PP 2348 UPQ	UCS-IOM -2204 UCS-IOM -2208 UCS-IOM -2408*	UCS-IOM -2304 V1/V2 UCS-IOM -2408	93180YC -FX3 (25G server ports) 2348 UPQ (10G server ports) 2232 PP	UCS-IOM -2204 UCS-IOM -2208 UCS-IOM -2408* UCS-IOM- 2304 UCS-IOM-2304V2
					* UCS-IOM-2408 supported on M4 and M5 only with UCS 6400 Series FI Cisco UCS IOMs are applicable only for Cisco UCS B-Series Servers					
	2.2(8a)	3.1(3a)	3.1(3a)	-	4.0(1a)	-	4.1(1a)	-	-	4.2(3s)

Adapters	Minimum Software Version UCS 6200 Series FI	Minimum Software Version UCS 6332, 6332-16UP	Minimum Software Version UCS 6332, 6332-16UP	Minimum Software Version UCS 6332, 6332 -16UP	Minimum Software Version UCS 6454	Minimum Software Version UCS 6454	Minimum Software Version UCS 64108	Minimum Software Version UCS 6536	Minimum Software Version UCS 6536	Suggested Software Version UCS 6200 Series FI UCS 6332, 6332-16UP FI UCS 6400 Series FI UCS 6500 Series FI
	UCS-IOM -2204 UCS-IOM -2208	UCS-IOM -2204 UCS-IOM -2208	UCS-IOM-2304 UCS-IOM-2304V2	2232 PP 2348	UCS-IOM- 2204 UCS-IOM -2208 UCS-IOM -2408*	93180YC -FX3 (25G server ports) 2232 PP 2348 UPQ	UCS-IOM -2204 UCS-IOM -2208 UCS-IOM -2408*	UCS-IOM -2304 V1/V2 UCS-IOM -2408	93180YC -FX3 (25G server ports) 2348 UPQ (10G server ports) 2232 PP	UCS-IOM -2204 UCS-IOM -2208 UCS-IOM -2408* UCS-IOM- 2304 UCS-IOM-2304V2
					* UCS-IOM-2408 supported on M4 and M5 only with UCS 6400 Series FI Cisco UCS IOMs are applicable only for Cisco UCS B-Series Servers					
UCSC-MLOM -C10T-02 (UCS VIC 1227T) UCSC-PCIE -C10T-02 (UCS VIC 1225T) UCSC-F-FIO -785M (Cisco UCS 785GB MLC Fusion ioDrive2 for C-Series Servers) UCSC-F-FIO -365M (Cisco UCS 365GB MLC Fusion ioDrive2 for C-Series Servers) UCSC-F-FIO -1205M (Cisco UCS 1205GB MLC Fusion ioDrive2 for C-Series Servers) UCSC-F-FIO -3000M (Cisco UCS 3.0TB MLC Fusion ioDrive2 for C-Series Servers) UCSC-F-FIO -1000PS (UCS 1000GB Fusion ioMemory3 PX Performance line for Rack										

Adapters	Minimum Software Version UCS 6200 Series FI	Minimum Software Version UCS 6332, 6332-16UP	Minimum Software Version UCS 6332, 6332-16UP	Minimum Software Version UCS 6332, 6332 -16UP	Minimum Software Version UCS 6454	Minimum Software Version UCS 6454	Minimum Software Version UCS 64108	Minimum Software Version UCS 6536	Minimum Software Version UCS 6536	Suggested Software Version UCS 6200 Series FI UCS 6332, 6332-16UP FI UCS 6400 Series FI UCS 6500 Series FI
	UCS-IOM -2204 UCS-IOM -2208	UCS-IOM -2204 UCS-IOM -2208	UCS-IOM-2304 UCS-IOM-2304V2	2232 PP 2348	UCS-IOM-2204 UCS-IOM -2208 UCS-IOM -2408*	93180YC -FX3 (25G server ports) 2232 PP 2348 UPQ	UCS-IOM -2204 UCS-IOM -2208 UCS-IOM -2408*	UCS-IOM -2304 V1/V2 UCS-IOM -2408	93180YC -FX3 (25G server ports) 2348 UPQ (10G server ports) 2232 PP	UCS-IOM -2204 UCS-IOM -2208 UCS-IOM -2408* UCS-IOM- 2304 UCS-IOM-2304V2
					* UCS-IOM-2408 supported on M4 and M5 only with UCS 6400 Series FI Cisco UCS IOMs are applicable only for Cisco UCS B-Series Servers					
M4) UCSC-F-FIO -1300PS (UCSC-F-FIO-1300PS) UCSC-F-FIO -2600PS (UCS 2600GB Fusion ioMemory3 PX Performance line for Rack M4) UCSC-F-FIO -5200PS (UCS 5200GB Fusion ioMemory3 PX Performance line for Rack M4) UCSC-F-FIO -6400SS (UCS 6400GB Fusion ioMemory3 SX Scale line for C-Series) UCSC-F-FIO -3200SS (UCS 3200GB Fusion ioMemory3SX Scale line for C-Series)										
UCSC-PCIE -E14102B (Emulex OCe14102B-F)	2.2(8a)	3.1(3a)	3.1(3a)	-	4.0(1a)	-	4.1(1a)	-	-	4.2(3s)

Adapters	Minimum Software Version UCS 6200 Series FI	Minimum Software Version UCS 6332, 6332-16UP	Minimum Software Version UCS 6332, 6332-16UP	Minimum Software Version UCS 6332, 6332 -16UP	Minimum Software Version UCS 6454	Minimum Software Version UCS 6454	Minimum Software Version UCS 64108	Minimum Software Version UCS 6536	Minimum Software Version UCS 6536	Suggested Software Version UCS 6200 Series FI / UCS 6332, 6332-16UP FI / UCS 6400 Series FI / UCS 6500 Series FI
	UCS-IOM -2204 UCS-IOM -2208	UCS-IOM -2204 UCS-IOM -2208	UCS-IOM-2304 UCS-IOM-2304V2	2232 PP 2348	UCS-IOM- 2204 UCS-IOM -2208 UCS-IOM -2408*	93180YC -FX3 (25G server ports) 2232 PP 2348 UPQ	UCS-IOM -2204 UCS-IOM -2208 UCS-IOM -2408*	UCS-IOM -2304 V1/V2 UCS-IOM -2408	93180YC -FX3 (25G server ports) 2348 UPQ (10G server ports) 2232 PP	UCS-IOM -2204 UCS-IOM -2208 UCS-IOM -2408* UCS-IOM- 2304 UCS-IOM-2304V2
					* UCS-IOM-2408 supported on M4 and M5 only with UCS 6400 Series FI Cisco UCS IOMs are applicable only for Cisco UCS B-Series Servers					
UCSC-PCIE -IQ10GF (Intel X710-DA4 adapter) UCSC-PCIE -ID10GF (Intel X710-DA2 adapter) UCSC-PCIE -ID40GF (Intel XL710 adapter)	—	—	3.1(3a)	-	4.0(1a)	-	4.1(1a)	-	-	4.2(3s)

Adapters	Minimum Software Version UCS 6200 Series FI	Minimum Software Version UCS 6332, 6332-16UP	Minimum Software Version UCS 6332, 6332-16UP	Minimum Software Version UCS 6332, 6332 -16UP	Minimum Software Version UCS 6454	Minimum Software Version UCS 6454	Minimum Software Version UCS 64108	Minimum Software Version UCS 6536	Minimum Software Version UCS 6536	Suggested Software Version UCS 6200 Series FI UCS 6332, 6332-16UP FI UCS 6400 Series FI UCS 6500 Series FI
	UCS-IOM -2204 UCS-IOM -2208	UCS-IOM -2204 UCS-IOM -2208	UCS-IOM-2304 UCS-IOM-2304V2	2232 PP 2348	UCS-IOM-2204 UCS-IOM -2208 UCS-IOM -2408*	93180YC -FX3 (25G server ports) 2232 PP 2348 UPQ	UCS-IOM -2204 UCS-IOM -2208 UCS-IOM -2408*	UCS-IOM -2304 V1/V2 UCS-IOM -2408	93180YC -FX3 (25G server ports) 2348 UPQ (10G server ports) 2232 PP	UCS-IOM -2204 UCS-IOM -2208 UCS-IOM -2408* UCS-IOM- 2304 UCS-IOM-2304V2
					* UCS-IOM-2408 supported on M4 and M5 only with UCS 6400 Series FI Cisco UCS IOMs are applicable only for Cisco UCS B-Series Servers					
	—	3.1(3a)	3.1(3a)	-	4.0(1a)	-	4.1(1a)	-	-	4.2(3s)

Adapters	Minimum Software Version UCS 6200 Series FI	Minimum Software Version UCS 6332, 6332-16UP	Minimum Software Version UCS 6332, 6332-16UP	Minimum Software Version UCS 6332, 6332 -16UP	Minimum Software Version UCS 6454	Minimum Software Version UCS 6454	Minimum Software Version UCS 64108	Minimum Software Version UCS 6536	Minimum Software Version UCS 6536	Suggested Software Version UCS 6200 Series FI UCS 6332, 6332-16UP FI UCS 6400 Series FI UCS 6500 Series FI
	UCS-IOM -2204 UCS-IOM -2208	UCS-IOM -2204 UCS-IOM -2208	UCS-IOM-2304 UCS-IOM-2304V2	2232 PP 2348	UCS-IOM-2204 UCS-IOM -2208 UCS-IOM -2408*	93180YC -FX3 (25G server ports) 2232 PP 2348 UPQ	UCS-IOM -2204 UCS-IOM -2208 UCS-IOM -2408*	UCS-IOM -2304 V1/V2 UCS-IOM -2408	93180YC -FX3 (25G server ports) 2348 UPQ (10G server ports) 2232 PP	UCS-IOM -2204 UCS-IOM -2208 UCS-IOM -2408* UCS-IOM- 2304 UCS-IOM-2304V2
					* UCS-IOM-2408 supported on M4 and M5 only with UCS 6400 Series FI Cisco UCS IOMs are applicable only for Cisco UCS B-Series Servers					
UCSC-F-I80010 (Intel P3700 HHHL 800GB NVMe PCIe SSD) UCSC-F-I12003 (Intel P3600 HHHL 1200GB NVMe PCIe SSD) UCSC-F-I160010 (Intel P3700 HHHL 1600GB NVMe PCIe SSD) UCSC-F-I20003 (Intel P3600 HHHL 2000GB NVMe PCIe SSD) UCS-PCI25 -40010 (Intel P3700 400GB NVMe PCIe SSD) UCS-PCI25 -8003 (Intel P3600 800GB NVMe PCIe SSD) UCS-PCI25 -80010 (Intel P3700 800GB NVMe PCIe SSD) UCS-PCI25 -16003 (Intel P3600 1600GB NVMe PCIe SSD)										

Adapters	Minimum Software Version UCS 6200 Series FI	Minimum Software Version UCS 6332, 6332-16UP	Minimum Software Version UCS 6332, 6332-16UP	Minimum Software Version UCS 6332, 6332 -16UP	Minimum Software Version UCS 6454	Minimum Software Version UCS 6454	Minimum Software Version UCS 64108	Minimum Software Version UCS 6536	Minimum Software Version UCS 6536	Suggested Software Version UCS 6200 Series FI UCS 6332, 6332-16UP FI UCS 6400 Series FI UCS 6500 Series FI
	UCS-IOM -2204 UCS-IOM -2208	UCS-IOM -2204 UCS-IOM -2208	UCS-IOM-2304 UCS-IOM-2304V2	2232 PP 2348	UCS-IOM-2204 UCS-IOM -2208 UCS-IOM -2408*	93180YC -FX3 (25G server ports) 2232 PP 2348 UPQ	UCS-IOM -2204 UCS-IOM -2208 UCS-IOM -2408*	UCS-IOM -2304 V1/V2 UCS-IOM -2408	93180YC -FX3 (25G server ports) 2348 UPQ (10G server ports) 2232 PP	UCS-IOM -2204 UCS-IOM -2208 UCS-IOM -2408* UCS-IOM- 2304 UCS-IOM-2304V2
					* UCS-IOM-2408 supported on M4 and M5 only with UCS 6400 Series FI Cisco UCS IOMs are applicable only for Cisco UCS B-Series Servers					
UCSC-F-H19001 (UCS Rack PCIe/NVMe Storage 1900GB HGST SN150) UCSC-F-H38001 (UCS Rack PCIe/NVMe Storage 3800GB HGST SN150) UCS-PCI25 -38001 (UCS PCIe/NVMe2.5"SFF Storage 3800GB HGST SN100)										

Adapters	Minimum Software Version UCS 6200 Series FI	Minimum Software Version UCS 6332, 6332-16UP	Minimum Software Version UCS 6332, 6332-16UP	Minimum Software Version UCS 6332, 6332 -16UP	Minimum Software Version UCS 6454	Minimum Software Version UCS 6454	Minimum Software Version UCS 64108	Minimum Software Version UCS 6536	Minimum Software Version UCS 6536	Suggested Software Version UCS 6200 Series FI UCS 6332, 6332-16UP FI UCS 6400 Series FI UCS 6500 Series FI
	UCS-IOM -2204 UCS-IOM -2208	UCS-IOM -2204 UCS-IOM -2208	UCS-IOM-2304 UCS-IOM-2304V2	2232 PP 2348	UCS-IOM-2204 UCS-IOM -2208 UCS-IOM -2408*	93180YC -FX3 (25G server ports) 2232 PP 2348 UPQ	UCS-IOM -2204 UCS-IOM -2208 UCS-IOM -2408*	UCS-IOM -2304 V1/V2 UCS-IOM -2408	93180YC -FX3 (25G server ports) 2348 UPQ (10G server ports) 2232 PP	UCS-IOM -2204 UCS-IOM -2208 UCS-IOM -2408* UCS-IOM- 2304 UCS-IOM-2304V2
					* UCS-IOM-2408 supported on M4 and M5 only with UCS 6400 Series FI Cisco UCS IOMs are applicable only for Cisco UCS B-Series Servers					
UCSC-PCIE -QD32GF (Qlogic QLE2742) N2XX-AQPCI05 (Qlogic QLE2562) UCSC-PCIE -Q2672 (Qlogic QLE2672-CSC) UCSC-PCIE -BD32GF (Emulex LPe32002) UCSC-PCIE -BS32GF (Emulex LPe32000) N2XX-AEPCI05 (Emulex LPe12002)	3.1(3a)	3.1(3a)	3.1(3a)	-	4.0(1a)	-	4.1(1a)	-	-	4.2(3s)
UCSC-PCIE -E16002 (Emulex LPe16002-M6 16G FC rack HBA)	3.1(3a)	3.2(1d)	3.2(1d)	-	4.0(1a)	-	4.1(1a)	-	-	4.2(3s)
UCSC-PCIE -ID10GC (Intel X550 Dual-port 10GBase-T NIC)	3.1(2b)	3.1(3a)	3.1(3a)	-	4.0(1a)	-	4.1(1a)	-	-	4.2(3s)

Adapters	Minimum Software Version UCS 6200 Series FI	Minimum Software Version UCS 6332, 6332-16UP	Minimum Software Version UCS 6332, 6332-16UP	Minimum Software Version UCS 6332, 6332 -16UP	Minimum Software Version UCS 6454	Minimum Software Version UCS 6454	Minimum Software Version UCS 64108	Minimum Software Version UCS 6536	Minimum Software Version UCS 6536	Suggested Software Version UCS 6200 Series FI UCS 6332, 6332-16UP FI UCS 6400 Series FI UCS 6500 Series FI
	UCS-IOM -2204 UCS-IOM -2208	UCS-IOM -2204 UCS-IOM -2208	UCS-IOM-2304 UCS-IOM-2304V2	2232 PP 2348	UCS-IOM-2204 UCS-IOM -2208 UCS-IOM -2408*	93180YC -FX3 (25G server ports) 2232 PP 2348 UPQ	UCS-IOM -2204 UCS-IOM -2208 UCS-IOM -2408*	UCS-IOM -2304 V1/V2 UCS-IOM -2408	93180YC -FX3 (25G server ports) 2348 UPQ (10G server ports) 2232 PP	UCS-IOM -2204 UCS-IOM -2208 UCS-IOM -2408* UCS-IOM- 2304 UCS-IOM-2304V2
					* UCS-IOM-2408 supported on M4 and M5 only with UCS 6400 Series FI Cisco UCS IOMs are applicable only for Cisco UCS B-Series Servers					
UCSC-O -ID25GF (Intel XXV710 - DA2 - OCP1 2x25/10GbE OCP 2.0 adapter)	3.1(3a)	4.1(1a)	4.1(1a)	-	4.1(1a)	-	4.1(1a)	-	-	4.2(3s)
UCSC-OCP -QD10GC (QLogic FastLinQ QL41132H Dual Port 10GbE Adapter)	4.0(1a)	4.0(1a)	4.0(1a)	-	4.0(1a)	-	4.0(1a)	-	-	4.2(3s)
UCSC-PCIE -QD25GF (QLogic FastLinQ QL41212H 25GbE adapter)	3.1(3a)	3.1(3a)	3.1(3a)	-	4.0(1a)	-	4.0(1a)	-	-	4.2(3s)
UCSC-OCP -QD25GF (QLogic FastLinQ QL41232H Dual Port 25GbE Adapter)	4.0(1a)	4.0(1a)	4.0(1a)	-	4.0(1a)	-	4.0(1a)	-	-	4.2(3s)
UCSC-PCIE -QD40GF (à QLogic FastLinQ QL45412H 40GbE adapter)	3.1(3a)	3.1(3a)	3.1(3a)	-	4.0(1a)	-	4.0(1a)	-	-	4.2(3s)
UCSC-PCIE -QD10GC (Qlogic QL41162HLRJ-11-SP dual-port 10GBase-T CAN)	4.0(2a)	4.0(2a)	4.0(2a)	-	4.0(2a)	-	4.0(2a)	-	-	4.2(3s)

Adapters	Minimum Software Version UCS 6200 Series FI	Minimum Software Version UCS 6332, 6332-16UP	Minimum Software Version UCS 6332, 6332-16UP	Minimum Software Version UCS 6332, 6332 -16UP	Minimum Software Version UCS 6454	Minimum Software Version UCS 6454	Minimum Software Version UCS 64108	Minimum Software Version UCS 6536	Minimum Software Version UCS 6536	Suggested Software Version UCS 6200 Series FI UCS 6332, 6332-16UP FI UCS 6400 Series FI UCS 6500 Series FI
	UCS-IOM -2204 UCS-IOM -2208	UCS-IOM -2204 UCS-IOM -2208	UCS-IOM-2304 UCS-IOM-2304V2	2232 PP 2348	UCS-IOM-2204 UCS-IOM -2208 UCS-IOM -2408*	93180YC -FX3 (25G server ports) 2232 PP 2348 UPQ	UCS-IOM -2204 UCS-IOM -2208 UCS-IOM -2408*	UCS-IOM -2304 V1/V2 UCS-IOM -2408	93180YC -FX3 (25G server ports) 2348 UPQ (10G server ports) 2232 PP	UCS-IOM -2204 UCS-IOM -2208 UCS-IOM -2408* UCS-IOM- 2304 UCS-IOM-2304V2
					* UCS-IOM-2408 supported on M4 and M5 only with UCS 6400 Series FI Cisco UCS IOMs are applicable only for Cisco UCS B-Series Servers					
UCSC-P -Q6D32GF (Cisco-QLogic QLE2772 2x32GFC Gen 6 Enhanced PCIe HBA)	4.2(1l)	4.2(1l)	4.2(1l)	-	4.2(1l)	-	4.2(1l)	-	-	4.2(3s)
UCSC-P -M6CD100GF (Mellanox MCX623106AC-CDAT 2x100GbE QSFP56 PCIe NIC)	4.2(1l)	4.2(1l)	4.2(1l)	-	4.2(1l)	-	4.2(1l)	-	-	4.2(3s)
UCSC-P -M6DD100GF (Mellanox MCX623106AS-CDAT 2x100GbE QSFP56 PCIe NIC)	4.2(1l)	4.2(1l)	4.2(1l)	-	4.2(1l)	-	4.2(1l)	-	-	4.2(3s)
UCSC-P -B7D32GF (Cisco-Emulex LPe35002-M2-2x32GFC Gen 7 PCIe HBA)	4.2(1l)	4.2(1l)	4.2(1l)	-	4.2(1l)	-	4.2(1l)	-	-	4.2(3s)
UCSC-P -I8D100GF(Cisco - Intel E810CQDA2 2x100 GbE QSFP28 PCIe NIC)	4.2(1l)	4.2(1l)	4.2(1l)	-	4.2(1l)	-	4.2(1l)	-	-	4.2(3s)
UCSC-P -I8Q25GF (Cisco - Intel E810XXVDA4 4x25/10 GbE SFP28 PCIe NIC)	4.2(1l)	4.2(1l)	4.2(1l)	-	4.2(1l)	-	4.2(1l)	-	-	4.2(3s)

Adapters	Minimum Software Version UCS 6200 Series FI	Minimum Software Version UCS 6332, 6332-16UP	Minimum Software Version UCS 6332, 6332-16UP	Minimum Software Version UCS 6332, 6332 -16UP	Minimum Software Version UCS 6454	Minimum Software Version UCS 6454	Minimum Software Version UCS 64108	Minimum Software Version UCS 6536	Minimum Software Version UCS 6536	Suggested Software Version UCS 6200 Series FI UCS 6332, 6332-16UP FI UCS 6400 Series FI UCS 6500 Series FI
	UCS-IOM -2204 UCS-IOM -2208	UCS-IOM -2204 UCS-IOM -2208	UCS-IOM-2304 UCS-IOM-2304V2	2232 PP 2348	UCS-IOM-2204 UCS-IOM -2208 UCS-IOM -2408*	93180YC -FX3 (25G server ports) 2232 PP 2348 UPQ	UCS-IOM -2204 UCS-IOM -2208 UCS-IOM -2408*	UCS-IOM -2304 V1/V2 UCS-IOM -2408	93180YC -FX3 (25G server ports) 2348 UPQ (10G server ports) 2232 PP	UCS-IOM -2204 UCS-IOM -2208 UCS-IOM -2408* UCS-IOM- 2304 UCS-IOM-2304V2
					* UCS-IOM-2408 supported on M4 and M5 only with UCS 6400 Series FI Cisco UCS IOMs are applicable only for Cisco UCS B-Series Servers					
UCSC-P -I8D25GF (Cisco - Intel E810XXVDA2 2x25/10 GbE SFP PCIe NIC)	4.2(1l)	4.2(1l)	4.2(1l)	-	4.2(1l)	-	4.2(1l)	-	-	4.2(3s)
UCSC-P -ID10GC (Cisco - Intel X710T2LG 2x10 GbE RJ45 PCIe NIC)	4.2(1l)	4.2(1l)	4.2(1l)	-	4.2(1l)	-	4.2(1l)	-	-	4.2(3s)
UCSC-O-N6CD100GF (Cisco-NVDA MCX623436AC-CDAB CX6Dx 2x100G QSFP56 x16 OCP NIC)	4.2(3e)	4.2(3e)	4.2(3e)	-	4.2(3e)	-	4.2(3e)	-	-	4.2(3s)
UCSC-O-N6CD25GF (Cisco-NVDA MCX631432AC-ADAB CX6 Lx 2x25G SFP28 x8 OCP NIC)	4.2(3e)	4.2(3e)	4.2(3e)	-	4.2(3e)	-	4.2(3e)	-	-	4.2(3s)

Cisco UCS Fabric Interconnect Server Compatibility Matrix - Release 4.2(3)

Cisco UCS 6536 FI

Cisco VIC	FEX/IOM				
	Direct Attach (40/100G)	Direct Attach (4x25G or 25G QSA28)	93180YC-FX3 (25G server ports)	2348 UPQ (10G server ports)	2304V1/V2 (40G) 2408 (40G)
15428 (UCSC-M-V5Q50G)	Not Supported	C225 M6, C245 M6, C220 M6, C240 M6	C225 M6, C245 M6, C220 M6, C240 M6	C225 M6, C245 M6, C220 M6, C240 M6	-
15238 (UCSC-M-V5D200G)	C225 M6, C245 M6, C220 M6, C240 M6	Not Supported	Not Supported	Not Supported	-
15411 (UCSB-ML-V5Q10G)	-	-	-	-	B200 M6
15411 + Port Expander (UCSB-ML-V5Q10G + UCSB-MLOM-PT-01)	-	-	-	-	B200 M6
1440 (UCSB-MLOM-40G-04)	-	-	-	-	B200 M6, B200 M5, B480 M5
1440 + Port Expander (UCSB-MLOM-40G-04 + UCSB-MLOM-PT-01)	-	-	-	-	B200 M6, B200 M5, B480 M5
1440 + 1480 (UCSB-MLOM-40G-04 + UCSB-VIC-M84-4P)	-	-	-	-	B200 M6, B200 M5, B480 M5
1440 + 1480 + Port Expander (UCSB-MLOM-40G-04 + UCSB-VIC-M84-4P) + UCSB-MLOM-PT-01	-	-	-	-	B480 M5
1440 + 1480 + 1480 (UCSB-MLOM-40G-04 + UCSB-VIC-M84-4P +UCSB-VIC-M84-4P)	-	-	-	-	B480 M5

Cisco VIC	FEX/IOM				
	Direct Attach (40/100G)	Direct Attach (4x25G or 25G QSA28)	93180YC-FX3 (25G server ports)	2348 UPQ (10G server ports)	2304V1/V2 (40G) 2408 (40G)
1455-10G/25G (UCSC-PCIEC25Q-04)	Not Supported	C225 M6, C245 M6, C220 M5, C240 M5, C480 M5, C480 ML M5, C125 M5, S3260 M5	C225 M6, C245 M6, C220 M5, C240 M5, C480 M5, C480 ML M5, C125 M5, S3260 M5	C225 M6, C245 M6, C220 M5, C240 M5, C480 M5, C480 ML M5, C125 M5, S3260 M5	-
1457-10G/25G (UCSC-MLOMC25Q-04)	Not Supported	C220 M5, C240 M5	C220 M5, C240 M5	C220 M5, C240 M5	-
1467-10G/25G (UCSC-MV25-04)	Not Supported	C225 M6, C245 M6, C220 M6, C240 M6	C225 M6, C245 M6, C220 M6, C240 M6	C225 M6, C245 M6, C220 M6, C240 M6	-
1495-40G/100G (UCSC-PCIEC100-04)	C220 M5, C240 M5, C480 M5, C480 ML M5, C125 M5, S3260 M5	Not Supported	Not Supported	Not Supported	-
1497-40G/100G (UCSC-MLOMC100-04)	C220 M5, C240 M5, C480 M5, C480 ML M5, C125 M5	Not Supported	Not Supported	Not Supported	-
1477-40G/100G (UCSC-MV100-04)	C225 M6, C245 M6, C220 M6, C240 M6	Not Supported	Not Supported	Not Supported	-
1340 - 10G/40G (UCSB-MLOM-40G-03)	-	-	-	-	B200 M4, B200 M5, B420 M4, B260 M4/B460 M4, B480 M5
1340 + 1380 (UCSB-MLOM-40G-03 + UCSB-VIC-M83-8P)	-	-	-	-	B200 M4, B200 M5, B420 M4, B260 M4/B460 M4, B480 M5
1340 + Port Expander - 10G/40G (UCSB-MLOM-40G-03 + UCSB-MLOM-PT-01)	-	-	-	-	B200 M4, B200 M5, B420 M4, B260 M4/B460 M4, B480 M5
1340 + 1380 + Port Expander	-	-	-	-	B260 M4/B460 M4, B420 M4, B480 M5
1340 + 1380 + 1380	-	-	-	-	B260 M4/B460 M4, B420 M4, B480 M5

Cisco VIC	FEX/IOM				
	Direct Attach (40/100G)	Direct Attach (4x25G or 25G QSA28)	93180YC-FX3 (25G server ports)	2348 UPQ (10G server ports)	2304V1/V2 (40G) 2408 (40G)
1387 - 40G (UCSC-MLOM-C40Q-03)	C220 M5, C240 M5, C480 M5, C480 ML M5, C125 M5, C220 M4, C240 M4, C460 M4	Not Supported	Not Supported	C220 M5, C240 M5, C480 M5, C480 ML M5, C125 M5, C220 M4, C240 M4, C460 M4 (QSA at the adapter)	-
1385 - 40G (UCSC-PCIE-C40Q-03)	C220 M5, C240 M5, C480 M5, C480 ML M5, C125 M5, C220 M4, C240 M4, C460 M4, S3260 M4 and S3260 M5	Not Supported	Not Supported	C220 M5, C240 M5, C480 M5, C480 ML M5, C125 M5, C220 M4, C240 M4, C460 M4	-

Cisco UCS 6400 and 64108 FIs

Cisco VIC	FEX/IOM							
	Direct Attach	Direct Attach (10G/25G)	Direct Attach (4x10G/4x25)	Direct Attach (40G/100G)	Direct Attach (Break-out)	2232 PP	93180YC-FX3 (25G server ports)	2204/2208/2408
15428 (UCSC-M -V5Q50G)	-	C225 M6, C245 M6, C220 M6, C240 M6	C225 M6, C245 M6, C220 M6, C240 M6	Not Supported	-	Not Supported	C225 M6, C245 M6, C220 M6, C240 M6	-
15238 (UCSC-M -V5D200G)	-	Not Supported	Not Supported	Not Supported	-	Not Supported	Not Supported	-
15411 (UCSB-ML -V5Q10G)	-	-	-	-	-	-	-	B200 M6
15411 + Port Expander (UCSB-ML -V5Q10G + UCSB-MLOM -PT-01)	-	-	-	-	-	-	-	B200 M6

Cisco VIC	FEX/IOM							
	Direct Attach	Direct Attach (10G/25G)	Direct Attach (4x10G/4x25)	Direct Attach (40G/100G)	Direct Attach (Break-out)	2232 PP	93180YC-FX3 (25G server ports)	2204/2208/2408
1440 (UCSB-MLOM-40G-04)	-	-	-	-	-	-	-	B200 M6, B200 M5, B480 M5
1440 + Port Expander (UCSB-MLOM-40G-04 + UCSB-MLOM-PT-01)	-	-	-	-	-	-	-	B200 M6, B200 M5, B480 M5
1440 + 1480 (UCSB-MLOM-40G-04 + UCSB-VIC-M84-4P)	-	-	-	-	-	-	-	B200 M6, B200 M5, B480 M5
1440 + 1480 + Port Expander (UCSB-MLOM-40G-04 + UCSB-VIC-M84-4P) + UCSB-MLOM-PT-01	-	-	-	-	-	-	-	B480 M5
1440 + 1480 + 1480 (UCSB-MLOM-40G-04 + UCSB-VIC-M84-4P +UCSB-VIC-M84-4P)	-	-	-	-	-	-	-	B480 M5

Cisco VIC	FEX/IOM							
	Direct Attach	Direct Attach (10G/25G)	Direct Attach (4x10G/4x25)	Direct Attach (40G/100G)	Direct Attach (Break-out)	2232 PP	93180YC-FX3 (25G server ports)	2204/2208/2408
1455-10G/25G (UCSC-PCIEC 25Q-04)	-	C220 M6, C240 M6, C225 M6, C245 M6, C220 M5, C240 M5, C480 M5, C480 ML M5, C125 M5, S3260 M5	C220 M6, C240 M6, C225 M6, C245 M6, C220 M5, C240 M5, C480 M5, C480 ML M5, C125 M5, S3260 M5	Not Supported	-	C220 M6, C240 M6, C225 M6, C245 M6, C220 M5, C240 M5, C480 M5, C480 ML M5, C125 M5, S3260 M5	C220 M6, C240 M6, C225 M6, C245 M6, C220 M5, C240 M5, C480 M5, C480 ML M5, C125 M5, S3260 M5	-
1457-10G/25G (UCSC-MLOM C25Q-04)	-	C220 M5, C240 M5	C220 M5, C240 M5	Not Supported	-	C220 M5, C240 M5	C220 M5, C240 M5	-
1467-10G/25G (UCSC -MV25-04)	-	C225 M6, C245 M6, C220 M6, C240 M6	C225 M6, C245 M6, C220 M6, C240 M6	Not Supported	-	C225 M6, C245 M6, C220 M6, C240 M6	C225 M6, C245 M6, C220 M6, C240 M6	-
1495-40G/100G (UCSC -PCIEC100 -04)	-	Not Supported	Not Supported	Not Supported	-	Not Supported	Not Supported	-
1497-40G/100G (UCSC -MLOMC100 -04)	-	Not Supported	Not Supported	Not Supported	-	Not Supported	Not Supported	-
1477-40G/100G (UCSC-MV100 -04)	-	Not Supported	Not Supported	Not Supported	-	Not Supported	Not Supported	-

Cisco VIC	FEX/IOM							
	Direct Attach	Direct Attach (10G/25G)	Direct Attach (4x10G/4x25)	Direct Attach (40G/100G)	Direct Attach (Break-out)	2232 PP	93180YC-FX3 (25G server ports)	2204/2208/2408
1340 - 10G/40G (UCSB-MLOM -40G-03)	-	-	-	-	-	-	-	B200 M4, B200 M5, B420 M4, B260 M4/B460 M4, B480 M5
1340 + 1380 (UCSB-MLOM -40G-03 + UCSB-VIC -M83-8P)	-	-	-	-	-	-	-	B200 M4, B200 M5, B420 M4, B260 M4/B460 M4, B480 M5
1340 + Port Expander - 10G/40G (UCSB-MLOM -40G-03 + UCSB-MLOM -PT-01)	-	-	-	-	-	-	-	B200 M4, B200 M5, B420 M4, B260 M4/B460 M4, B480 M5
1340 + 1380 + Port Expander	-	-	-	-	-	-	-	B260 M4/B460 M4, B420 M4, B480 M5
1340 + 1380 + 1380	-	-	-	-	-	-	-	B260 M4/B460 M4, B420 M4, B480 M5

Cisco VIC	FEX/IOM							
	Direct Attach	Direct Attach (10G/25G)	Direct Attach (4x10G/4x25)	Direct Attach (40G/100G)	Direct Attach (Break-out)	2232 PP	93180YC-FX3 (25G server ports)	2204/2208/2408
1387 - 40G (UCSC-MLOM-C40Q-03)	-	C220 M5, C240 M5, C480 M5, C480 ML M5, C125 M5, C220 M4, C240 M4, C460 M4 (QSA at the adapter)	Not Supported	Not Supported	-	C220 M5, C240 M5, C480 M5, C480 ML M5, C125 M5, C220 M4, C240 M4, C460 M4 (QSA at the adapter)	Not Supported	-
1385 - 40G (UCSC-PCIE-C40Q-03)	-	C220 M5, C240 M5, C480 M5, C480 ML M5, C125 M5, C220 M4, C240 M4, C460 M4, S3260 M4 and S3260 M5 (QSA at the adapter)	Not Supported	Not Supported	-	C220 M5, C240 M5, C480 M5, C480 ML M5, C125 M5, C220 M4, C240 M4, C460 M4, S3260 M4 and S3260 M5 (QSA at the adapter)	Not Supported	-

Cisco UCS 6300 FI

Cisco VIC	FEX/IOM				
	Direct Attach	Direct Attach (Break-out)	2232 PP	2348	2304v1/v2 2204/2208
15428 (UCSC-M-V5Q50G)	C225 M6, C245 M6, C220 M6, C240 M6 (10G and 25G)	C225 M6, C245 M6, C220 M6, C240 M6	Not Supported	C225 M6, C245 M6, C220 M6, C240 M6	-
15238 (UCSC-M-V5D200G)	C225 M6, C245 M6, C220 M6, C240 M6 (40G)	Not Supported	Not Supported	Not Supported	-
15411 (UCSB-ML-V5Q10G)	-	-	-	-	B200 M6

Cisco VIC	FEX/IOM				
	Direct Attach	Direct Attach (Break-out)	2232 PP	2348	2304v1/v2 2204/2208
15411 + Port Expander (UCSB-ML-V5Q10G + UCSB-MLOM-PT-01)	-	-	-	-	B200 M6
1440 (UCSB-MLOM-40G-04)	-	-	-	-	B200 M5, B480 M5, B200 M6
1440 + Port Expander (UCSB-MLOM-40G-04 + UCSB-MLOM-PT-01)	-	-	-	-	B200 M5, B480 M5, B200 M6
1440 + 1480 (UCSB-MLOM-40G-04 + UCSB-VIC-M84-4P)	-	-	-	-	B200 M5, B480 M5, B200 M6
1440 + 1480 + Port Expander (UCSB-MLOM-40G-04 + UCSB-VIC-M84-4P) + UCSB-MLOM-PT-01	-	-	-	-	B480 M5
1440 + 1480 + 1480 (UCSB-MLOM-40G-04 + UCSB-VIC-M84-4P +UCSB-VIC-M84-4P)	-	-	-	-	B480 M5
1455-10G/25G (UCSC-PCIEC25Q-04)	C220 M6, C240 M6, C225 M6, C245 M6, C220 M5, C240 M5, C480 M5, C480 ML M5, C125 M5, S3260 M5 (10G speed with 6332-16UP)	C220 M6, C240 M6, C225 M6, C245 M6, C220 M5, C240 M5, C480 M5, C480 ML M5, C125 M5, S3260 M5	C220 M6, C240 M6, C225 M6, C245 M6, C220 M5, C240 M5, C480 M5, C480 ML M5, C125 M5, S3260 M5	C220 M6, C240 M6, C225 M6, C245 M6, C220 M5, C240 M5, C480 M5, C480 ML M5, C125 M5, S3260 M5	-
1457-10G/25G (UCSC-MLOMC25Q-04)	C220 M5, C240 M5 (10G speed with 6332-16UP)	C220 M5, C240 M5	C220 M5, C240 M5	C220 M5, C240 M5	-

Cisco VIC	FEX/IOM				
	Direct Attach	Direct Attach (Break-out)	2232 PP	2348	2304v1/v2 2204/2208
1467-10G/25G (UCSC-MV25-04)	C220 M6, C240 M6,C225 M6, C245 M6 (10G speed with 6332-16UP)	C225 M6, C245 M6, C220 M6, C240 M6	C225 M6, C245 M6, C220 M6, C240 M6	C225 M6, C245 M6, C220 M6, C240 M6	-
1495-40G/100G (UCSC-PCIEC100-04)	C220 M6, C240 M6, C225 M6, C245 M6, C220 M5, C240 M5, C480 M5, C480 ML M5, C125 M5, S3260 M5 (10G speed with 6332-16UP)	Not Supported	Not Supported	Not Supported	-
1497-40G/100G (UCSC-MLOMC100-04)	C220 M5, C240 M5	Not Supported	Not Supported	Not Supported	-
1477-40G/100G (UCSC-MV100-04)	C225 M6, C245 M6, C220 M6, C240 M6	Not Supported	Not Supported	Not Supported	-
1340 - 10G/40G (UCSB-MLOM-40G-03)	-	-	-	-	B200 M4, B200 M5, B420 M4, B260 M4/B460 M4, B480 M5
1340 + 1380 (UCSB-MLOM-40G-03 + UCSB-VIC-M83-8P)	-	-	-	-	B200 M4, B200 M5, B420 M4, B260 M4/B460 M4, B480 M5
1340 + Port Expander - 10G/40G (UCSB-MLOM-40G-03 + UCSB-MLOM-PT-01)	-	-	-	-	B200 M4, B200 M5, B420 M4, B260 M4/B460 M4, B480 M5
1340 + 1380 + Port Expander	-	-	-	-	B260 M4/B460 M4, B420 M4, B480 M5
1340 + 1380 + 1380	-	-	-	-	B260 M4/B460 M4, B420 M4, B480 M5
1387 - 40G (UCSC-MLOM-C40Q-03)	C220 M5, C240 M5, C480 M5, C480 ML M5, C125 M5, C220 M4, C240 M4, C460 M4	Not Supported	C220 M5, C240 M5, C480 M5, C480 ML M5, C125 M5, C220 M4, C240 M4, C460 M4 (QSA at adapter)	C220 M5, C240 M5, C480 M5, C480 ML M5, C125 M5, C220 M4, C240 M4, C460 M4 (QSA at adapter)	-

Cisco VIC	FEX/IOM				
	Direct Attach	Direct Attach (Break-out)	2232 PP	2348	2304v1/v2 2204/2208
1385 - 40G (UCSC-PCIE-C40Q-03)	C220 M5, C240 M5, C480 M5, C480 ML M5, C125 M5, C220 M4, C240 M4, C460 M4, S3260 M4 and S3260 M5	Not Supported	C220 M5, C240 M5, C480 M5, C480 ML M5, C125 M5, C220 M4, C240 M4, C460 M4, S3260 M4 and S3260 M5	C220 M5, C240 M5, C480 M5, C480 ML M5, C125 M5, C220 M4, C240 M4, C460 M4, S3260 M4 and S3260 M5	-

Cisco UCS 6324 FI

Cisco VIC	FEX/IOM			6324 (Primary Chassis)
	Direct Attach (10G)	Direct Attach (Break-out)	2204/2208 (Secondary Chassis)	
15428 (UCSC-M-V5Q50G)	Not Supported	Not Supported	-	-
15238 (UCSC-M-V5D200G)	Not Supported	Not Supported	-	-
15411 (UCSB-ML-V5Q10G)	-	-	Not Supported	Not Supported
15411 + Port Expander (UCSB-ML-V5Q10G + UCSB-MLOM-PT-01)	-	-	Not Supported	Not Supported
1440 (UCSB-MLOM-40G-04)	-	-	Not Supported	B200 M5, B480 M5, B200 M6
1440 + Port Expander (UCSB-MLOM-40G-04 + UCSB-MLOM-PT-01)	-	-	Not Supported	B200 M5, B480 M5, B200 M6
1440 + 1480 (UCSB-MLOM-40G-04 + UCSB-VIC-M84-4P)	-	-	Not Supported	B200 M5, B480 M5, B200 M6
1440 + 1480 + Port Expander (UCSB-MLOM-40G-04 + UCSB-VIC-M84-4P) + UCSB-MLOM-PT-01	-	-	Not Supported	B480 M5

Cisco VIC	FEX/IOM			6324 (Primary Chassis)
	Direct Attach (10G)	Direct Attach (Break-out)	2204/2208 (Secondary Chassis)	
1440 + 1480 + 1480 (UCSB-MLOM-40G-04 + UCSB-VIC-M84-4P +UCSB-VIC-M84-4P)	-	-	Not Supported	B480 M5
1455-10G/25G (UCSC-PCIEC25Q-04)	C220 M5, C240 M5, C480 M5, C480 ML M5, C125 M5, S3260 M5	C220 M5, C240 M5, C480 M5, C480 ML M5, C125 M5, S3260 M5	-	-
1457-10G/25G (UCSC-MLOMC25Q-04)	C220 M5, C240 M5	C220 M5, C240 M5	-	-
1467-10G/25G (UCSC-MV25-04)	Not Supported	Not Supported	-	-
1495-40G/100G (UCSC-PCIEC100-04)	Not Supported	Not Supported	-	-
1497-40G/100G (UCSC-MLOMC100-04)	Not Supported	Not Supported	-	-
1477-40G/100G (UCSC-MV100-04)	Not Supported	Not Supported	-	-
1340 - 10G/40G (UCSB-MLOM-40G-03)	-	-	B200 M4, B200 M5, B420 M4, B260 M4/B460 M4, B480 M5	B200 M4, B200 M5, B420 M4, B260 M4/B460 M4, B480 M5
1340 + 1380 (UCSB-MLOM-40G-03 + UCSB-VIC-M83-8P)	-	-	B200 M4, B200 M5, B420 M4, B260 M4/B460 M4, B480 M5	B200 M4, B200 M5, B420 M4, B260 M4/B460 M4, B480 M5
1340 + Port Expander - 10G/40G (UCSB-MLOM-40G-03 + UCSB-MLOM-PT-01)	-	-	B200 M4, B200 M5, B420 M4, B260 M4/B460 M4, B480 M5	B200 M4, B200 M5, B420 M4, B260 M4/B460 M4, B480 M5
1340 + 1380 + Port Expander	-	-	B260 M4/B460 M4, B420 M4, B480 M5	B260 M4/B460 M4, B420 M4, B480 M5
1340 + 1380 + 1380	-	-	B260 M4/B460 M4, B420 M4, B480 M5	B260 M4/B460 M4, B420 M4, B480 M5
1387 - 40G (UCSC-MLOM-C40Q-03)	C220 M5, C240 M5, C480 M5, C480 ML M5, C125 M5, C220 M4, C240 M4, C460 M4 (QSA at the adapter)	Not Supported	-	-

Cisco VIC	FEX/IOM			6324 (Primary Chassis)
	Direct Attach (10G)	Direct Attach (Break-out)	2204/2208 (Secondary Chassis)	
1385 - 40G (UCSC-PCIE-C40Q-03)	C220 M5, C240 M5, C480 M5, C480 ML M5, C125 M5, C220 M4, C240 M4, C460 M4 (QSA at the adapter)	Not Supported	-	-

Cisco UCS 6200 FI

Cisco VIC	FEX/IOM		
	Direct Attach	2232 PP	2304v1/v2 2204/2208
15428 (UCSC-M-V5Q50G)	Not Supported	Not Supported	-
15238 (UCSC-M-V5D200G)	Not Supported	Not Supported	-
15411 (UCSB-ML-V5Q10G)	-	-	Not Supported
15411 + Port Expander (UCSB-ML-V5Q10G + UCSB-MLOM-PT-01)	-	-	Not Supported
1440 (UCSB-MLOM-40G-04)	-	-	B200 M5, B480 M5
1440 + Port Expander (UCSB-MLOM-40G-04 + UCSB-MLOM-PT-01)	-	-	B200 M5, B480 M5
1440 + 1480 (UCSB-MLOM-40G-04 + UCSB-VIC-M84-4P)	-	-	B200 M5, B480 M5
1440 + 1480 + Port Expander (UCSB-MLOM-40G-04 + UCSB-VIC-M84-4P) + UCSB-MLOM-PT-01	-	-	B480 M5
1440 + 1480 + 1480 (UCSB-MLOM-40G-04 + UCSB-VIC-M84-4P +UCSB-VIC-M84-4P)	-	-	B480 M5
1455-10G/25G (UCSC-PCIEC25Q-04)	C220 M5, C240 M5, C480 M5, C480 ML M5, C125 M5, S3260 M4 and S3260 M5	C220 M5, C240 M5, C480 M5, C480 ML M5, C125 M5, S3260 M5	-

Cisco VIC	FEX/IOM		
	Direct Attach	2232 PP	2304v1/v2 2204/2208
1457-10G/25G (UCSC-MLOMC25Q-04)	C220 M5, C240 M5	C220 M5, C240 M5	-
1467-10G/25G (UCSC-MV25-04)	Not Supported	Not Supported	-
1495-40G/100G (UCSC-PCIEC100-04)	Not Supported	Not Supported	-
1497-40G/100G (UCSC-MLOMC100-04)	Not Supported	Not Supported	-
1477-40G/100G (UCSC-MV100-04)	Not Supported	Not Supported	-
1340 - 10G/40G (UCSB-MLOM-40G-03)	-	-	B200 M4, B200 M5, B420 M4, B260 M4/B460 M4, B480 M5
1340 + 1380 (UCSB-MLOM-40G-03 + UCSB-VIC-M83-8P)	-	-	B200 M4, B200 M5, B420 M4, B260 M4/B460 M4, B480 M5
1340 + Port Expander - 10G/40G (UCSB-MLOM-40G-03 + UCSB-MLOM-PT-01)	-	-	B200 M4, B200 M5, B420 M4, B260 M4/B460 M4, B480 M5
1340 + 1380 + Port Expander	-	-	B260 M4/B460 M4, B420 M4, B480 M5
1340 + 1380 + 1380	-	-	B260 M4/B460 M4, B420 M4, B480 M5
1387 - 40G (UCSC-MLOM-C40Q-03)	C220 M5, C240 M5, C480 M5, C480 ML M5, C125 M5, C220 M4, C240 M4, C460 M4	C220 M5, C240 M5, C480 M5, C480 ML M5, C220 M4, C240 M4, C460 M4, S3260 M4 and S3260 M5	-
1385 - 40G (UCSC-PCIE-C40Q-03)	C220 M5, C240 M5, C480 M5, C480 ML M5, C125 M5, C220 M4, C240 M4, C460 M4, S3260 M4 and S3260 M5 (QSA at adapter)	C220 M5, C240 M5, C480 M5, C480 ML M5, C220 M4, C240 M4, C460 M4, S3260 M4 and S3260 M5 (QSA at adapter)	-

Other Hardware

Other Hardware

We recommend that you use the latest software version for all Chassis, Fabric Interconnects, Fabric Extenders, Expansion Modules and Power Supplies. To determine the minimum software version for your mixed environment, see Cross-Version Firmware Support, on page 31. The following is the list of other supported hardware:

Table 18: Supported Hardware for UCS 6500 Series Fabric Interconnects

Type	Details
Chassis	UCSB-5108-AC2 UCSB-5108-DC2
Fabric Interconnects	UCS 6500
Fabric Extenders	93180YC-FX3 (25G server ports) Cisco UCS 2348 UPQ (10G server ports) Cisco UCS 2304 V1/V2 (40G) Cisco UCS 2408 (40G)
Power Supplies	UCS-PSU-6536-AC

Table 19: Supported Hardware for UCS 6400 Series Fabric Interconnects

Type	Details
Chassis	UCSC-C4200-SFF N20–C6508 UCSB-5108-DC UCSB-5108-AC2 UCSB-5108-DC2 UCSB-5108-HVDC
Fabric Interconnects	UCS 64108 UCS 6454
Fabric Extenders	Cisco UCS 2204XP Cisco UCS 2208XP Cisco Nexus 2232PP Cisco Nexus 2232TM-E Cisco UCS 2408 Cisco Nexus C93180YC-FX3

Type	Details
Power Supplies	UCS-PSU-6332-AC UCS-PSU-6332-DC UCS-PSU-64108-AC UCS-PSU-6332-DC

Table 20: Supported Hardware for UCS 6332, UCS 6332-16UP Fabric Interconnects

Type	Details
Chassis	N20–C6508 UCSB-5108-DC UCSB-5108-AC2 UCSB-5108-DC2 UCSB-5108-HVDC
Fabric Interconnects	UCS 6332UP UCS 6332-16UP
Fabric Extenders	Cisco UCS 2208XP Cisco UCS 2204XP Cisco Nexus 2232PP Cisco Nexus 2232TM-E Cisco UCS 2304 Cisco UCS 2304V2 Cisco Nexus 2348UPQ
Power Supplies	UCS-PSU-6332-AC UCS-PSU-6332-DC

Note The 40G backplane setting is not applicable for 22xx IOMs.

Table 21: Supported Hardware for UCS 6200 Fabric Interconnects

Type	Details
Chassis	N20–C6508 UCSB-5108-DC UCSB-5108-AC2 UCSB-5108-DC2 UCSB-5108-HVDC
Fabric Interconnects	UCS 6248UP UCS 6296UP
Fabric Extenders	UCS 2208XP UCS 2204XP Cisco Nexus 2232PP Cisco Nexus 2232TM-E
Expansion Modules	UCS-FI-E16UP
Power Supplies	UCS-PSU-6248UP-AC UCS-PSU-6248UP-DC UCS-PSU-6248-HVDC UCS-PSU-6296UP-AC UCS-PSU-6296UP-DC

GB Connector Modules, Transceiver Modules, and Cables

Following is the list of Gb connector modules, transceiver modules, and supported cables:

Note

- Transceiver modules and cables that are supported on a specific Fabric Interconnect are not always supported on all VIC adapters, IOMs, or FEXes that are compatible with that Fabric Interconnect. Detailed compatibility matrices for the transceiver modules are available here:https://www.cisco.com/c/en/us/support/interfaces-modules/transceiver-modules/products-device-support-tables-list.html
- S-Class transceivers, for example, QSFP-40G-SR4-S, do not support FCoE.

Table 22: Supported Transceiver Modules and Cables for GB Connector Modules

Gb Connector Modules	Transceiver Modules and Cables
FC for UCS 6500 Series Fabric Interconnects	DS-SFP-4X32G-SW

Gb Connector Modules	Transceiver Modules and Cables
1GbE for UCS 6500 Series Fabric Interconnects	GLC-TE (QSA), port 9, 10 GLC-SX-MMD (QSA)
10GbE for UCS 6500 Series Fabric Interconnects	SFP-10G-SR (QSA) SFP-10G-SR-S(QSA) SFP-10G-LR (QSA) SFP-10G-LR-S (QSA) CVR-QSFP-SFP10G SFP-H10GB-CU1M
25GbE for UCS 6500 Series Fabric Interconnects	SFP-10/25G-LR-S SFP-10/25G-CSR-S SFP-25G-SL QSA28 SFP-H25G-CU1M (P1) SFP-H25G-CU2M (P1) SFP-H25GB-CU3M SFP-25G-AOC2M SFP-25G-AOC3M SFP-25G-SR-S

Gb Connector Modules	Transceiver Modules and Cables
40GbE for UCS 6500 Series Fabric Interconnects	QSFP-H40G-AOC1M QSFP-H40G-AOC2M QSFP-H40G-AOC3M QSFP-H40G-AOC5M QSFP-H40G-AOC15M QSFP-H40G-AOC25M QSFP-40G-CU1M QSFP-40G-CU2M QSFP-40G-CU3M QSFP-40G-CU5M QSFP-40G-SR4 QSFP-40G-SR4-S QSFP-40G-CSR4 QSFP-40G-LR4 QSFP-40G-LR4-S QSFP-4SFP10G-CU1M QSFP-4SFP10G-CU3M FET-40G QSFP-40G-ACU10M QSFP-40G-SR-BD

Gb Connector Modules	Transceiver Modules and Cables
100GbE for UCS 6500 Series Fabric Interconnects	QSFP-100G-SR4-S QSFP-100G-LR4-S QSFP-100G-SM-SR QSFP-100G-SL4 QSFP-40/100-SRBD (or) QSFP-100G40G-BIDI **Note** QSFP-100G40G-BIDI is supported only on border ports/uplink ports. QSFP-100G-CU1M QSFP-100G-CU2M QSFP-100G-CU3M QSFP-100G-CU5M QSFP-4SFP25G-CU1M QSFP-4SFP25G-CU2M QSFP-4SFP25G-CU3M QSFP-4SFP25G-CU5M QSFP-100G-AOC1M QSFP-100G-AOC2M QSFP-100G-AOC3M QSFP-100G-AOC5M QSFP-100G-AOC7M QSFP-100G-AOC10M QSFP-100G-AOC15M QSFP-100G-AOC20M QSFP-100G-AOC25M QSFP-100G-AOC30M QSFP-100G-DR-S QSFP-100G-FR-S
FC for UCS 6400 Series Fabric Interconnects	DS-SFP-FC8G-SW DS-SFP-FC8G-LW DS-SFP-FC16G-SW DS-SFP-FC16G-LW DS-SFP-FC32G-SW DS-SFP-FC32G-LW

Gb Connector Modules	Transceiver Modules and Cables
100-Gb for UCS 6400 Series Fabric Interconnects	QSFP-40/100G-SRBD QSFP-100G-SR4-S QSFP-100G-LR4-S QSFP-100G-SM-SR QSFP-100G-CU1M QSFP-100G-CU2M QSFP-100G-CU3M QSFP-100G-AOC1M QSFP-100G-AOC2M QSFP-100G-AOC3M QSFP-100G-AOC5M QSFP-100G-AOC7M QSFP-100G-AOC10M QSFP-100G-AOC15M QSFP-100G-AOC20M QSFP-100G-AOC25M QSFP-100G-AOC30M

Gb Connector Modules	Transceiver Modules and Cables
40-Gb for UCS 6400 Series Fabric Interconnects	QSFP-40G-SR4 QSFP-40G-SR4-S QSFP-40G-SR-BD QSFP-40G-LR4 QSFP-40G-LR4-S QSFP-40G-ER4 WSP-Q40GLR4L QSFP-H40G-CU1M QSFP-H40G-CU3M QSFP-H40G-CU5M QSFP-H40G-ACU7M QSFP-H40G-ACU10M QSFP-H40G-AOC1M QSFP-H40G-AOC2M QSFP-H40G-AOC3M QSFP-H40G-AOC5M QSFP-H40G-AOC10M QSFP-H40G-AOC15M

Gb Connector Modules	Transceiver Modules and Cables
40-Gb for UCS 6300 Series Fabric Interconnects	QSFP-40G-SR4 in 4x10G mode with external 4x10G splitter cable to SFP-10G-SR QSFP-40G-CSR4 QSFP-40G-LR4 QSFP-40G-LR4-S QSFP-40G-SR-BD QSFP-40G-SR4 QSFP-40G-SR4-S FET-40G QSFP-4SFP10G-CU1M QSFP-4SFP10G-CU3M QSFP-4SFP10G-CU5M QSFP-4X10G-AC7M QSFP-4X10G-AC10M QSFP-4X10G-AOC1M QSFP-4X10G-AOC2M QSFP-4X10G-AOC3M QSFP-4X10G-AOC5M QSFP-4X10G-AOC7M QSFP-4X10G-AOC10M QSFP-H40G-ACU7M QSFP-H40G-ACU10M QSFP-H40G-AOC1M QSFP-H40G-AOC2M QSFP-H40G-AOC3M QSFP-H40G-AOC5M QSFP-H40G-AOC7M QSFP-H40G-AOC10M QSFP-H40G-AOC15M QSFP-H40G-CU1M QSFP-H40G-CU3M QSFP-H40G-CU5M

Gb Connector Modules	Transceiver Modules and Cables
32-Gb FC for UCS 6454 Fabric Interconnects	DS-SFP-FC32G-SW DS-SFP-FC32G-LW
25-Gb for UCS 6454 Fabric Interconnects	4x25GbE 10M[1]
25-Gb for UCS 6400 Series Fabric Interconnects	SFP-25G-SR-S SFP-H25G-CU1M SFP-H25G-CU2M SFP-H25G-CU3M SFP-H25G-CU5M SFP-H25G-AOC1M SFP-H25G-AOC2M SFP-H25G-AOC3M SFP-H25G-AOC5M SFP-H25G-AOC7M SFP-H25G-AOC10M
16-Gb for UCS 6454 and UCS 6332UP Fabric Interconnects	DS-SFP-FC16G-LW DS-SFP-FC16G-SW

Gb Connector Modules	Transceiver Modules and Cables
10-Gb for UCS 6400 Series Fabric Interconnects	SFP-10G-SR SFP-10G-SR-S SFP-10G-LR SFP-10G-LR-S SFP-10G-ER SFP-10G-ER-S SFP-10G-ZR SFP-10G-ZR-S FET-10G **Note** FET-10G is only supported between Fabric Interconnects and IOMs/FEXs. SFP-10G-LRM SFP-H10GB-CU1M SFP-H10GB-CU2M SFP-H10GB-CU3M SFP-H10GB-CU5M SFP-H10GB-ACU7M SFP-H10GB-ACU10M SFP-10G-AOC1M SFP-10G-AOC2M SFP-10G-AOC3M SFP-10G-AOC5M SFP-10G-AOC7M SFP-10G-AOC10M

Gb Connector Modules	Transceiver Modules and Cables
10-Gb for UCS 6300 and 6200 Series Fabric Interconnects	SFP-10G-SR SFP-10G-SR-S SFP-10G-LR SFP-10G-LR-S SFP-H10GB-CU1M SFP-H10GB-CU2M SFP-H10GB-CU3M SFP-H10GB-CU5M SFP-H10GB-ACU7M SFP-H10GB-ACU10M FET-10G [2]SFP-10G-AOC1M SFP-10G-AOC2M SFP-10G-AOC3M SFP-10G-AOC5M SFP-10G-AOC7M SFP-10G-AOC10M
8-Gb FC for UCS 6400 Series and UCS 6332UP Fabric Interconnects	DS-SFP-FC8G-SW DS-SFP-FC8G-LW
4-Gb FC for UCS 6300 and 6200 Series Fabric Interconnects	DS-SFP-FC4G-SW DS-SFP-FC4G-LW
1-Gb for UCS 6400 Series Fabric Interconnects	GLC-TE GLC-SX-MMD SFP-GE-T
1-Gb for UCS 6300 and 6200 Series Fabric Interconnects	GLC-TE GLC-SX-MM GLC-LH-SM

[1] Supported from Cisco UCS Manager, Release 4.1(2)
[2] SFP-10G-AOC cables are only supported for Cisco 1455 and 1457 VIC cards.

Note The maximum length of fiber optic runs is limited to 300 meters. This is imposed by our use of 802.3X/802.1Qbb Priority Pauses. SFP-10G-LR is supported between fabric interconnect and FEX, but the 300 m limit still applies.

Cisco UCS Mini and Components

UCS Mini Supported Chassis

Table 23: Minimum Software Versions for UCS Mini Chassis

Chassis	Minimum Software Version	Suggested Software Version
UCSB-5108-AC2	3.0(1e)	4.2(3s)
UCSB-5108-DC2	3.0(2c)	4.2(3s)

UCS Mini Supported Blade and Rack Servers

Table 24: Minimum Host Firmware Versions for Blade and Rack Servers on UCS Mini

Servers	Minimum Software Version	Suggested Software Version
B200 M6	4.2(1d)	4.2(3s)
B200 M5	4.0(1a)	4.2(3s)
B200 M4	4.0(1a)	4.2(3s)
B260 M4	4.0(1a)	4.2(3s)
B420 M4	4.0(1a)	4.2(3s)
B460 M4	4.0(1a)	4.2(3s)
B480 M5	4.0(1a)	4.2(3s)
C220 M4	4.0(1a)	4.2(3s)
C240 M4	4.0(1a)	4.2(3s)
C460 M4	4.0(1a)	4.2(3s)
C220 M5	4.0(1a)	4.2(3s)
C240 M5	4.0(1a)	4.2(3s)
C480 M5	4.0(1a)	4.2(3s)

UCS Mini Supported Adapters

Adapters	Minimum Software Version	Suggested Software Version
UCSC-PCIE-IQ10GC (Intel X710-T4)	3.2(2b)	4.2(2d)
UCSC-PCIE-QD25GF (QLogic QL41212H 25GbE) UCSC-PCIE-QD40GF (QLogic QL45212H 40GbE)	3.2(2b)	4.2(2d)
UCSC-PCIE-C40Q-03 (UCS VIC 1385) UCSC-MLOM-C40Q-03 (UCS VIC 1387)	3.1(3a)	4.2(3s)
UCS-VIC-M82-8P (UCS VIC 1280) UCSB-MLOM-40G-01 (UCS VIC 1240) UCSB-MLOM-PT-01 (Cisco Port Expander Card)	3.1(3a)	4.2(2d)
UCSB-MLOM-40G-03 (UCS VIC 1340) UCSB-VIC-M83-8P (UCS VIC 1380) UCSC-MLOM-CSC-02 (UCS VIC 1227)	3.1(3a)	4.2(3s)
UCSC-PCIE-CSC-02 (UCS VIC 1225)	3.1(3a)	4.2(2d)
UCSB-MLOM-40G-04 (UCS VIC 1440)	4.2(2a)	4.2(2d)
UCSB-VIC-M84-4P (UCS VIC 1480)	4.2(2a)	4.2(2d)
UCSC-PCIE-C25Q-04 (UCS VIC 1455)	4.2(2a)	4.2(3s)
UCSC-MLOM-C25Q-04 (UCS VIC 1457)	4.2(2a)	4.2(3s)

UCS Mini Supported Fabric Interconnects

Fabric Interconnects	Minimum Software Version	Suggested Software Version
Cisco UCS 6324	3.1(3a)	4.2(3s)

UCS Mini Supported Fabric Extenders for Secondary Chassis

Fabric Extenders	Minimum Software Version	Suggested Software Version
UCS 2204 XP	3.1(3a)	4.2(3s)
UCS 2208 XP	3.1(3a)	4.2(3s)

UCS Mini Supported Power Supplies

Power Supplies	Minimum Software Version	Suggested Software Version
UCSB-PSU-2500ACDV UCSB-PSU-2500DC48 UCSC-PSU-930WDC UCSC-PSU2V2-930WDC UCSC-PSUV2-1050DC UCSC-PSU1-770W UCSC-PSU2-1400 UCSC-PSU2V2-1400W UCSC-PSU2V2-650W UCSC-PSU2V2-1200W	3.1(3a)	4.2(3s)

UCS Mini Supported Gb Connector Modules

We recommend that you use the current software version for Gb port speed connections. Following is the list of Gb connector modules and supported cables:

Note Transceiver modules and cables that are supported on a specific Fabric Interconnect are not always supported on all VIC adapters, IOMs, or FEXes that are compatible with that Fabric Interconnect. Detailed compatibility matrices for the transceiver modules are available here:https://www.cisco.com/c/en/us/support/interfaces-modules/transceiver-modules/products-device-support-tables-list.html

Gb Connector Modules	Transceivers Modules and Cables
40-Gb	QSFP-40G-SR4 in 4x10G mode with external 4x10G splitter cable to SFP-10G-SR QSFP-4SFP10G-CU1M QSFP-4SFP10G-CU3M QSFP-4SFP10G-CU5M QSFP-4X10G-AC7M QSFP-4X10G-AC10M QSFP-4X10G-AOC1M QSFP-4X10G-AOC2M QSFP-4X10G-AOC3M QSFP-4X10G-AOC5M QSFP-4X10G-AOC7M QSFP-4X10G-AOC10M
10-Gb	SFP-10G-LR SFP-10G-LR-S SFP-10G-LR-X SFP-10G-SR SFP-10G-SR-S SFP-10G-SR-X SFP-H10GB-CU1M SFP-H10GB-CU2M SFP-H10GB-CU3M SFP-H10GB-CU5M SFP-H10GB-ACU7M SFP-H10GB-ACU10M SFP-10G-AOC1M SFP-10G-AOC2M SFP-10G-AOC3M SFP-10G-AOC5M SFP-10G-AOC7M SFP-10G-AOC10M
8-Gb	DS-SFP-FC8G-SW DS-SFP-FC8G-LW

Gb Connector Modules	Transceivers Modules and Cables
4-Gb	DS-SFP-FC4G-SW DS-SFP-FC4G-LW
1-Gb	GLC-TE GLC-LH-SM GLC-SX-MM

Capability Catalog

The Cisco UCS Manager Capability Catalog is a set of tunable parameters, strings, and rules. Cisco UCS uses the catalog to update the display and configurability of components such as newly qualified DIMMs and disk drives for servers.

The Capability Catalog is embedded in Cisco UCS Manager, but at times it is also released as a single image file to make updates easier.

The following table lists the PIDs added in this release and maps UCS software releases to the corresponding Capability Catalog file.

Table 25: Version Mapping

UCS Release	Catalog File Name	Additional PIDs in this Release
4.2(3s)	ucs-catalog.4.2.3n.T.bin	—
4.2(3r)	ucs-catalog.4.2.3n.T.bin	—
4.2(3p)	ucs-catalog.4.2.3m.T.bin	—
4.2(3o)	ucs-catalog.4.2.3l.T.bin	—
4.2(3n)	ucs-catalog.4.2.3l.T.bin	—
4.2(3m)	ucs-catalog.4.2.3l.T.bin	—
4.2(3l)	ucs-catalog.4.2.3l.T.bin	—
4.2(3k)	ucs-catalog.4.2.3k.T.bin	—
4.2(3j)	ucs-catalog.4.2.3j.T.bin	—
4.2(3i)	ucs-catalog.4.2.3i.T.bin	—
4.2(3h)	ucs-catalog.4.2.3h.T.bin	—
4.2(3g)	ucs-catalog.4.2.3g.T.bin	—
4.2(3e)	ucs-catalog.4.2.3f.T.bin	—
4.2(3b)	ucs-catalog.4.2.3b.T.bin	—
4.2(2e)	ucs-catalog.4.2.2e.T.bin	—

UCS Release	Catalog File Name	Additional PIDs in this Release
4.2(2d)	ucs-catalog.4.2.2d.T.bin	—
4.2(2c)	ucs-catalog.4.2.2c.T.bin	—
4.2(2a)	ucs-catalog.4.2.2a.T.bin	—
4.2(1n)	ucs-catalog.4.2.1n.T.bin	—
4.2(1m)	ucs-catalog.4.2.1l.T.bin	—
4.2(1l)	ucs-catalog.4.2.1j.T.bin	—

UCS Release	Catalog File Name	Additional PIDs in this Release
4.2(1i)	ucs-catalog.4.2.1f.T.bin	

UCS Release	Catalog File Name	Additional PIDs in this Release
		Drives for C3X60 M4 storage server: • UCS-C3K-HD4TB • UCS-C3K-HD4TBRR • UCSC-C3X60-HD6TB • UCSC-C3X60-6TBRR Drives for S3260 M5 storage server: • UCS-S3260-HD8TA • UCS-S3260-HD8TARR Drives for C220 M5, C240 M5, and C240 M6 servers: • UCS-HD4T7KL12N • UCS-HD6T7KL4KN • UCS-HD6T7KL4KM (Mid/M6) • UCS-HD8T7K4KAN • UCS-HD8T7K4KAM (Mid/M6) Drives for C220 M4 and C240 M4 servers: • UCS-HD4T7KL12G • UCS-HD6T7KL4K • UCS-HD8T7K4KAG Drives for C220 M6 and C240 M6 servers: • UCS-HD18TW7KL4KM Drives for C220 M5, C240 M5, C480 M5, C220 M6, and C240 M6 servers: • UCS-SD76TBKNK9 Drives for C220 M5, C240 M5, C480 M5, C220 M6, and C240 M6 servers: • UCS-SD960GS1X-EV • UCS-SD19TS1X-EV • UCS-SD38TS1X-EV Drives for B200 M5 and B480 M5 servers: • UCS-SD960GSB1X-EV

UCS Release	Catalog File Name	Additional PIDs in this Release
		• UCS-SD19TSB1X-EV • UCS-SD38TSB1X-EV

UCS Release	Catalog File Name	Additional PIDs in this Release
4.2(1f)	ucs-catalog.4.2.1f.T.bin	

UCS Release	Catalog File Name	Additional PIDs in this Release
		Drives for C3X60 M4 storage server: • UCS-C3K-HD4TB • UCS-C3K-HD4TBRR • UCSC-C3X60-HD6TB • UCSC-C3X60-6TBRR Drives for S3260 M5 storage server: • UCS-S3260-HD8TA • UCS-S3260-HD8TARR Drives for C220 M5, C240 M5, and C240 M6 servers: • UCS-HD4T7KL12N • UCS-HD6T7KL4KN • UCS-HD6T7KL4KM (Mid/M6) • UCS-HD8T7K4KAN • UCS-HD8T7K4KAM (Mid/M6) Drives for C220 M4 and C240 M4 servers: • UCS-HD4T7KL12G • UCS-HD6T7KL4K • UCS-HD8T7K4KAG Drives for C220 M6 and C240 M6 servers: • UCS-HD18TW7KL4KM Drives for C220 M5, C240 M5, C480 M5, C220 M6, and C240 M6 servers: • UCS-SD76TBKNK9 Drives for C220 M5, C240 M5, C480 M5, C220 M6, and C240 M6 servers: • UCS-SD960GS1X-EV • UCS-SD19TS1X-EV • UCS-SD38TS1X-EV Drives for B200 M5 and B480 M5 servers: • UCS-SD960GSB1X-EV

UCS Release	Catalog File Name	Additional PIDs in this Release
		• UCS-SD19TSB1X-EV • UCS-SD38TSB1X-EV
4.2(1d)	ucs-catalog.4.2.1c.T.bin	Drives for B480 M5, UCS C240 M5, and UCS C220 M6 servers: • UCS-SD960GBKNK9 • UCS-SD38TBKNK9 • UCS-SD800GBKNK9 • UCS-SD16TBKNK9

For detailed list of PIDs and Manufacturing Part Numbers (MPN) released with Cisco UCS Capability Catalog, Release 4.2, refer Release Notes for Cisco UCS Capability Catalog, Release 4.2

Security Fixes

Security Fixes in Release 4.2(3s)

There are no security fixes in release 4.2(3s).

Security Fixes in Release 4.2(3r)

The following security issue is resolved:

CSCwn02394

A vulnerability in the web-based management interface of Cisco FXOS Software and Cisco UCS Manager Software could allow an authenticated, local attacker with administrative privileges to perform command injection attacks on an affected system and elevate privileges to root.

This vulnerability is due to insufficient input validation of command arguments supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system of the affected device with root-level privileges.

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

For more detailed information, see Cisco FXOS and UCS Manager Software Command Injection Vulnerability.

CSCwm68935

A vulnerability in the logging subsystem of the Cisco product could allow an authenticated, local attacker to view sensitive information in a system log file which should be restricted.

The vulnerability is due to a lack of proper masking of sensitive information before being written to system log files. An attacker could exploit this vulnerability by authenticating to the targeted device and inspecting a specific system log file. A successful exploit could allow the attacker to view sensitive data that was not properly masked.

Cisco has released software updates that address this vulnerability. Future versions of the product(s) will include the necessary fixes to ensure sensitive information is correctly masked.

CSCwn23026

A vulnerability in the CLI and web-based management interface of the Cisco UCS Manager Software could allow an authenticated, remote attacker with valid administrative privileges to execute arbitrary commands on the underlying operating system of an affected device.

This vulnerability is due to insufficient input validation of command arguments supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system of an affected device with root-level privileges.

Cisco has released software updates that address this vulnerability. Future versions of the product(s) will not be affected by this vulnerability.

CSCws66235

A vulnerability in the logging subsystem of the Cisco product could allow an authenticated, local attacker to view sensitive information in a system log file which should be restricted.

The vulnerability is due to a lack of proper masking of sensitive information before being written to system log files. An attacker could exploit this vulnerability by authenticating to the targeted device and inspecting a specific system log file. The attacker would need valid user credentials to successfully exploit this issue.

Cisco has released software updates that address this vulnerability. Future versions of the product(s) will include the necessary fixes to ensure sensitive information is correctly masked.

CSCwm68934

The Cisco UCS Manager Software is affected by the vulnerability identified by the following Common Vulnerability and Exposures (CVE) ID:

CVE-2023-20076—A vulnerability in the NX-OS CLI privilege levels of Cisco UCS Manager Software could allow an authenticated, local attacker with read-only privileges to modify files and perform unauthorized actions on an affected system. This vulnerability exists because unnecessary privileges are granted to the user, which could allow an attacker to create or overwrite files in the file system or perform limited privileged actions on an affected device.

The affected software has been upgraded to a version that includes fixes for the vulnerability. Future versions of the product(s) will not be affected by this vulnerability.

For more information, see: Cisco UCS Manager Software Privilege Escalation Vulnerability

CSCwm57437

A vulnerability in the web-based management interface of Cisco FXOS Software and Cisco UCS Manager Software could allow an authenticated, remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the interface.

This vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of an affected system. An attacker could exploit this vulnerability by injecting malicious data into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit this vulnerability, the attacker must have valid Administrator or AAA Administrator credentials.

Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability. For more information, see Cisco FXOS and UCS Manager Software Stored Cross-Site Scripting Vulnerability.

Security Fixes in Release 4.2(3p)

The following security issue is resolved:

CSCwo49706 and CSCwo49702

The Cisco UCS B-Series M5/M6 Blade Servers and UCS C-Series M5/M6 Rack Servers include an Intel CPU that is affected by the vulnerability identified by the following Common Vulnerability and Exposures (CVE) ID:

- CVE-2024-45332—Exposure of sensitive information caused by shared microarchitectural predictor state that influences transient execution in the indirect branch predictors for some Intel® Processors may allow an authenticated user to potentially enable information disclosure via local access.

The affected third-party software component has been upgraded to a version that includes fixes for the vulnerability. Future versions of the product(s) will not be affected by this vulnerability.

CSCwn06798 and CSCwn23023

Cisco NX-OS Software for Cisco Nexus 3000 Series Switches, Cisco Nexus 9000 Series Switches in standalone NX-OS mode, Cisco UCS 6400 Series Fabric Interconnects, Cisco UCS 6500 Series Fabric Interconnects, and Cisco UCS 9108 100G Fabric Interconnects includes Third-party Software that is affected by the vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) IDs:

- CVE-2025-20290 — A vulnerability in the logging feature of Cisco NX-OS Software and Cisco UCS Fabric Interconnects could allow a local, authenticated attacker to access sensitive information.

The affected software component has been upgraded to a version that includes fixes for the vulnerability. Future versions of the product(s) will not be affected by this vulnerability.

For additional information, see the Cisco Security Advisory:

Cisco NX-OS Software Sensitive Log Information Disclosure Vulnerability

CSCwn06825

Cisco UCS Manager Software includes multiple vulnerabilities in its CLI and web-based management interface identified by the following Common Vulnerability and Exposures (CVE) ID:

- CVE-2025-20294 — Multiple command injection vulnerabilities exist due to insufficient input validation of command arguments. An authenticated, remote attacker with administrative privileges could exploit these vulnerabilities by submitting crafted input, allowing execution of arbitrary commands on the underlying operating system with root-level privileges.

Cisco has released software updates that address these vulnerabilities. There are no workarounds available. Future versions of the product will not be affected by these issues.

CSCwm57438

Cisco UCS Manager Software includes a vulnerability in its web-based management interface identified by the following Common Vulnerability and Exposures (CVE) ID:

- CVE-2025-20296 — A stored cross-site scripting (XSS) vulnerability exists due to insufficient validation of user-supplied input. An authenticated, remote attacker with Administrator or AAA Administrator privileges could exploit this vulnerability by injecting malicious script code into the interface, potentially executing arbitrary scripts in the context of other users and accessing sensitive browser-based information.

Cisco has released software updates that address this vulnerability. There are no workarounds available. Future versions of the product will not be affected by this issue.

CSCwm88176

Cisco UCS Manager Software includes a vulnerability in the CLI identified by the following Common Vulnerability and Exposures (CVE) ID:

- CVE-2025-20295 — A vulnerability due to insufficient input validation of command arguments allows an authenticated, local attacker with administrative privileges to read, create, or overwrite any file on the underlying operating system file system, including system files. Exploitation requires valid administrative credentials.

Cisco has released software updates that address this vulnerability. There are no workarounds available. Future versions of the product will not be affected by this issue.

CSCwo04043

Cisco Integrated Management Controller (IMC), including the vKVM client in Cisco UCS Manager, includes a vulnerability identified by the following Common Vulnerability and Exposures (CVE) ID:

- CVE-2025-20317 — A vulnerability in the Virtual Keyboard Video Monitor (vKVM) connection handling due to insufficient verification of vKVM endpoints allows an unauthenticated, remote attacker to redirect a user to a malicious website by persuading the user to click a crafted link. Successful exploitation could lead to credential capture.

Cisco has released software updates that address this vulnerability. There are no workarounds available. Future versions of the product will not be affected by this issue.

CSCwm88173

Cisco NX-OS Software includes a vulnerability in the CLI identified by the following Common Vulnerability and Exposures (CVE) ID:

- CVE-2025-20292 — A command injection vulnerability due to insufficient validation of user-supplied input allows an authenticated, local attacker with valid credentials to execute commands on the underlying operating system with non-root user privileges. Successful exploitation could allow reading and writing files limited to the attacker’s account permissions.

Cisco has released software updates that address this vulnerability. There are no workarounds available. Future versions of the product will not be affected by this issue.

Security Fixes in Release 4.2(3o)

The following security issue is resolved:

CSCwj35846

A vulnerability in the bootloader of Cisco NX-OS Software could allow an unauthenticated attacker with physical access to an affected device, or an authenticated local attacker with administrative credentials, to bypass NX-OS image signature verification.

This vulnerability is due to insecure bootloader settings. An attacker could exploit this vulnerability by executing a series of bootloader commands. A successful exploit could allow the attacker to bypass NX-OS image signature verification and load unverified software.

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

See advisory for more details:

Cisco NX-OS Software Image Verification Bypass Vulnerability

Security Fixes in Release 4.2(3n)

The are no security issues in release 4.2(3n).

Security Fixes in Release 4.2(3m)

The are no security issues in release 4.2(3m).

Security Fixes in Release 4.2(3l)

The following security issues are resolved:

CSCwk62264

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

- CVE-2024-6387—A race condition has been identified in the sshd service related to its signal handler. If a client fails to authenticate within the LoginGraceTime period (default is 120 seconds, previously 600 seconds in older OpenSSH versions), the sshd SIGALRM handler is triggered asynchronously. This handler, however, invokes several functions that are not safe to call from within a signal handler, such as syslog().

The affected third-party software component has been upgraded to a version that includes fixes for the vulnerability. Future versions of the product(s) will not be affected by this vulnerability.

CSCwi59915

Cisco UCS Manager 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).

The affected third-party software component has been upgraded to a version that includes fixes for the vulnerability. Future versions of the product(s) will not be affected by this vulnerability.

Security Fixes in Release 4.2(3k)

The following security issues are resolved:

Defect ID - CSCwh58728

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

- CVE-2023-38408—The PKCS#11 feature in ssh-agent in OpenSSH before 9.3p2 has an insufficiently trustworthy search path, leading to remote code execution if an agent is forwarded to an attacker-controlled system. (Code in `/usr/lib` is not necessarily safe for loading into ssh-agent.)

The affected third-party software component has been upgraded to a version that includes fixes for the vulnerability. Future versions of the product(s) will not be affected by this vulnerability.

Security Fixes in Release 4.2(3j)

The following security issues are resolved:

Defect ID - CSCwh58728

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

- CVE-2023-38408—The PKCS#11 feature in ssh-agent in OpenSSH before 9.3p2 has an insufficiently trustworthy search path, leading to remote code execution if an agent is forwarded to an attacker-controlled system. (Code in `/usr/lib` is not necessarily safe for loading into ssh-agent.)

The affected third-party software component has been upgraded to a version that includes fixes for the vulnerability. Future versions of the product(s) will not be affected by this vulnerability.

Security Fixes in Release 4.2(3i)

The are no security issues in release 4.2(3i).

Security Fixes in Release 4.2(3h)

The following security issues are resolved:

Defect ID - CSCwf30468

Cisco UCS M5 B-Series and 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® 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® Processors may allow a privileged user to potentially enable denial of service through local access.

Defect ID - CSCwf30460

Cisco UCS M6 B-Series and 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® SGX or Intel® TDX for some Intel® Xeon® 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® Xeon® 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® Processors may allow a privileged user to potentially enable escalation of privilege through local access.

Security Fixes in Release 4.2(3g)

The are no security issues in release 4.2(3g).

Security Fixes in Release 4.2(3e)

The are no security issues in release 4.2(3e).

Security Fixes in Release 4.2(3d)

The following security issues are resolved:

Defect ID—CSCwc73237

Cisco UCS B-Series M6 Blade Servers and Cisco UCS C-Series M6 Rack Servers include an Intel® processor that is affected by the vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) ID(s):

- 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-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-2022-33196—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-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-2022-21216—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-2022-36348—Active debug code in some Intel® SPS firmware before version SPS_E5_04.04.04.300.0 may allow an authenticated user to potentially enable escalation of privilege through local access.

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

Defect ID—CSCwd61013

Cisco UCS B-Series M5 Blade Servers and Cisco UCS C-Series M5 Rack Servers include an Intel® processor that is affected by the vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) ID(s):

- 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.

Defect ID—CSCvy93801

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

- CVE-2005-2811—Untrusted search path vulnerability in Net-SNMP 5.2.1.2 and earlier, on Gentoo Linux, installs certain Perl modules with an insecure DT_RPATH, which could allow local users to gain privileges.
- CVE-2007-5846—The SNMP agent (snmp_agent.c) in net-snmp before 5.4.1 allows remote attackers to cause a denial of service (CPU and memory consumption) through a GETBULK request with a large max-repeaters value.

  CVE-2012-6151—Net-SNMP 5.7.1 and earlier, when AgentX is registering to handle a MIB and processing GETNEXT requests, allows remote attackers to cause a denial of service (crash or infinite loop, CPU consumption, and hang) by causing the AgentX subagent to timeout.

  CVE-2014-2310—The AgentX subagent in Net-SNMP before 5.4.4 allows remote attackers to cause a denial of service (hang) by sending a multi-object request with an Object ID (OID) containing more subids than previous requests, a different vulnerability than CVE-2012-6151.

  CVE-2014-3565—`snmplib/mib.c` in net-snmp 5.7.0 and earlier, when the -OQ option is used, allows remote attackers to cause a denial of service (snmptrapd crash) through a crafted SNMP trap message,

which triggers a conversion to the variable type designated in the MIB file, as demonstrated by a NULL type in an ifMtu trap message.

CVE-2015-5621—The snmp_pdu_parse function in `snmp_api.c` in net-snmp 5.7.2 and earlier does not remove the varBind variable in a netsnmp_variable_list item when parsing of the SNMP PDU fails, which allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code through a crafted packet.

CVE-2015-8100—The net-snmp package in OpenBSD through 5.8 uses 0644 permissions for snmpd.conf, which allows local users to obtain sensitive community information by reading this file.

CVE-2018-18065—`_set_key in agent/helpers/table_container.c` in Net-SNMP before 5.8 has a NULL Pointer Exception bug that can be used by an authenticated attacker to remotely cause the instance to crash via a crafted UDP packet, resulting in Denial of Service.

CVE-2018-18066—`snmp_oid_compare in snmplib/snmp_api.c` in Net-SNMP before 5.8 has a NULL Pointer Exception bug that can be used by an unauthenticated attacker to remotely cause the instance to crash via a crafted UDP packet, resulting in Denial of Service.

CVE-2019-20892—net-snmp before 5.8.1.pre1 has a double free in usm_free_usmStateReference in `snmplib/snmpusm.c` through an SNMPv3 GetBulk request. NOTE: this affects net-snmp packages shipped to end users by multiple Linux distributions, but might not affect an upstream release.

CVE-2020-15861—Net-SNMP through 5.7.3 allows Escalation of Privileges because of UNIX symbolic link (symlink) following.

CVE-2020-15862—Net-SNMP through 5.7.3 has Improper Privilege Management because SNMP WRITE access to the EXTEND MIB provides the ability to run arbitrary commands as root.

Defect ID—CSCwc01592

A vulnerability in the backup configuration feature of Cisco UCS Manager Software could allow an unauthenticated attacker with access to a backup file to decrypt sensitive information stored in the full state and configuration backup files.

This vulnerability is due to a weakness in the encryption method used for the backup function. An attacker could exploit this vulnerability by leveraging a static key used for the backup configuration feature. A successful exploit could allow the attacker to decrypt sensitive information that is stored in full state and configuration backup files, such as local user credentials, authentication server passwords, Simple Network Management Protocol (SNMP) community names, and other credentials.

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

See advisory for more details:

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ucsm-bkpsky-H8FCQgsA

Security Fixes in Release 4.2(3b)

The are no security issues in release 4.2(3b).

Security Fixes in Release 4.2(2e)

The are no security issues in release 4.2(2e).

Security Fixes in Release 4.2(2d)

The are no security issues in release 4.2(2d).

Security Fixes in Release 4.2(2c)

The following security issues are resolved:

Defect ID—CSCwb67205

Cisco UCS B-Series M6 Blade Servers; Cisco UCS C-Series M6 Rack Servers include an Intel CPU that is affected the vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) ID(s):

- 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.
- CVE-2021-33060—Users have access to the directory where the installation repair occurs. Since the MS Installer allows regular users to run the repair, an attacker can initiate the installation repair and place a specially crafted EXE in the repair folder which runs with the Check Point Remote Access Client privileges.
- CVE-2022-21233—Stale data may be returned as the result of unauthorized reads to the legacy xAPIC MMIO region. This issue is present only in the legacy xAPIC mode and does not affect the x2APIC mode. This can be used to expose sensitive information in an SGX enclave.

Security Fixes in Release 4.2(2a)

The following security issues are resolved:

Defect ID—CSCwa33718

Cisco has concluded that Cisco UCS Manager contains a vulnerable version of Apache httpd and is affected by the following vulnerabilities:

- CVE-2021-33193—A request sent through HTTP/2 bypasses validation and is forwarded by **mod_proxy**, which can lead to request splitting or cache poisoning. This issue affects Apache HTTP Server 2.4.17 to 2.4.48.
- CVE-2021-34798—A request may cause the server to dereference a NULL pointer. This issue affects Apache HTTP Server 2.4.48 and earlier.
- CVE-2021-36160—A request **uri-path** can cause **mod_proxy_uwsgi** to read above the allocated memory and crash (DoS). This issue affects Apache HTTP Server versions 2.4.30 to 2.4.48.

For more information, see:

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-apache-httpd-2.4.49-VWL69sWQ

Defect ID—CSCwb67158

Cisco UCS B-Series M4 Blade Servers (except B260, B460) and Cisco UCS C-Series M4 Rack Servers (except C460) include an Intel® Processor that is affected by the vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) ID(s):

- CVE-2021-0153—Out-of-bounds write in the BIOS firmware for some Intel® Processors may allow a privileged user to potentially enable escalation of privilege through local access.
- CVE-2021-0154—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-2021-0155—Unchecked return value in the BIOS firmware for some Intel® Processors may allow a privileged user to potentially enable information disclosure through local access.
- CVE-2021-0190—Uncaught exception in the BIOS firmware for some Intel® Processors may allow a privileged user to potentially enable escalation of privilege through local access.
- CVE-2021-33123—Improper access control in the BIOS authenticated code module for some Intel® Processors may allow a privileged user to potentially enable escalation of privilege through local access.
- CVE-2021-33124—Out-of-bounds write in the BIOS authenticated code module for some Intel® Processors may allow a privileged user to potentially enable escalation of privilege through local access.

Defect ID—CSCwb67159

Cisco UCS B-Series M5 Blade Servers and Cisco UCS C-Series M5 Rack Servers include an Intel® processor that is affected by the vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) ID(s):

- CVE-2021-0189—Use of out-of-range pointer offset in the BIOS firmware for some Intel® Processors may allow a privileged user to potentially enable aescalation of privilege through local access.
- CVE-2021-0159—Improper input validation in the BIOS authenticated code module for some Intel® Processors may allow a privileged user to potentially enable aescalation of privilege through local access.
- CVE-2021-33123—Improper access control in the BIOS authenticated code module for some Intel® Processors may allow a privileged user to potentially enable aescalation of privilege through local access.
- CVE-2021-33124—Out-of-bounds write in the BIOS authenticated code module for some Intel® Processors may allow a privileged user to potentially enable aescalation of privilege through local access.
- CVE-2022-21131—Improper access control for some Intel® Xeon® Processors may allow an authenticated user to potentially enable information disclosure through local 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.

Defect ID—CSCwb67157

Cisco UCS B260 M4 Blade Server, Cisco UCS B460 M4 Blade Server, and Cisco UCS C460 M4 Rack Server includes an Intel CPU that is affected by the vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) ID(s):

- CVE-2021-0154—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-2021-0155—Unchecked return value in the BIOS firmware for some Intel® Processors may allow a privileged user to potentially enable information disclosure through local access.
- CVE-2021-0189—Use of out-of-range pointer offset in the BIOS firmware for some Intel® Processors may allow a privileged user to potentially enable aescalation of privilege through local access.
- CVE-2021-33123—Improper access control in the BIOS authenticated code module for some Intel® Processors may allow a privileged user to potentially enable aescalation of privilege through local access.
- CVE-2021-33124—Out-of-bounds write in the BIOS authenticated code module for some Intel® Processors may allow a privileged user to potentially enable aescalation of privilege through local access.

Defect ID—CSCvy67497

Cisco UCS 6400 series FIs include third-party Software that are affected by vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) IDs:

- CVE-2018-14567—If lzma is used with libxml2 2.9.8, it allows remote attackers to cause a denial of service (infinite loop) through a crafted XML file that triggers LZMA_MEMLIMIT_ERROR, as demonstrated by xmllint, a different vulnerability than CVE-2015-8035 and CVE-2018-9251.
- CVE-2018-9251—If lzma is used with the **xz_decomp** function in **xzlib.c** in libxml2 2.9.8, then it allows remote attackers to cause a denial of service (infinite loop) through a crafted XML file that triggers LZMA_MEMLIMIT_ERROR, as demonstrated by xmllint, a different vulnerability than CVE-2015-8035.
- CVE-2021-3541—A flaw was found in libxml2. Exponential entity expansion attack its possible bypassing all existing protection mechanisms and leading to denial of service.

The affected third-party software component has been upgraded to a version that includes fixes for the vulnerability.

CSCwb59981

Cisco UCS M5 Servers include third-party Software that is affected by the vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) IDs:

- CVE-2021-22600—A double free bug in packet_set_ring() in net/packet/af_packet.c can be exploited by a local user through crafted syscalls to escalate privileges or deny service. We recommend upgrading kernel past the effected versions or rebuilding past ec6af094ea28f0f2dda1a6a33b14cd57e36a9755.

The affected third-party software component has been upgraded to a version that includes fixes for the vulnerability.

CSCvm84140

Cisco UCS Manager is updated with new secure code best practices to enhance the security posture and resilience.

CSCvt82214

Cisco UCS 6400 series FIs include third-party Software that are affected by vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) IDs:

- CVE-2017-15906—The process_open function in sftp-server.c in OpenSSH before 7.6 does not properly prevent write operations in readonly mode, which allows attackers to create zero-length files.

- CVE-2018-15919—Remotely observable behavior in auth-gss2.c in OpenSSH through 7.8 could be used by remote attackers to detect existence of users on a target system when GSS2 is in use.
- CVE-2019-6111—An issue was discovered in OpenSSH 7.9. Due to the scp implementation being derived from 1983 rcp, the server chooses which files/directories are sent to the client. However, the scp client only performs cursory validation of the object name returned (only directory traversal attacks are prevented). A malicious scp server (or Man-in-The-Middle attacker) can overwrite arbitrary files in the scp client target directory. If recursive operation (-r) is performed, the server can manipulate subdirectories as well (for example, to overwrite the .ssh/authorized_keys file).

Cisco has released software updates that address these vulnerability.

CSCvu63738

Cisco UCS 6400 series FIs include third-party Software that are affected by vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) IDs:

- CVE-2018-15473—OpenSSH through 7.7 is prone to a user enumeration vulnerability due to not delaying bailout for an invalid authenticating user until after the packet containing the request has been fully parsed, related to auth2-gss.c, auth2-hostbased.c, and auth2-pubkey.c.
- CVE-2018-15919—Remotely observable behavior in auth-gss2.c in OpenSSH through 7.8 could be used by remote attackers to detect existence of users on a target system when GSS2 is in use.
- CVE-2019-6111—An issue was discovered in OpenSSH 7.9. Due to the scp implementation being derived from 1983 rcp, the server chooses which files/directories are sent to the client. However, the scp client only performs cursory validation of the object name returned (only directory traversal attacks are prevented). A malicious scp server (or Man-in-The-Middle attacker) can overwrite arbitrary files in the scp client target directory. If recursive operation (-r) is performed, the server can manipulate subdirectories as well (for example, to overwrite the .ssh/authorized_keys file).

CSCwa65691

Cisco UCS 6400 series FIs include third-party Software that are affected by vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) IDs:

- CVE-2017-15906—The process_open function in sftp-server.c in OpenSSH before 7.6 does not properly prevent write operations in readonly mode, which allows attackers to create zero-length files.
- CVE-2018-15919—Remotely observable behavior in auth-gss2.c in OpenSSH through 7.8 could be used by remote attackers to detect existence of users on a target system when GSS2 is in use.
- CVE-2019-6111—An issue was discovered in OpenSSH 7.9. Due to the scp implementation being derived from 1983 rcp, the server chooses which files/directories are sent to the client. However, the scp client only performs cursory validation of the object name returned (only directory traversal attacks are prevented). A malicious scp server (or Man-in-The-Middle attacker) can overwrite arbitrary files in the scp client target directory. If recursive operation (-r) is performed, the server can manipulate subdirectories as well (for example, to overwrite the .ssh/authorized_keys file).

Security Fixes in Release 4.2(1n)

The following security issues are resolved:

Defect ID—CSCwb67157

Cisco UCS B260 M4 Blade Server, Cisco UCS B460 M4 Blade Server, and Cisco UCS C460 M4 Rack Server includes an Intel CPU that is affected by the vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) ID(s):

- CVE-2021-0154—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-2021-0155—Unchecked return value in the BIOS firmware for some Intel® Processors may allow a privileged user to potentially enable information disclosure through local access.
- CVE-2021-0189—Use of out-of-range pointer offset in the BIOS firmware for some Intel® Processors may allow a privileged user to potentially enable aescalation of privilege through local access.
- CVE-2021-33123—Improper access control in the BIOS authenticated code module for some Intel® Processors may allow a privileged user to potentially enable aescalation of privilege through local access.
- CVE-2021-33124—Out-of-bounds write in the BIOS authenticated code module for some Intel® Processors may allow a privileged user to potentially enable aescalation of privilege through local access.

Defect ID—CSCwb67158

Cisco UCS B-Series M4 Blade Servers (except B260, B460) and Cisco UCS C-Series M4 Rack Servers (except C460) include an Intel® Processor that is affected by the vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) ID(s):

- CVE-2021-0153—Out-of-bounds write in the BIOS firmware for some Intel® Processors may allow a privileged user to potentially enable escalation of privilege through local access.
- CVE-2021-0154—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-2021-0155—Unchecked return value in the BIOS firmware for some Intel® Processors may allow a privileged user to potentially enable information disclosure through local access.
- CVE-2021-0190—Uncaught exception in the BIOS firmware for some Intel® Processors may allow a privileged user to potentially enable escalation of privilege through local access.
- CVE-2021-33123—Improper access control in the BIOS authenticated code module for some Intel® Processors may allow a privileged user to potentially enable escalation of privilege through local access.
- CVE-2021-33124—Out-of-bounds write in the BIOS authenticated code module for some Intel® Processors may allow a privileged user to potentially enable escalation of privilege through local access.

Defect ID—CSCwb67159

Cisco UCS B-Series M5 Blade Servers and Cisco UCS C-Series M5 Rack Servers include an Intel® processor that is affected by the vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) ID(s):

- CVE-2021-0189—Use of out-of-range pointer offset in the BIOS firmware for some Intel® Processors may allow a privileged user to potentially enable aescalation of privilege through local access.
- CVE-2021-0159—Improper input validation in the BIOS authenticated code module for some Intel® Processors may allow a privileged user to potentially enable aescalation of privilege through local access.

- CVE-2021-33123—Improper access control in the BIOS authenticated code module for some Intel® Processors may allow a privileged user to potentially enable aescalation of privilege through local access.
- CVE-2021-33124—Out-of-bounds write in the BIOS authenticated code module for some Intel® Processors may allow a privileged user to potentially enable aescalation of privilege through local access.
- CVE-2022-21131—Improper access control for some Intel® Xeon® Processors may allow an authenticated user to potentially enable information disclosure through local 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.

Defect ID—CSCwb67205

Cisco UCS B-Series M6 Blade Servers; Cisco UCS C-Series M6 Rack Servers include an Intel CPU that is affected the vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) ID(s):

- 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(1m)

The are no security issues in release 4.2(1m).

Security Fixes in Release 4.2(1l)

The are no security issues in release 4.2(1l).

Security Fixes in Release 4.2(1k)

The are no security issues in release 4.2(1k).

Security Fixes in Release 4.2(1i)

The are no security issues in release 4.2(1i).

Security Fixes in Release 4.2(1f)

The are no security issues in release 4.2(1f).

Security Fixes in Release 4.2(1d)

The are no security issues in release 4.2(1d).

Resolved Caveats

The resolved bugs for a release are accessible through the Cisco Bug Search Tool. This web-based tool provides you with access to the Cisco bug tracking system, which maintains up-to-date information about bugs and vulnerabilities in this product and other Cisco hardware and software products.

Resolved Caveats in Release 4.2(3s)

The following caveats are resolved in Release 4.2(3s):

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCwn60596	After an infrastructure firmware upgrade, KVM consoles can become inoperable even though the assigned KVM IP address remains reachable. This issue has been observed in domains with multiple chassis and out-of-band management after firmware upgrades or PMON restarts. This issue is resolved.	4.3(4a)	4.2(3s)

Resolved Caveats in Release 4.2(3r)

The following caveats are resolved in Release 4.2(3r):

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCwt18924	Cisco UCS C220 M6 servers with Cisco UCS VIC 1467 adapters experience an adapter crash caused by a memory leak in the MCP process during an upgrade of the ACI fabric. After the adapter reset, physical ports come back online, but the vNICs remain stuck in initializing and do not recover without a server reboot. This issue occurs when upstream ACI switches are upgraded and rebooted, causing link flaps and requiring manual server reboot for vNICs recovery. The adapter logs indicate fatal errors related to out-of-memory conditions leading to the MCP process termination and adapter reset. This issue is resolved.	4.2(3m)	4.2(3r)
CSCwo84672	The UCS-S3260-NVMW64T drive may report a `Drive Failed. Needs reseat or replacement: Fault State 1` error. The failure is also logged in OBFL logs and the drive status shows as failed with a corresponding LED fault indication. This issue is resolved.	4.3(6c)	4.2(3r)

Resolved Caveats in Release 4.2(3p)

The following caveats are resolved in Release 4.2(3p):

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCwo48958	The KVM launch from Cisco UCS Central fails when using Cisco UCS Manager 4.3(6a) with KVM client version 1.0.21. The launch opens a vKVM login page, but after accepting the certificate, the connection times out. This issue does not occur with Cisco UCS Manager 4.3(5c) and KVM client version 1.0.17, where KVM launches successfully from Cisco UCS Central GUI. The problem is specific to the integration of KVM client 1.0.21 with Cisco UCS Manager 4.3(6a) domains. This issue is resolved.	4.3(6c)	4.2(3p)

Resolved Caveats in Release 4.2(3o)

The following caveats are resolved in Release 4.2(3o):

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCwn00366	Server discovery failures occur on Cisco UCS C-series FI-managed Intersight Rack Servers with only eNICs or only vHBAs configured, due to a memory leak in the vniccfgd process triggered by the palo_vnic_listtype() API call. Over months, the memory leak accumulates, leading to failures once a threshold is crossed. Cisco UCS VIC 14xx and 15xxx series adapters experience persistent failures, while Cisco UCS VIC 13xx series adapters may reboot due to out-of-memory errors. This issue is resolved.	4.2(3b)	4.2(3o)
CSCwm47183	Certain HDDs (model MG06SCA800A) unexpectedly show removal marks by the backup application, even though Cisco IMC logs do not indicate any failures. This issue occurs on the Cisco UCS C240 M6 servers with firmware version 4.3(2.240002) equipped with Cisco 12G SAS HBA controller. Disk I/O errors indicate timeouts and read issues, preventing successful mounting and leading to removal marks on the disks. This situation impacts clusters using the backup application, requiring further investigation to prevent disruptions. This issue is resolved.	4.3(2e)C	4.2(3o)C

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCwm83085	In Cisco UCS Manager, changing the FCoE VLAN associated with a VSAN can result in the loss of storage paths from the operating system perspective, even though Fibre Channel interfaces remain active and stable. This issue occurs in Cisco UCS 6454 FI environments using FC Switching mode connected directly to storage. Although the switch accurately reflects the changes, the operating system reports a loss of storage paths. Flapping the FC interfaces temporarily restores connectivity. This issue is resolved.	4.3(5a)B	4.2(3o)B
CSCwn32035	On certain Cisco UCS-IOM-2408 boards, system fans may cause the SDA line of the I2C bus to remain low for extended periods, resulting in a bus lockup. This issue arises when the I2C hub channel is deselected during its built-in unlocking process. This issue is resolved.	4.3(5a)	4.2(3o)

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCwf61769	After upgrading the Cisco UCS 6554 or 64108 FI infrastructure bundle to release 4.2(2c) or later, you may experience issues with specific SNMP OIDs at random times. The SNMP agent may intermittently report noSuchInstance for OID ".1.3.6.1.2.1.2.2.1.10.xxxxx", which tracks the total number of octets received on the interface. Additionally, it may incorrectly report a value of 1 for OID ".1.3.6.1.2.1.2.1.0", which represents the total number of network interfaces present on the system, regardless of their current state. Only these two OIDs are affected under these conditions. This issue is resolved.	4.2(2c)A	4.2(3o)A
CSCwf63137	Cisco UCS Manager may temporarily lose connection with Cisco UCS-FI-6454 running release 4.2(2c). This potential issue occurs during the restart of the NGINX process. Although no direct impact has been observed, faults may be presented in Cisco UCS Manager and detected by various monitoring tools if FI Syslogs are being monitored. This issue is resolved.	4.2(2c)A	4.2(3o)A

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCwm80801	After applying the July 2024 patch KB5040434, you may experience issues logging into UCS devices through Radius, although other Cisco devices remain unaffected. This problem impacts UCS devices. The issue occurs in a system equipped with Cisco UCS 6332 FI managed by Cisco UCS Manager version 4.2(3h), and it may potentially affect any UCS device following the NPS upgrade with the specified patch. This issue is resolved.	4.2(3h)A	4.2(3o)A
CSCwm62828	Cisco UCS Manager may display a warning indicating that the service profile association is not fulfilled due to an incompatible number of local disks while managing Cisco UCS B200 M5 servers equipped with a Cisco UCSB-MRAID12G-HE RAID controller. This issue is resolved.	4.1(3d)	4.2(3o)
CSCwn65779	In Cisco UCS Manager release version 4.2(3g), the Cisco UCS 64108 Fabric Interconnects experience unexpected reboots due to kernel panics, resulting in cluster failovers. This issue is resolved	4.2(3g)A	4.2(3o)A

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCwn69805	The Cisco UCS 64108 Fabric Interconnect reboots unexpectedly, leading to a loss of network redundancy and high availability (HA), although the fabric interconnect eventually recovers itself. This issue is resolved.	4.2(1n)A	4.2(3o)A
CSCwn83351	In certain conditions, a system reload may occur due to a **watchdog timeout** without generating cores or traces. The issue is identified when the system reset reason indicates a **watchdog timeout** or **CATERR**. This issue is resolved.	4.3(5a)A	4.2(3o)A
CSCwm13829	On Cisco UCS X210c M6/M7 servers with a UCSX-X10C-RAIDF RAID controller, a BBU fault may occur, indicated by Safety Status Register 0xf000 in logs. This indicates a corrupted voltage reading, marking the BBU as bad and potentially needing replacement. To resolve, access the RAID setup during boot, reset to factory defaults, confirm, and save changes.	5.2(0.230092)	4.2(3o)

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCwn41380	In Fibre Channel (FC) connectivity, a faulty FC link (such as a bad SFP or cable) might cause the upstream switch to attempt recovery or shut down the port. This can lead to UCS Manager reporting that chassis connectivity is down or disconnected, even though the links remain functional. This issue is resolved.	4.3(4b)A	4.2(3o)A

Resolved Caveats in Release 4.2(3n)

The following caveats are resolved in Release 4.2(3n):

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCwn42969	After power cycling or resetting a Cisco UCS server, NVME disk FRONT-NVME-2 may become inoperable when left idle for over 1.5 weeks or under minimal workload. If this issue occurs and the drive is inoperable, check your drive PID against Drive PIDs for NVME Disk FRONT-NVME Inoperable Issue - CSCwn42969, on page 116. If listed, contact Cisco TAC for a replacement. If not listed, upgrade to firmware release 9CV10490.	4.3(4e)	4.2(3n)

Drive PIDs for NVME Disk FRONT-NVME Inoperable Issue - CSCwn42969

UCSX-NVME4-1600-D, UCSX-NVME4-1600-D=, HX-NVME4-1600, HX-NVME4-1600=, UCS-NVME4-3200, UCS-NVME4-3200=, UCSB-NVME4-3200, UCSB-NVME4-3200=, UCSX-NVME4-3200, UCSX-NVME4-3200=, UCS-NVME4-3200-D, UCS-NVME4-3200-D=,

UCSX-NVME4-3200-D, UCSX-NVME4-3200-D=, HX-NVME4-3200, HX-NVME4-3200=, UCS-NVME4-6400, UCS-NVME4-6400=, UCSB-NVME4-6400, UCSB-NVME4-6400=, UCSX-NVME4-6400, UCSX-NVME4-6400=, UCS-NVME4-6400-D, UCS-NVME4-6400-D=, UCSX-NVME4-6400-D, UCSX-NVME4-6400-D=, HX-NVME4-6400, HX-NVME4-6400=, UCS-NVME4-1920, UCS-NVME4-1920=, UCSB-NVME4-1920, UCSB-NVME4-1920=, UCSX-NVME4-1920, UCSX-NVME4-1920=, UCS-NVME4-1920-D, UCS-NVME4-1920-D=, UCSX-NVME4-1920-D, UCSX-NVME4-1920-D=, HX-NVME4-1920, HX-NVME4-1920=, UCS-NVME4-3840, UCS-NVME4-3840=, UCSB-NVME4-3840, UCSB-NVME4-3840=, UCSX-NVME4-3840, UCSX-NVME4-3840=, UCS-NVME4-3840-D, UCS-NVME4-3840-D=, UCSX-NVME4-3840-D, UCSX-NVME4-3840-D=, HX-NVME4-3840, HX-NVME4-3840=, UCS-NVME4-7680, UCS-NVME4-7680=, UCSB-NVME4-7680, UCSB-NVME4-7680=, UCSX-NVME4-7680, UCSX-NVME4-7680=, UCS-NVME4-7680-D, UCS-NVME4-7680-D=, UCSX-NVME4-7680-D, UCSX-NVME4-7680-D=, HX-NVME4-7680, HX-NVME4-7680=, UCS-NVME4-15360, UCS-NVME4-15360, UCSB-NVME4-15360, UCSB-NVME4-15360, UCSX-NVME4-15360, UCS-NVME4-15360-D, UCSX-NVME4-15360D, HX-NVME4-15360, HX-NVME4-15360, UCSX-NVB1T6O1P, UCSX-NVB1T6O1P=, HX-NVB1T6O1PM6, HX-NVB1T6O1PM6=, UCS-NVB3T2O1PM6, UCS-NVB3T2O1PM6=, UCSB-NVA3T2O1P, UCSB-NVA3T2O1P=, UCSX-NVB3T2O1PM6, UCSX-NVB3T2O1PM6=, UCS-NVB3T2O1P, UCS-NVB3T2O1P=, UCSX-NVB3T2O1P, UCSX-NVB3T2O1P=, HX-NVB3T2O1PM6, HX-NVB3T2O1PM6=, UCS-NVB6T4O1PM6, UCS-NVB6T4O1PM6=, UCSB-NVA6T4O1P, UCSB-NVA6T4O1P=, UCSX-NVB6T4O1PM6, UCSX-NVB6T4O1PM6=, UCS-NVB6T4O1P, UCS-NVB6T4O1P=, UCSX-NVB6T4O1P, UCSX-NVB6T4O1P=, HX-NVB6T4O1PM6, HX-NVB6T4O1PM6=, UCS-NVB1T9O1VM6, UCS-NVB1T9O1VM6=, UCSB-NVA1T9O1V, UCSB-NVA1T9O1V=, UCSX-NVB1T9O1VM6, UCSX-NVB1T9O1VM6=, UCS-NVB1T9O1V, UCS-NVB1T9O1V=, UCSX-NVB1T9O1V, UCSX-NVB1T9O1V=, HX-NVB1T9O1VM6, HX-NVB1T9O1VM6=, UCS-NVB3T8O1VM6, UCS-NVB3T8O1VM6=, UCSB-NVA3T8O1V, UCSB-NVA3T8O1V=, UCSX-NVB3T8O1VM6, UCSX-NVB3T8O1VM6=, UCS-NVB3T8O1V, UCS-NVB3T8O1V=, UCSX-NVB3T8O1V, UCSX-NVB3T8O1V=, HX-NVB3T8O1VM6, HX-NVB3T8O1VM6=, UCS-NVB7T6O1VM6, UCS-NVB7T6O1VM6=, UCSB-NVA7T6O1V, UCSB-NVA7T6O1V=, UCSX-NVB7T6O1VM6, UCSX-NVB7T6O1VM6=, UCS-NVB7T6O1V, UCS-NVB7T6O1V=, UCSX-NVB7T6O1V, UCSX-NVB7T6O1V=, HX-NVB7T6O1VM6, HX-NVB7T6O1VM6=, UCS-NVB15TO1VM6, UCS-NVB15TO1VM6, UCSB-NVA15TO1V, UCSB-NVA15TO1V, UCSX-NVB15TO1VM6, UCS-NVB15TO1V, UCSX-NVB15TO1V, HX-NVB15TO1VM6, HX-NVB15TO1VM6

Resolved Caveats in Release 4.2(3m)

The following caveats are resolved in Release 4.2(3m):

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCwm72893	Under rare conditions, Cisco UCS VIC adapter may experience a firmware hang due to a software anomaly in the embedded CPU (eCPU), leading to a watchdog timeout and Non-Maskable Interrupt (NMI). This can result in temporary storage connectivity loss. This issue is resolved. The latest firmware update addresses this issue by enhancing error-handling mechanisms to prevent such occurrences.	4.2(3i)A	4.2(3m)A

Resolved Caveats in Release 4.2(3l)

The following caveats are resolved in Release 4.2(3l):

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCwk28221	When changing the FCoE VLAN from 3121 to 3120 in Cisco UCS Manager while FI is in FC Switch mode, initiators can FLOGI and obtain FCID but fail to PLOGI to target ports, resulting in indefinite timeouts. Admin down/up of the FC link or port-channel resolves the issue. This change causes path loss in ESXi, with host logs showing successful FLOGI and FCID assignment but PLOGI timeouts. This issue is resolved.	4.3(2b)A	4.2(3l)A
CSCwj28488	Cisco UCS server is unable to start the PNUOS because BIOS/bt/biosSecureVars/dbx_os file with an invalid certificate prevents PNUOS from operating. The dbx_os file holds certificates added by the operating system and specifies which certificates are prohibited from loading. The cause of the failure is a secure boot violation and following error message is displayed: `Invalid signature detected. Check secure boot policy in setup` This issue is resolved.	4.3(3a)A	4.2(3l)A
CSCwk47042	During migration from Cisco UCS 6300 FI Series to Cisco UCS 6500 FI Series, configuring FC storage ports results in errors in both Cisco UCS Manager GUI and CLI, indicating that FC Breakout is not supported. This issue is resolved.	4.2(3i)A	4.2(3l)A
CSCwf96053	When deploying a new Cisco UCS Domain within a Cisco UCS Central environment, global identifiers such as MAC pools, UUID pools, and iSCSI IP pools are not visible on Cisco UCS 6454 FI domains. This issue does not affect Cisco UCS 6300 FI. The issue occurs with Cisco UCS Central 2.0(1r) and Cisco UCS Manager 4.2(3d) on Cisco UCS 6454 FI, while Cisco UCS Manager 4.2(2c) or 4.2(1d) on Cisco 6300 FI works fine. The issue persists despite pushing global policies and identifiers from Cisco UCS Central. This issue is resolved.	4.2(3k)A	4.2(3l)A

Resolved Caveats in Release 4.2(3k)

The following caveats are resolved in Release 4.2(3k):

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCwe35644	Several ECCs are observed on a single DIMM with no fault from Cisco UCS Manager in Cisco UCS C-Series and B-Series M5 and M6 servers equipped with 64GB DIMMs (UCS-MR-X64G2RW) and ADDDC enabled. This issue is resolved.	4.1(3e)B and C	4.2(3k)B and C
CSCwf03588	In a setup equipped with Cisco UCS 6454 FI, all the IOMs display the following fault: `Critical F1707 time-stamp 6270802 CMCLowMem : Please check the Health tab for more details` This issue is resolved.	4.2(2d)A	4.2(3k)A
CSCwh65058	Cisco UCS 6454 FI operating on release 4.2(1l) might experience difficulties establishing FC (Fibre Channel) port-channels with 93180YC-FX switches that are on release 10.2(6)M. There is a possibility that the port-channel could enter an error-disabled state as soon as the links are activated. This issue is resolved.	4.2(1l)A	4.2(3k)A
CSCwe38504	Cisco UCS 6454 FI operating on any 4.2(1) release cause a surge in CPU utilization to 100% for bladeAG, resulting in the process exhausting available memory. As a result, this prevents the peer Fabric Interconnect from being programmed during startup. This issue is resolved.	4.2(1i)A	4.2(3k)A
CSCwi76042	Upon deletion of a VLAN from the VLAN group that is utilized by both Uplinks and vNICs, the vNICs momentarily lose connection, displaying an ENM Pinning failure error. The vNICs are expected to automatically restore their connection and become operational again. Cisco UCS Manager indicate the vNIC status as **down** and attribute the cause to an ENM pinning source failure. This issue is resolved.	4.2(3e)A	4.2(3k)A

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCwj10758	In Cisco UCS Manager release 4.3(3), 4.3(2), and 4.2(3), an issue has been identified where SSH logins for users authenticated through LDAP, RADIUS, or TACACS fail on Cisco UCS 6500 and 6400 series FIs, but not on Cisco UCS 6300 FIs. The SSH login succeeds if there is an active HTTP/HTTPS web session or an existing SSH session for the same user. This issue does not affect GUI or telnet logins for remotely authenticated users, nor does it impact SSH logins using local Cisco UCS Manager credentials. This issue is resolved.	4.2(3i)	4.2(3k)A
CSCwj28369	Cisco UCS 6454 Fabric Interconnect experiences failures attributed to a High Availability (HA) policy reset, specifically due to Link Layer Discovery Protocol (LLDP) related issues. System logs obtained via show system reset-reason confirm that the device is automatically performing resets due to an HA policy. This issue is resolved.	4.2(3j)	4.2(3k)A
CSCwd35712	A critical defect has been identified in the Cisco UCS Manager where the Data Management Engine (DME) crashes due to an **instance id not found** error. Additional symptoms include the inability to access the Cisco UCS Manager GUI, non-functionality of cluster management services, and a core dump indicated by the **show pmon state** command via SSH. The problem is not firmware-specific and can impact any Cisco UCS Manager domain. Although the data plane and server operations of the domain remain unaffected, there is no workaround for this issue, and affected environments may require restoration from a backup. This issue is resolved.	4.2(1d)	4.2(3k)

Resolved Caveats in Release 4.2(3j)

The following caveats are resolved in Release 4.2(3j):

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCwi54393	When Cisco UCS setup with Linux OS, some LUNs do not get mounted when the setup is starting boot time with PXE boot along with lot of SAN LUNs. This issue is resolved.	4.1(3k)A	4.2(3j)A
CSCwh30074	Cisco UCS 6332 FI unexpectedly gets reset with the following reason: `vlan_mgr hap reset` This issue is resolved.	4.2(2c)A	4.2(3j)A
CSCwh67130	In a setup equipped with Cisco UCS X-Series servers with Cisco UCS 9108 25G IFMs, communication issues are seen with the upstream network. This issue is resolved.	4.2(1i)A	4.2(3j)A
CSCwi22301	In a setup with Cisco UCS 6332-16UP FIs, unconnected FC interfaces on both the FIs log unexpected errors. This issue is resolved.	4.1(2b)A	4.2(3j)A
CSCwe95417	After upgrading Cisco UCS 6332-16UP FIs to infra bundle release 4.2(2c)A, chassis power chart shows abnormal readings. This issue is resolved.	4.2(2c)A	4.2(3j)A
CSCwe88483	Cisco UCS 6454 FIs crash with MCE errors This issue is resolved.	4.2(2c)A	4.2(3j)A
CSCwe73172	Cisco UCS Manager fails to connect to NX-OS from CLI interface. This issue is resolved.	4.2(3i)	4.2(3j)
CSCwi07879	When VLAN group permissions are provided at the root level to the vNIC created at sub-org level, shows configuration failure. This issue is resolved.	4.2(2c)A	4.2(3j)A
CSCwe96606	Cisco UCS 6454 FIs display `svc_sam_samcproxy` process failure messages. This issue is resolved.	4.2(3d)A	4.2(3j)A
CSCwh31644	Cisco UCS Manager fails to discover any Chassis or rack servers. This issue is resolved.	4.2(3e)A	4.2(3j)A

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCwd15750	In a setup equipped with Cisco UCS 645 FIs, primary FI reboots during auto-install, without user acknowledgement. This issue is resolved.	4.1(3e)A	4.2(3j)A
CSCwh28338	vMedia image mount fails during OS deployment on a server with OOB IP configuration. This issue happens because the IP NAT is on the secondary FI, while the Cisco IMC is informed that it resides on primary FI. This issue is resolved.	4.2(3g)A	4.2(3j)A
CSCwh28856	In a setup equipped with Cisco UCS 6454 FIs, Cisco UCS Manager BladeAG crashes due to lack of memory. This issue is resolved.	4.2(3d)A	4.2(3j)A
CSCwh47000	Cisco UCS Manager does not show updated IOM transceiver information. This issue is resolved.	4.2(1l)A	4.2(3j)A
CSCwh75796	SCP backup on Linux host server fails due to MOD message. This issue is resolved.	4.2(3h)C	4.2(3j)C
CSCwf93621	In a setup equipped with Cisco UCS M5 servers, discovery and association may fail due to a faulty drive. This issue is resolved.	4.2(3d)C	4.2(3j)C
CSCwi54458	Cisco UCS Manager may show incorrect firmware version of storage controllers. This issue is resolved.	4.2(3i)C	4.2(3j)C
CSCwh04150	In a setup equipped with Cisco UCS 6400 Series FI and UCSX-I-9108-25G IOM, packets destined to IP addresses ending in **136.204** are dropped before reaching the FI. These packets do not show up in ELAM. Packets to other IP addresses in that same subnet are not impacted. This issue is resolved.	4.2(3d)A	4.2(3j)A

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCwh86319	Storage space is taken up by files with the name `libsatmgr-pid-<number>.log`, which continuously get created. This leads to lack of storage space and as a result the following error message is seen while logging into Cisco UCS FI using CLI interface: `2023-10-11 12:36:40.292501665 -0700 PDT m=+1800.083030916 write error: write /var/sysmgr/sam_logs/ism_shell_20231011120640.log: no space left on device` This issue is resolved.	4.1(3m)A	4.2(3j)A
CSCvq34125	In a setup equipped with 6400 or 64108 FIs, Cisco UCS Manager GUI and CLI interface show FI fan RPM as zero This issue is resolved.	4.0(4c)A	4.2(3j)A

Resolved Caveats in Release 4.2(3i)

The following caveats are resolved in Release 4.2(3i):

Defect ID	Symptom	First Bundle 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 resolved.	4.1(3d)A	4.2(3i)A
CSCwf88211	Cisco UCS C240 M6 servers may show the following error while in operation: `AdapterHostEthInterfaceDown` There is no functionality impact. This issue is resolved.	4.2(3h)A	4.2(3i)A

Resolved Caveats in Release 4.2(3h)

The following caveats are resolved in Release 4.2(3h):

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCwf61835	In a setup equipped with Cisco UCS 15000 Series VIC adatpers and ESXi OS, the adapters may become unreachable and be in hung state. Internal PO goes down and the backplane connection link also shows as link down. All the vNICs/vHBAs are also in a down state. This issue is resolved.	4.2(2a)B and C	4.2(3h)B and C
CSCwf52054	Cisco UCS 2200/2300/2400 IOMs may go offline after upgrading to release 4.2(3d). This issue is resolved.	4.2(3d)A	4.2(3h)A
CSCwe98053	CRC errors are seen in a setup equipped with Cisco UCS 2408 IOM connected to Cisco UCS B-Series server HIF ports. This issue is resolved.	4.2(2a)A	4.2(3h)A
CSCwh15315	Third-party SFP goes into unsupported state after upgrading to release 4.2(2a)A or later. This issue is resolved.	4.2(2a)A	4.2(3h)A
CSCwf92065	SNMP configuration does not restore in NXOS after SNMPD restart. This issue is resolved.	4.2(2c)A	4.2(3h)A
CSCwf56940	Cisco UCS Manager does not display Mexico timezones/daylight saving updates correctly. This issue is resolved.	4.2(1l)A	4.2(3h)A
CSCwf56305	Cisco UCS VIC 1455 shows incorrect Port enumeration. This issue is resolved.	4.2(2a)A	4.2(3h)A
CSCwf73403	On a Cisco UCS 6454 Fabric Interconnect, on initial boot or after an erase configuration, the fabric interconnect did not boot to the initial configuration prompt. After finishing boot, the fabric interconnect showed a login prompt with the default hostname of switch. This issue is resolved.	4.2(3b)A	4.2(3h)A

Resolved Caveats in Release 4.2(3g)

The following caveats are resolved in Release 4.2(3g):

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCwe45912	In a cluster setup with Cisco UCS 6400 series FI or 6536 FI, after a server reboot, if the MAC address is learned through the impacted FI, then the ARP is unable to resolve on any OS. This issue does not impact the servers, which are not rebooted. This issue is resolved.	4.2(1i)A	4.2(3g)A
CSCwf05062	Cisco UCS 6454 FI crashes and recovers due to following error: `%SYSMGR-2-SERVICE_CRASHED: Service "mfdm" (PID 15518) hasn't caught signal 6 (core will be saved). %$ VDC-1 %$ %SYSMGR-2-HAP_FAILURE_SUP_RESET: Service "mfdm" in vdc 1 has had a hap failure` This issue is resolved.	4.1(3h)A	4.2(3g)A
CSCwf44680	In a setup equipped with Cisco UCS 6454 FI, when IP Unicast/Subnet-broadcast packet destined to Link-Layer broadcast is received over Mgmt port of FI, the packet is routed over Mgmt0 Interface. This results in FI sending back the received packet with the Mgmt0 source MAC address leading to upstream device on the network detecting the same destination IP address with a different source MAC address. This issue is resolved.	4.2(3e)A	4.2(3g)A
CSCwe54991	Following command is unavailable in Cisco UCS 6400 FI series: **`show platform software enm internal info vlandb`** This issue is resolved.	4.2(1m)A	4.2(3g)A
CSCwf14446	Cisco UCS 6296 FI resets without warning. Following reset reason is displayed: `Reason: Reset triggered due to HA policy of Reset Service: npv hap reset` This issue is resolved.	4.1(3i)A	4.2(3g)A

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCwf28562	In a setup equipped with Cisco UCS 6300 Series FI, DME service crashes when the server is upgraded from 4.0(4b) to 4.2(2), which is not supported. This issue is resolved. DME services do not crash. Refer Upgrade and Downgrade Guidelines, on page 8 for supported upgrade paths.	4.2(2c)A	4.2(3g)A
CSCwf31814	In a setup equipped with the following: • Cisco UCS 64108 FI • Cisco UCS 1340 VIC or Intelx710 adapter • Cisco UCS C240 M4 server svc_sam_samcproxy and svc_sam_dme services crash. This issue is resolved.	4.2(2e)A	4.2(3g)A

Resolved Caveats in Release 4.2(3e)

The following caveats are resolved in Release 4.2(3e):

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCwe51233	After successfully adding the LDAP provider, unable to view the details in Cisco UCS Manager GUI. However, the details can be viewed in UCS Manager CLI. The following error is displayed when attempted to re-add the LDAP provider details: `Cannot create; object already exists` This issue is resolved.	4.2(2a)A	4.2(3e)A
CSCwe25437	Unable to proceed with the Certificate Signing Request (CSR) due to same name entered on both DNS and Subject fields. The following error message is displayed: `Failed to change Certificate Request. DNS value and subject value is the same. Modify any one and retry` This issue is resolved.	4.2(2c)A	4.2(3e)A

Resolved Caveats in Release 4.2(3d)

The following caveats are resolved in Release 4.2(3d):

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCwd77505	In a setup equipped with Cisco UCS 6300 FI, VM losses connectivity in case of a fail over event or if the VM is migrated to a different host. This issue is resolved.	4.2(2b)	4.2(3d)
CSCwd41247	Multiple instances of hung **Samcproxy** is observed in a setup equipped with Cisco UCS 6400 FI. There may also be other miscellaneous faults on the domain related to **Samcproxy** being in a bad state. This issue is resolved.	4.2(1i)A	4.2(3d)A
CSCwe24011	Unexpected reboot is observed during normal operation in Cisco UCS 6536 FI and Cisco UCS 6400 FI series FIs. This issue is resolved.	4.2(2d)A	4.2(3d)A
CSCwd90187	In a setup equipped with Cisco UCS 6536 FI, port goes to **Link not connected** status when QSFP-100G-DR/FR-S is replaced with QSFP-100G-CUxM under the following conditions: • 100G interface Interface is configured with **FEC Auto** Interface was using QSFP-100G-FR, QSFP-100G-DR transceivers Interface now uses QSFP-100G-CUxM, where CUxM refers to CU1M, CU2M, and so on. This issue is resolved.	4.2(2a)A	4.2(3d)A
CSCvz81322	In a setup configured with VLAN groups and mapped with FI uplink interfaces, an unexpected outage was experienced when a VLAN is removed from a vNIC template or from a VLAN group. This issue has been resolved. This issue is resolved.	4.1(3c)A	4.2(3d)A

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCwd66780	While upgrading Cisco UCS Manager from release 4.2(1f) to 4.2(2a) , SAN port-channel reports the following admin down error: `san port-channel 50 on fabric interconnect B oper state: admin-down, reason: Administratively downSan port-channel 50 On fabric Interconnect A oper state : admin-down reason : Administratively down` This issue is resolved.	4.2(1f)A	4.2(3d)A
CSCwe28336	MTS buffer stuck on `vsh.bin` process. The process crashes and impacts other functionality once the limit is reached. This issue is resolved.	4.2(2a)A	4.2(3d)A
CSCwe02107	In a setup equipped with Cisco UCS 6400 FI, Multicast streams are not accepted by the server. This issue is resolved.	4.1(3b)A	4.2(3d)A

Resolved Caveats in Release 4.2(3b)

The following caveats are resolved in Release 4.2(3b):

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCwc66309	Activity LED on Intel P5520/P5620 and P5316 QLC drives on Cisco UCS M6 servers switch off once it is plugged in and when the server is idle. It displays no activity but the drive is operational. This issue is resolved.	4.2(2b)	4.2(3b)
CSCwb90877	In a setup equipped with Cisco UCS 6400 series FI, Cisco UCS rack server discovery fails if the server ID is configured a 255 while recommissioning. Discovery fails during **PnuosIdent** stage. This issue occurs while recommissioning through Cisco UCS Manager GUI. This issue is resolved.	4.2(2b)	4.2(3b)

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCwd58327	HTTPD process consumes 100% CPU utilization while running monitoring and reporting tool. There are no cores generated. HA is functional but UCS Manager GUI login fails. This issue is resolved.	4.2(1m)	4.2(3b)

Resolved Caveats in Release 4.2(2e)

The following caveats are resolved in Release 4.2(2e):

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCwd41247	Multiple instances of hung **Samcproxy** is observed in a setup equipped with Cisco UCS 6400 FI. There may also be other miscellaneous faults on the domain related to **Samcproxy** being in a bad state. This issue is resolved.	4.2(1i)A	4.2(2e)A
CSCwe24011	Unexpected reboot is observed during normal operation in Cisco UCS 6536 FI and Cisco UCS 6400 FI series FIs. This issue is resolved.	4.2(2d)A	4.2(2e)A
CSCwe28336	MTS buffer stuck on `vsh.bin` process. The process crashes and impacts other functionality once the limit is reached. This issue is resolved.	4.2(2a)A	4.2(2e)A

Resolved Caveats in Release 4.2(2d)

The following caveats are resolved in Release 4.2(2d):

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCwc99962	Unable to form san-port-channel between UCS and Nexus 9000 switch in a setup equipped with 6200 series FI. This issue is resolved.	4.1(3h)A	4.2(2d)A
CSCvx79037	Cisco UCS Manager GUI displayed a Transceiver Mismatch alarm for both VIC 6400 Series Fabric Interconnects even though the interface was up. This issue is resolved.	4.1(3b)A	4.2(2d)A

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCwc55154	Infrastructure downgrade from release 4.2(2a)A or later to release 4.2(1n) or earlier fails when 100 GB port is configured or enabled. Following error is displayed 100G port is configured please unconfigure it to continue downgrade. This issue is resolved.	4.2(2c)A	4.2(2d)A
CSCwc56208	Cisco UCS Manager GUI shows DIMM inoperable error even though all DIMMS are available. This issue is resolved.	4.2(1l)A	4.2(2d)A
CSCvn71034	In a setup equipped with Cisco UCS 6400 FI series, SNMP traps were sent out for high value on a rcvDelta counter on Fabric Interconnect Ethernet uplinks, but no traps or counters are logged in the Cisco UCS Manager logs. This issue is resolved.	4.0(4b)A	4.2(2d)A

Resolved Caveats in Release 4.2(2c)

The following caveats are resolved in Release 4.2(2c):

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCwb88005	Under the following setup conditions, **AutoInstall** FSM is stuck at **WaitForDeploy** stage: • when FI-B is primary and FI-A is subordinate • setup was restored with full state backup file This issue is resolved.	4.2(2a)A	4.2(2c)A
CSCwb27664	In a setup equipped with Cisco 6454 Fabric Interconnect and 2408 IOM, Cisco UCS Manager reports frequent fan inoperable alerts.	4.0(4i)A	4.2(2c)A
CSCvt22099	In a setup equipped with Cisco UCS B200 M5 servers and 6248 FIs, the server discovery fails with the following FSM message even though the OS runs normally: `Unsupported adapter on the current UCS Firmware Version, therefore discovery of this system will not complete successfully.` This issue is resolved.	4.0(4e)A	4.2(2c)A

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCwc18223	In a set up equipped with Cisco UCS C240 M56 servers, one or more SED drives are marked as unconfigured good after a server reboot. This issue is resolved.	4.2(1f)C	4.2(2c)C
CSCwc62657	Cisco UCS B200 M6, C220 M6, and C240 M6 servers running BIOS versions 4.0.1h.0 or 4.0.1j.0 or 4.0.2d.0 display multiple uncorrectable errors after multiple Memory ECC errors and ADDDC/PCL event when PPR is completed on next reboot. This issue is resolved.	4.2(1m)A	4.2(2c)A
CSCwc53807	In Cisco UCS blade servers, DIMMs map out because of SPD memory corruption. This issue is resolved.	4.1(3j)b	4.2(2c)B
CSCwc60322	In Cisco UCS C240 M6 servers equipped with Cisco UCS VIC 1455 in slot 2, TAC support fails inclusion in overall C-Server tech-support. This issue is resolved.		4.2(2c)C
CSCwc60012	In Cisco UCS rack servers, DIMMs map out because of SPD memory corruption. This issue is resolved.	4.1(3j)b	4.2(2c)B
CSCvw73506	Failure of module 3 in a Cisco UCS 6296 Fabric Interconnect resulted in the ASIC error:`show hardware internal sunny counters interrupts all`. This issue is resolved.	4.0(4h)A	4.2(2c)A

Resolved Caveats in Release 4.2(2a)

The following caveats are resolved in Release 4.2(2a):

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCwb03425	SNMP reports incorrect fan module status. This issue is resolved.	4.1(2c)A	4.2(2a)A
CSCwb76862	SAN-Port-channel does not work with Nexus 9000. This issue is resolved.	4.2(1m)C	4.2(2a)C

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCwa58954	It is observed that in a setup equipped with 6400 Series FIs, you are unable to login to Cisco UCS Manager GUI or other issues like discovery or shallow discovery failure. This issue is resolved.	4.1(3e)A	4.2(2a)A
CSCwa66342	In a setup equipped with Cisco UCS B200 M5 servers running RHEL 7.9 version, experience IO issues to FC storage array due to underlying VIC issue. This issue is resolved.	4.1(3f)B	4.2(2a)B
CSCwb83355	When SCSI reservation is used by ESX cluster software to manage access to shared volumes, Cisco UCS VIC 14xx reports firmware/SCSI status as DATA_CNT_MISMATCH/RESERVATION_CONFLICT if the target does not set RESID bits for any IO that receives RESERVATION_CONFLICT status. ESX SCSI layer considers DATA_CNT_MISMATCH as a failure and ignores the RESERVATION_CONFLICT SCSI status. When too many reservation conflicts are received, it degrades the Virtual Machines performance. This issue is resolved.	4.1(3g)	4.2(2a)
CSCvt29521	Cisco UCS Manager raises two F0185 (DIMM Inoperable) faults DIMMs when only one DIMM is faulty. This issue is resolved.	4.1(1a)A	4.2(2a)A
CSCwb12460	In a setup equipped with 2400 series IOMs, logs show incorrect data about only IOM B reboot. Issue is seen with all the chassis after IOM B reboot during service profile association on server after DIMM replacement. This issue is resolved.	4.1(2b)A	4.2(2a)A
CSCwb71882	FI-6332-UP running 4.2(1g) firmware is unable to run **ethanalyzer** commands. This issue is resolved.	4.2(1g)A	4.2(2a)A
CSCwb86804	During infrastructure upgrade, **satctrl_log** cores got generated after IOM got updated and went into discovery mode. This issue is resolved.	4.2(2a)A	4.2(2a)A

Resolved Caveats in Release 4.2(1n)

The following caveats are resolved in Release 4.2(1n):

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCvz98195	If large numbers of LUNs are zoned to a Cisco UCS C-Series server, with Emulex HBA, integrated with Cisco UCS Manager using Cisco UCS 6200 FI, and if the HBA is not managed by Cisco UCS Manager, then it leads to discovery and re-acknowledgment failures. This issue is resolved.	4.1(3c)A	4.2(1n)A
CSCwb83355	When SCSI reservation is used by ESX cluster software to manage access to shared volumes, Cisco UCS VIC 14xx reports firmware/SCSI status as DATA_CNT_MISMATCH/RESERVATION_CONFLICT if the target does not set RESID bits for any IO that receives RESERVATION_CONFLICT status. ESX SCSI layer considers DATA_CNT_MISMATCH as a failure and ignores the RESERVATION_CONFLICT SCSI status. When too many reservation conflicts are received, it degrades the Virtual Machines performance. This issue is resolved.	4.1(3g)	4.2(1n)
CSCwb89732	In a setup with 6400 FIs, while accessing the KVM IP address, you are redirected to Cisco UCS Manager GUI. This issue is resolved.	4.1(3f)A	4.2(1n)A
CSCwc18223	In a set up equipped with Cisco UCS C240 M56 servers, one or more SED drives are marked as unconfigured good after a server reboot. This issue is resolved.	4.2(1f)C	4.2(1n)C

Resolved Caveats in Release 4.2(1m)

The following caveats are resolved in Release 4.2(1m):

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCwa57947	It is observed in Cisco UCS VIC 14xx series adapters that incoming LLDP/CDP packets are dropped. ESXi vmNIC does not report any details despite that the FI TX counters reports LLDP packets leaving the FIs. This issue is resolved.	4.1(1f)B	4.2(1m)B

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCwa84439	Cisco UCS 6400 FI experience a kernel panic after upgrading to release 4.2(1i). This issue is resolved.	4.2(1i)A	4.2(1m)A
CSCwa85389	Cisco UCS server connected to Cisco UCS 6454 FI reboots unexpectedly with a CFS core dump.. This issue is resolved.	4.2(1i)A	4.2(1m)A
CSCwa89200	Cisco UCS B200 M6 server freezes at **Waiting for BIOS POST Completion** screen while upgrading. This issue is resolved.	4.2(1l)B	4.2(1m)B
CSCwa90880	Both the Cisco UCS 6330 FIs reboot after upgrading to release 4.1(3f) due to LLDP Hap reset. This issue is resolved.	4.1(3f)A	4.2(1m)A
CSCwb19524	When the size of the bundle file is greater than 2GB, Cisco UCS Manager upgrade from few earlier releases to release 4.2(1l) fails with the following error message: `Unable to open downloaded image` This issue is resolved.	4.2(1l)A	4.2(1m)A
CSCwb21128	Under certain conditions, the hard drive may experience long latency times, leading to undesirable results while working with latency-sensitive applications. This issue may happen with small block size and sequential writes. This issue is resolved.	4.1(3c)C	4.2(1m)C
CSCwb34837	Cisco UCS B-Series servers take a long time to load Microsoft Windows 2016 and 2019 login screen due to FC remote volume map attempts. This issue is resolved.	4.1(3b)B	4.2(1m)B
CSCvv57606	Cisco UCS Manager fails to associate Service Profile for Cisco UCS servers connected to Cisco UCS 6400 FI through 2408 IOMs. Following error message is displayed: `Connection Placement Error` This issue is resolved.	4.0(4e)	4.2(1m)B

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCvz81322	In a system configured with VLAN groups and mapped with FI uplink interfaces, an unexpected outage was experienced when a VLAN is removed from a vNIC template or from a VLAN group. This issue has been resolved.	4.1(3c)A	4.2(1m)A
CSCwa47901	E2E diagnostics fails in Cisco UCS B200 M6 servers because PNUOS discovery fails. PNUOS does not boot and is stuck at grub boot menu screen. It neither times out nor boots with default PNUOS. This issue has been resolved.	4.2(1d)A	4.2(1m)A
CSCwa49820	Cisco UCS Manager access is lost due to configuration changes in Cisco UCS 6454 FI after upgrading the infrastructure firmware to release 4.2(1). This issue has been resolved.	4.2(1f)A	4.2(1m)A
CSCwa85667	BMC reset is observed on Cisco UCS C-Series and B-Series M5/M6 servers due to kernel crash and watchdog reset. This issue has been resolved.	4.0(4m)	4.2(1m)A
CSCwb02128	In a setup with Cisco UCS 6400 FIs, after upgrading the secondary FI to release 4.2(1i), the Communication Services FSM fails with the folloowing critical error: `Description : [FSM:FAILED]: communication service configuration(FSM:sam:dme:CommSvcEpUpdateSvcEp). Remote-Invocation-Error: UUID Not found Code : F999616` This issue has been resolved.	4.2(1l)	4.2(1m)A
CSCwb33900	In a setup with Cisco UCS 6400 FIs, SNMPd crashes with core to a stateful crash. This issue has been resolved.	4.1(3h)A	4.2(1m)A

Defect ID	Symptom	First Bundle Affected	Resolved in Release

CSCvy90515	Following fault is observed after upgrading Cisco UCS 6300 FI to release 4.1(3):
	`Severity: Minor`
	`Code: F2016 Description: Partition bootflash on fabric interconnect A|B is clean but with errors`
	This issue has been resolved.
		4.1(3c)A	4.2(1m)A

CSCvz49048	In a setup equipped with Cisco UCS 2408 IOMs, it is observed that the I2C errors increase and this turns on amber LEDs for fans. This issue has been resolved.	4.1(2b)A	4.2(1m)A
CSCvx37634	Cisco UCS B200 M5 server discovery fails with the following fault message: `Setup of Vmediafailed(sam:dme:ComputeBladeDiscover:SetupVm` This issue has been resolved.	4.1(1c)B	4.2(1m)
CSCwa61427	Cisco UCS 64108 FI LCAP services crash without causing any FI reboot or service outage. This issue has been resolved.	4.2(1i)A	4.2(1m)
CSCwa84899	In a setup equipped with Cisco UCS 6400 FI, uplink fiber ports go into disable state due to Unidirectional Link Detection (UDLD) even though UDLD policy is set as **disabled**. This issue has been resolved.	4.2(1d)A	4.2(1m)

Resolved Caveats in Release 4.2(1l) (Deprecated Release)

The following caveats are resolved in Release 4.2(1l):

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCvz45484	After the inventory of drives, the Front NVMe and the Rear NVMe slot id does not match with mechanical slot numbers. The slot ids for a NVMe drive are assigned based on the total number of drives supported by the server. This issue is resolved.	4.1(34a)A	4.2(1l)A

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCvz64536	A Cisco UCS M5 rack server failed discovery when all PCIe slots were populated. This issue is resolved.	4.1(3c)A	4.2(1l)A
CSCwa11621	On a Cisco UCS B-series blade server with VIC 6454 fabric interconnects, when vCenter port mirror is configured with a session type of "Encapsulated Remote Mirroring (L3) Source" the GRE traffic was disrupted. This issue is resolved.	4.1(2b)A	4.2(1l)A
CSCvz74423	A VIC 6400 series Fabric Interconnect running UCS Manager with NXOS crashed and rebooted. The system showed a reset reason: `Reset Reason (SW): Reset triggered due to HA policy of Reset (16) at time...` This issue is resolved.	4.2(1d)A	4.2(1l)A
CSCvx54145	When using the Chrome and Edge browsers, navigating through Firmware Management by clicking **Installed Firmware** > **Activate Firmware**, then clicking on the + sign did not open the list view. This issue is resolved.	4.2(0.138)A	4.2(1l)A
CSCvz72923	On UCS Managed blade servers with VIC 1300 Series Fabric Interconnects, intermittent connectivity loss occurred, followed by full connectivity loss. This issue is resolved.	4.1(3a)B	4.2(1l)B
CSCvn71034	SNMP traps were sent out for high value on a rcvDelta counter on Fabric Interconnect Ethernet uplinks, but no traps or counters were logged in the UCS Manager logs. This issue is resolved.	4.0(4b)A	4.2(1l)B
CSCwa45286	On a UCS-Managed system running NXOS9, the SAN port channel to a Cisco VIC 6400 Series Fabric Interconnect failed to link up. This issue is resolved.	4.2(1f)A	4.2(1l)A
CSCvx79037	The Cisco UCS Manager GUI displayed a Transceiver Mismatch alarm for both VIC 6400 Series Fabric Interconnects even though the interface was up. This issue is resolved.	4.1(3b)A	4.2(1l)A

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCvz95932	A Cisco UCS blade server with a VIC 6400 Series Fabric Interconnect was displaying a log message similar to the following: `2021 Sep 10 17:31:22 %$ VDC-1 %$ %CALLHOME-2-EVENT: SW_SYSTEM_INCONSISTENT` This issue is resolved.	4.2(1f)A	4.2(1l)A
CSCwa11069	A Cisco UCS-Managed blade server with a VIC 6454 Fabric Interconnect experienced a SNMPd failure and core dump. This issue is resolved.	4.2(1d)A	4.2(1l)A
CSCwa30221	On a Cisco UCS blade server running NXOS with VIC 6400 Series Fabric Interconnects, the 2204XP IOM did not receive a IP address during discovery: This issue is resolved.	4.1(3f)A	4.2(1l)A
CSCvz25713	On a Cisco UCS C245 M6 rack server, the UCS Manager BIOS tokens were not being applied after CMOS reset. This issue is resolved.	4.2(1.21)A	4.2(1l)A
CSCvz43359	On a Cisco UCS server using an NSX-T topology, data traffic using a GENEVE overlay sometimes left the wrong vNIC when GENEVE Offload was enabled on a VIC 1400 series Fabric Interconnect. This issue is resolved.	4.2(1d)C	4.2(1l)C

Resolved Caveats in Release 4.2(1i)

The following caveats are resolved in Release 4.2(1i):

Defect ID	Symptom	First Bundle Affected	Resolved in Release

CSCvz44891	During UCS Manager upgrade, on a Cisco UCS 5108 chassis, power appeared to be off and all blades became unreachable. The IOM obfl log displayed the messages:
	`OBFL:341:policy:No fans present and temperatures are high, shutting down pre-emptively`
	`2019-06-24T15:14:49.940216-07:00 CMC NOCSN_thermal-5-CMC OBFL:153:psu_shutdown:153 Successfully made psu 0 active`
	`2019-06-24T15:14:49.942860-07:00 CMC NOCSN_dmserver-6-CMC OBFL:2141:proc_req_set_ps_vs_latch_off:PSU0: Setting latch_off to: 1`
	`2019-06-24T15:14:49.958449-07:00 CMC NOCSN_thermal-5-CMC OBFL:164:psu_shutdown:164 Successfully shut down psu 0`
	`2019-06-24T15:14:49.971312-07:00 CMC NOCSN_thermal-5-CMC OBFL:153:psu_shutdown:153 Successfully made psu 1 active`
	This issue is resolved.
		4.1(2b)A	4.2(1i)A

CSCvy63500	After replacing a VIC 6200 series fabric interconnect on a UCS Managed server, the server was not discovered. The system displayed the message: `Port x/x on IOM is error-disabled. Slow-drain feature is enabled, if enabled, you can try selecting the 'Correct Slow-Drain congestions' option on the IOM` but no slow drain triggers were present in the syslog. This issue is resolved.	4.1(2b)A	4.2(1i)A
CSCvy72488	On a Cisco 6400 series fabric interconnect, an IOM FRU read failure caused user account decryption failure. This issue is resolved.	4.1(3c)	4.2(1i)

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCvy74106	On a UCS Managed blade server with a 6200 Series fabric interconnect the DME process could fail with a core dump after continuous authorized web logins with LDAP based remote user logins, This issue is resolved.	4.1(2b)A	4.2(1i)A
CSCvy91473	A 2304 NXOS IOM CPU could send frames to a down or unused 10G queue while HIF ports are in 40G mode. This issue is resolved.	4.1(1c)A	4.2(1i)
CSCvy94497	Intel 520 adapters in UCS Managed C-Series servers showed inconsistent firmware levels across multiple adapters in the same host, even if the the adapters were the same model. This issue is resolved.	3.2(3p)C	4.2(1i)C
CSCvz01679	When performing SNMP pollIng using OID on a blade server with 6400 series fabric interconnects, a FEX2 PSU2 offdenied was generated, though there was no issue found with the server chassis or fabric interconnects. This issue is resolved.	4.1(3b)A	4.2(1i)A
CSCvz21538	On a blade server with 2400 series fabric extender running NXOS, a fabric interconnect reboot with FI evacuation mode set to disable resulted in an 8 to 10 second delay in packet traffic. This issue is resolved.	4.1(3d)A	4.2(1i)A
CSCvz29291	Attempting to mount an ISO to a Cisco UCS C Series server using the Cisco APIs through HTTP or HTTPS resulted in a failure. The message: `Local Device Mount Failed` was displayed. This issue is resolved.	4.1(3b)A	4.2(1i)A
CSCvz34187	UCS Manager displayed incorrect PSU temp thresholds for PSU3 and 4. This issue is resolved.	4.1(3d)A	4.2(1i)A
CSCvz56406	A blade server with a 6454 Fabric Interconnect running UCS Manager was unable to upload internal backups through SFTP. This issue is resolved.	4.0(4k)A	4.2(1i)A

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCvz26396	A Cisco UCS blade server with VIC 1400 series adapter could abort or drop packets during the initial link-up period. This issue is resolved.	4.1(3b)A	4.2(1i)
CSCvz26417	On a Cisco UCS blade server with VIC 1400 series adapter, packet drops occurred during the first 2 seconds of link up between IOM and VIC adapter. This issue is resolved.	4.1(3b)A	4.2(1i)A
CSCvz50749	Changing the power state on a Cisco UCS C200 Series M6 server with non-expander attached storage controller could fail after decommission/recommission or CIMC reset. This issue is resolved.	4.2(1.15b)A	4.2(1i)A
CSCvy40579	The BIOS token settings in the service profile were reset to default values after disassociation.	4.2(0.019a)A	4.2(1i)A

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCvx93197	After hot-plug, the NVMe drives inventory data such as size and block, etc. was missing in the UCS Manager GUI and CLI. The server needed to be re-acknowledged to display the data. The following drives were affected: Intel: • SSDPE2ME800G4K • SSDPE2ME016T4K • SSDPE2MD400G4K • SSDPE2MD800G4KE Arbordale: • SSDPF2KX019T9K • SSDPF2KX038T9K • SSDPF2KX076T9K • SSDPF2KE016T9K • SSDPF2KE032T9K • SSDPF2KE064T9K WD SN840: • WUS4C6416DSP3X3 • WUS4C6432DSP3X3 • WUS4C6464DSP3X3 • WUS4BA176DSP3X3 • WUS4BA1A1DSP3X3 This issue is resolved.	4.2(0.189)A	4.2(1i)A
CSCvx18989	On a UCS-Managed B series blade server attached to a 64108 Fabric Interconnect, enabling ports from port 49 used a 100G license instead of a 10G license. This issue is resolved.	4.1(2b)	4.2(1i)

Resolved Caveats in Release 4.2(1f)

The following caveats are resolved in Release 4.2(1f):

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCvy80431	When a blade server was removed from a chassis and re-added, core file dumps were created in the BladeAG service, leading to a BladeAG service disruption and continuous restarts. This issue is resolved.	4.1(2b)A	4.2(1f)A
CSCvy81441	In rare situations, on UCS 6324 Fabric Interconnects, high availability was not ready in the peer Fabric Interconnect, resulting in a DME crash and core dump. This issue is resolved.	4.1(2b)A	4.2(1f)A
CSCvy69863	On Cisco UCS 6454 Fabric Interconnects, repeated remote logins (LDAP, Radius, etc) issued from a monitoring service several times per minute, resulted in a `samcproxy_proxy` process crash and a core dump. Faults related to Fabric Interconnect ports or user login could also occur. This issue is resolved.	4.1(3d)A	4.2(1f)A
CSCvy98914	Under certain conditions, Cisco UCS 6332 Fabric Interconnect experienced a DME crash and core dump while de-commissioning or re-commissioning the server. This issue is resolved.	4.1(2b)A	4.2(1f)A
CSCvy63500	A Cisco UCS 6296 Fabric Interconnect was disabled and the server was not discovered . The system suggested the **`Correct Slow-Drain congestions`** option on the IOM. Because the slow drain feature is supported only on UCS 6454 and 64108 Fabric Interconnects, the error message has been corrected to reflect this.	4.1(2b)A	4.2(1f)A
CSCvy64094	On downgrading from Cisco UCS Manager 4.2 to UCS Manager 4.1, core files were generated. This issue is resolved.	4.2.1A	4.2(1f)A
CSCvv75590	On a Cisco UCS M5 blade server with 256 GB LRDIMM or 512 GB DCPMM, the system failed to complete reboot after enabling Advanced Memory Test. This issue is resolved by applying BIOS 4.1.2.48 in this release.	4.1(2a)B	4.2(1f)B

Resolved Caveats in Release 4.2(1d)

The following caveats are resolved in Release 4.2(1d):

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCvf88524	Creating and storing kernel dump on any alternate drive (other than C drive) corrupts the OS even if the Challenge-Handshake Authentication Protocol (CHAP) is enabled in the boot policy and in iSCSI SAN. This issue is resolved.	3.1(3a)B	4.2(1d)B
CSCvv08931	On the Cisco UCS S3260 Storage Server, the Chassis profile association failed due to configuration issues such as `connection management-expander-inoperable` and `insufficient-resources`. This issue is resolved.	4.0(4h)A	4.2(1d)A
CSCvv71216	In the Cisco UCS server, whenever the FlexFlash controller is reset, the operating mode of the SD card is switched between 3.3 V signaling (during initialization) and 1.8 V signaling (for data transfers). This condition results in the disappearance of SD card to OS. Thereby, resulting in OS crash. This issue is resolved.	4.0(1d)	4.2(1d)

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCvw64456	The multiple Cisco UCS Virtual Interface Card 1400 series adapters reported error message as "hang_notify" followed with I/O halt. This condition triggered catastrophic error (CATERR) #0x03 and further resulted in server shutdown in a cluster. This issue is resolved.	4.0(4c)C	4.2(1d)C
CSCvx37120	When the BIOS policy is not used in the Service Profile of Cisco UCS M6 servers, the "$" sign may appear in CDN names for network interfaces in OS. This issue has no functional impact on ethernet interfaces. This issue is resolved.	4.2A	4.2(1d)A
CSCvh04298	The IOMs connected to an FI no longer reboot unexpectedly due to software-controlled resets. This issue is resolved.	3.1(3c) A	4.2(1d)A
CSCvt78954	Windows 2019 server OS installation fails on Cisco UCS C125 servers equipped with Cisco boot optimized m.2 RAID controller. This issue is resolved.	4.1(1e)	4.2(1d)

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCvv57606	On installing a M5 server in a chassis for the first time, a service profile may fail and throw the connection placement error. This issue is seen as the path is not being established for the adapter on Fabric Interconnect A and Fabric Interconnect B. Re-acknowledge IOM on path that is missing to re-establish connectivity and associate the service profile.	4.0(4e)A	4.2(1d)
CSCvw76521	On 6400 series Fabric Interconnect, if vHBA or vNIC is disabled when server is in shutdown state, vHBA or vNIC fails to come up when vHBA or vNIC is enabled after the server OS is booted up. This issue is resolved.	4.1(2)A	4.2(1d)

Open Caveats

The open bugs for a release are accessible through the Cisco Bug Search Tool. This web-based tool provides you with access to the Cisco bug tracking system, which maintains up-to-date information about bugs and vulnerabilities in this product and other Cisco hardware and software products.

Open Caveats for Release 4.2(3s)

There are no open caveats in release 4.2(3s).

Open Caveats for Release 4.2(3r)

There are no open caveats in release 4.2(3r).

Open Caveats for Release 4.2(3p)

There are no open caveats in release 4.2(3p).

Open Caveats for Release 4.2(3o)

The following caveats are open in release 4.2(3o).

Defect ID	Symptom	Workaround	First Bundle Affected
CSCwn65484	In a configuration equipped with Cisco UCS 6500 FI series, Cisco UCS Manager may report a warning indicating that a feature requiring the FCOE_NPV_PKG license is not installed. The warning message is: `%LICMGR-2-LOG_LIC_MISSING_WARNING: A feature that requires FCOE_NPV_PKG license is not installed. System supports honor based licensing so feature will continue to be fully functional.` Despite the FCoE feature being enabled by default, syslog on both FIs logs these warnings.	There is no known workaround.	4.3(3a)
CSCwn50433	After upgrading or downgrading server firmware to releases 4.1, 4.2, or 4.3, Cisco UCS Manager may incorrectly display the package release for the local disk. This discrepancy pertains to the mapping of the firmware release to the package release, as the firmware release itself remains accurate and fully functional.	The firmware version is correct and no action is required for functionality.	4.1(1a)

Open Caveats for Release 4.2(3n)

There are no open caveats in release 4.2(3n).

Open Caveats for Release 4.2(3m)

There are no open caveats in release 4.2(3m).

Open Caveats for Release 4.2(3l)

There are no open caveats in release 4.2(3l).

Open Caveats for Release 4.2(3k)

There are no open caveats in release 4.2(3k).

Open Caveats for Release 4.2(3j)

There are no open caveats in release 4.2(3j).

Open Caveats for Release 4.2(3i)

There are no open caveats in release 4.2(3i).

Open Caveats for Release 4.2(3h)

There are no open caveats in release 4.2(3h).

Open Caveats for Release 4.2(3g)

The following caveats are open in Release 4.2(3g):

Defect ID	Symptom	Workaround	First Bundle Affected
CSCwh28338	vMedia image mount fails during OS deployment on a server with OOB IP configuration. This issue happens because the IP NAT is on the secondary FI, while the CIMC is informed that it resides on primary FI.	Perform one of the following: 1. Decommission and recommission the server. OR 2. Restart blade-AG on both the FIs (Fabric Interconnect A and B)	4.2(3g)

Open Caveats for Release 4.2(3e)

There are no open caveats in release 4.2(3e).

Open Caveats for Release 4.2(3d)

The following caveats are open in Release 4.2(3d):

Defect ID	Symptom	Workaround	First Bundle Affected
CSCwe32091	When **LUNs Per Target** field is set to more than 1024 in FC adapter policy of vHBAs of Service Profile, the actual value deployed in FC vNIC is capped to 1024. This issue occurs because the firmware version on the VIC adapter is old and does not support more than 1024 value for **LUNs Per Target**.	There is no known workaround.	4.2(3d)
CSCwd82136	In a setup equipped with Cisco UCS 6400 series FI connected to Cisco UCS C-Series servers using Cisco VIC 1457/1455/1467, ports on the FI may go to error-disabled state with **errDisabledExcessportIn** reason after a link flap.	Flap the FI port connected to the Cisco UCS C-Series servers.	4.2(3b)A

Open Caveats for Release 4.2(3b)

The following caveats are open in Release 4.2(3b):

Defect ID	Symptom	Workaround	First Bundle Affected
CSCwd82597	Infrastructure downgrade fails due to missing image. This issue occurs under the following condition: If Q-in-Q feature is enabled while downgrading, it will block the downgrade process. When Q-in-Q feature is manually disabled, and downgraded is restarted, delete package script and auto-install scrip may start at the same time and auto-install may not find the correct image version to set boot path.	Contact Cisco TAC.	4.2(3b)
CSCwd71199	Cisco IMC VMedia mounts with out of band external IP addresses assigned to management interfaces do not work.	Move CIMC management connection to inband and back to out of band to help clear the stale entries.	4.2(3b)

Defect ID	Symptom	Workaround	First Bundle Affected
CSCwc85559	Currently, Cisco UCS Manager does not support a speed configuration of 40G for FCoE ports and sets the speed as **auto**. Therefore, with a 40G transceiver, FCoE uplink port and Port channel go into **Admin State down** state. Cisco UCS Manager is unable to match the speed configuration with the upstream switch speed of 40G.	Ensure that the speed is set as **Auto** and **Auto Negotiation** is set to **ON** on the upstream switch side.	4.2(3b)
CSCwc87968	Associated vLANs do not show up as enabled while removing them for a border port from **LAN Uplinks Manager** in Cisco UCS Manager UI option. As a result, you cannot remove vLAN from the border port. This issue happens only while using Cisco UCS Manager in Google Chrome browser.	Use any other supported web browser to access Cisco UCS Manager.	4.2(3b)
CSCwd82136	In a setup equipped with Cisco UCS 6400 series FI connected to Cisco UCS C-Series servers using Cisco VIC 1457/1455/1467, ports on the FI may go to error-disabled state with **errDisabledExcessportIn** reason after a link flap.	Flap the FI port connected to the Cisco UCS C-Series servers.	4.2(3b)
CSCwd80915	Cisco UCS 6300 series FI migration to Cisco UCS 6536 FI connected to UCS-IOM-2304 may take longer than expected (up to 90 minutes). This issue occurs when passive copper cables are used to connect to Cisco UCS 6536 FI on ports 1 to 8.	Connect the UCS-IOM-2304 to ports 9 to 36 on the Cisco UCS 6536 FI. Or, use AOC cables or fiber cables.	4.2(3b)

Defect ID	Symptom	Workaround	First Bundle Affected
CSCwd90187	In a setup equipped with Cisco UCS 6536 FI, port goes to **Link not connected** status when QSFP-100G-DR/FR-S is replaced with QSFP-100G-CUxM under the following conditions: • 100G interface • interface is configured with **FEC Auto** • interface was using QSFP-100G-FR, QSFP-100G-DR transceivers • interface now uses QSFP-100G-CUxM, where CUxM refers to CU1M, CU2M, and so on.	There are two workarounds for this issue: • Perform the following steps: 1. Insert an optic or AOC transceiver that do not have FEC capability. For example, QSFP-100G-SR or QSFP-100G-AOC3M on the interface. 2. Remove the transceiver in step 1. 3. Re-insert passive copper cable. OR • Reboot the FI.	4.2(3b)

Open Caveats for Release 4.2(2e)

There are no open caveats in release 4.2(2e).

Open Caveats for Release 4.2(2d)

There are no open caveats in release 4.2(2d).

Open Caveats for Release 4.2(2c)

There are no open caveats in release 4.2(2c).

Open Caveats for Release 4.2(2a)

The following caveats are open in Release 4.2(2a):

Defect ID	Symptom	Workaround	First Bundle Affected
CSCwb41346	In a setup equipped with Cisco UCS M5 servers and Cisco VIC 1385 cards, FcIfs creation XML query displays invalid PCI order error (0,1) for PCI order 2, and (0,2) for PCI order 3. This issue occurs only when you configure the PCI link as **0** for second default vNIC present for the Cisco VIC 1385.	Do not send PCI Link for the second adapter in the request. All other parameters given in the request for modification, will be modified successfully.	4.1(2f)
CSCwc13966	Cisco UCS B200 M5 servers reboot without user acknowledgment after applying new firmware policy.	No known workarounds. Server reboots and applies the new firmware.	4.1(2f)
CSCwb88005	Under the following setup conditions, **AutoInstall** FSM is stuck at **WaitForDeploy** stage: • hen FI-B is primary and FI-A is subordinate • setup was restored with full state backup file	Cluster lead to FI-A before triggering infrastructure upgrade.	4.2(2a)

Open Caveats for Release 4.2(1n)

The are no open caveats in Release 4.2(1n).

Open Caveats for Release 4.2(1m)

There are no open caveats in Release 4.2(1m):

Open Caveats for Release 4.2(1l)

The following caveats are open in Release 4.2(1l):

Defect ID	Symptom	Workaround	First Bundle Affected
CSCwb19524	When the size of the bundle file is greater than 2GB, Cisco UCS Manager upgrade from few earlier releases to release 4.2(1l) or later fails with the following error message: `Unable to open downloaded image`	If you experience this issue, follow one of the upgrade paths appropriate for your release: • If you are upgrading from any 4.2(1) release, then first upgrade to release 4.2(1i)A bundle. After that, activate and then upgrade to release 4.2(1l). • If you are upgrading from any 4.1(3) release, then first upgrade to release 4.1(3h)A bundle. After that, activate and then upgrade to release 4.2(1l). • If you are upgrading from any 4.0(4) release, then first upgrade to release 4.0(4n)A bundle. After that, activate and then upgrade to release 4.2(1l).	4.2(1l)A

Open Caveats for Release 4.2(1k)

The are no open caveats in Release 4.2(1k).

Open Caveats for Release 4.2(1i)

The following caveats are open in Release 4.2(1i):

Defect ID	Symptom	Workaround	First Bundle Affected
CSCvy52458	The system time on Cisco UCS Manager is not in synchronization with the NTP servers. This issue is seen when: • The NTP server configuration is present in Cisco UCS Manager but missing in the NXOS configuration. • The NTP server is configured with domain name.	Remove and re-add the NTP servers to Cisco UCS Manager. If the NTP server is connected to Cisco UCS Central, set Time Zone Management and Communication Services to **Local** and then remove and re-add the NTP servers.	4.0(4g)A
CSCvz25713	The BIOS token changes done in the BIOS policy are restored on resetting CMOS of server, though the BIOS policy with the updated BIOS token is associated to Service Profile of the server.	After resetting CMOS of server, apply the BIOS policy with the updated BIOS token again to the server.	4.2(1)A
CSCvz65401	While adding an embedded local disk on a Cisco UCS C245 M6 Server, UCS Manager shows the message: `Failure Reason: issue with boot order, possibly specified LUN/JBOD target not found or not in correct state or not a supported configuration.`	There is no known workaround.	4.2(1h)A and C

Open Caveats for Release 4.2(1f)

The are no open caveats in Release 4.2(1f).

Open Caveats for Release 4.2(1d)

The following caveats are open in Release 4.2(1d):

Defect ID	Symptom	Workaround	First Bundle Affected
CSCvy46079	After decommission or recommission of fabric extender, the connection between Fabric Interconnect and Cisco UCS C-series server with multiport adaptor through that fabric extender is not established.	Re-acknowledgement of the server will recover connection.	4.2(1d)A
CSCvy52309	In certain models of PM6 series SSDs running with FW 0102 and 4TB or bigger capacity models that uses 512Gb Flash memory, the firmware may detect LBA mismatch condition internally and stop the drive operation. SSD goes to the failure mode and does not recover by the drive power cycle.	This issue is fixed in FW 0103 by increasing the BiCS4 512Gb Cache Entry Table length from 10 to 11 bits. The FW 0103 will be released in the upcoming patches.	4.1(3c)C
CSCvy74293	During the upgrade of Cisco UCS Manager with Cisco UCS B200 M6 servers from release 4.1(4a)A to 4.2(1)A, the upgrade validation fails. This situation is faced only when a BIOS policy with CDN Control token is configured as **"Platform Default"** in UCS B200 M6 servers. The issue is hit as the default value of CDN Control for UCSB200 M6 servers is changed from **Disabled** to **Enabled** in the release 4.2(1)A.	Disable the CDN Control token in the BIOS policy before upgrading Cisco UCS Manager from release 4.1(4a)A to 4.2(1)A.	4.2(1)A

Defect ID	Symptom	Workaround	First Bundle Affected
CSCvu90175	On Cisco UCS 6400 Series Fabric Interconnects, when an Admin user is created with the same name as an SNMP v3 user, the Admin user is not able to login to Cisco UCS Manager.	Create an Admin user with a unique name.	4.1(2)A
CSCvv10194	Cisco IMC Web GUI is inaccessible when: • TLS 1.3 communication is enabled and TLS 1.2 communication is disabled in the web browser. • **Common Criteria mode** is enabled in Cisco IMC.	Enable TLS 1.2 communication in the web browser.	4.1(2)
CSCvv76888	When a Virtual Machine Queue (VMQ) policy with Number of VMQ = 10 and Interrupts = 10 is associated with a network interface and the enic6x64.sys driver is installed on that device, the installation fails. The interface shows up with a yellow bang on the device manager.	When a VMQ policy is created, ensure that there are at least 32 interrupts, even though the number of VMQs in the policy is lower. This will enable the driver to load and function correctly.	4.1(2)B
CSCvv87655	On Cisco UCS B-Series and C-Series servers, Ubuntu 18.04.4 and 20.04 cannot be installed on VROC volumes for Desktop and Live Server versions as they don't have new Kernel integrated with VMD/VROC drivers.	Get a legacy server version from Cannonical which has the latest Kernel supporting VMD/VROC driver for Ubuntu 18.04.4 and Ubuntu 20.04 install to work.	4.1(2)

Defect ID	Symptom	Workaround	First Bundle Affected
CSCvp31928	For Intel® Optane™ Data Center persistent memory modules in UCS-managed mode, after local security is configured on a server, it can be deleted. This will disable security.	Use host-based tools to configure persistent memory module security	4.0(4a)B and C
CSCvw58884	On applying Host Firmware Pack (HFP) of version 4.1(1d) from Cisco UCS Central, the multiple local-disk and storage-controller faults are reported on the UCS Manager Domains. These faults have occurred as the B-Series and C-Series bundles firmware package exists on the UCS Manager domain even after deleting the images post the service profile update.	Upload the same B-Series and C-Series bundles firmware package to the Cisco UCS Manager domain to clear the local-disk and storage-controller faults.	4.1(1c)A
CSCvx81384	During installation of Windows 2016 or Windows 2019 on Cisco UCS B200 M5 server, blue screen of death (BSoD) is observed. This condition is observed when the server is running with Cisco UCS VIC 14xx series and the IO Queue is set to 8 in the fibre channel adapter policy.	If this issue occurs, modify the the fibre channel adapter policy to set the IO Queue value to 1 (the default value).	4.0(2a)

Defect ID	Symptom	Workaround	First Bundle Affected
CSCvx88159	When a power grid policy is enabled, the maximum power limit for chassis is set as 5 KW. However, while creating a power group for chassis having M6 blades, the range of values shown for power group is 6400-8300W which is beyond the set limit for the power grid policy.	There is no known workaround.	4.2(1d)
CSCvx88769	In the scenario where Cisco UCS Manager is downgraded from 4.2 to 4.1 or any other previous release version but if the switch fails to downgrade to previous release and gets rebooted, that is, the switch remains at 4.2, the user will not be able to login as all the UCS management services will be down.	Power cycle the Fabric Interconnect. While the Fabric Interconnect is booting up, press **Ctrl + C** to get to the loader prompt, and then boot the Fabric Interconnect with the previous release version of the image. Contact TAC for any assistance with this issue.	4.2(1d)
CSCvy02823	Re-enabling of vHBA on sever side is taking 120 seconds after flapping, instead of 60 seconds.	There is no known workaround.	4.2(1d)
CSCvy53631	The NVME drive locate LED functionality is not working as expected in B200-M6 servers when VMD is enabled: only the Status LED is blinking Amber at 4Hz. Expected behavior: • Activity LED: blinking green 4Hz • Status LED: blinking amber 4Hz	There is no known workaround.	4.2(1d)B

Defect ID	Symptom	Workaround	First Bundle Affected
CSCvy80777	During upgrade of NVME mSwitch firmware for the following models through Host Firmware Pack (HFP), the incorrect firmware version is shown in the C-bundle: • UCSC-C240-M6SN-HDDEx1 • UCSC-C240-M6SN-HDDEx2 • UCSC-C240-M6SN-HDDEx3	Re-acknowledge the server to view the correct firmware version.	4.2(1)

Known Behavior and Limitations

Release 4.2(3s)

There are no known limitations in release 4.2(3s).

Release 4.2(3r)

There are no known limitations in release 4.2(3r).

Release 4.2(3p)

There are no known limitations in release 4.2(3p).

Release 4.2(3o)

There are no known limitations in release 4.2(3o).

Release 4.2(3n)

There are no known limitations in release 4.2(3n).

Release 4.2(3m)

There are no known limitations in release 4.2(3m).

Release 4.2(3l)

Defect ID	Symptom	Workaround	First Bundle Affected
CSCwq27350	After upgrading to release 4.3(5c), some UCS 5100 series chassis with B200-M5 servers may show high power budget allocations despite low average power consumption. This can cause chassis capacity alerts, especially when the chassis is configured as Grid. The issue leads to power budget unavailability faults and server discovery or association failures due to insufficient power availability.	Perform one of the following actions: • Change the blade power priority setting from **no-cap** to **cap**. OR • Change the PSU redundancy policy to N or N+1 to increase the available power for chassis allocation.	4.2(3l)

Release 4.2(3k)

There are no known limitations in release 4.2(3k).

Release 4.2(3j)

There are no known limitations in release 4.2(3j).

Release 4.2(3i)

There are no known limitations in release 4.2(3i).

Release 4.2(3h)

There are no known limitations in release 4.2(3h).

Release 4.2(3g)

There are no known limitations in release 4.2(3g).

Release 4.2(3e)

There are no known limitations in release 4.2(3e).

Release 4.2(3d)

- **CSCwe41248**—If **LUNs Per Target** is set to greater than 1024 with multiple paths running RHEL 8.7, the OS takes a long time to scan all the paths. Eventually, the scan fails and the OS boots to the emergency shell.

  Workaround—Reduce the number of **LUNs Per Target** (paths) to be scanned by the OS.

Release 4.2(3b)

- **CSCwd32544**—Cisco Nexus 2348UPQ connected to Cisco UCS 6500 FI series with 40G CU cable does not get discovered in Cisco UCS Manager after configuring the FI ports as server port.

  Workaround—Disable **Auto Negotiation** for the FI ports.

- **CSCwd48246**—Cisco UCS-IOM-2304 or UCS-IOM-2304V2 IOMs may get stuck at identity state when connected to Cisco UCS-FI-6332.

  Workaround—Perform one of the following:

  - Shut and no-shut fabric port
  - Reconfigure fabric port
  - Reset IOM

Release 4.2(2e)

There are no known limitations in release 4.2(2e).

Release 4.2(2d)

- **CSCwb01457**—Cisco UCS B200 M5 servers running releases 4.1 or 4.2 and booting from iPXE display **Parity Error**.

  Workaround—

  - Roll back to release 4.0(4g).

    OR

  - Disable PCIe RAS from BIOS policy.

Release 4.2(2c)

- **CSCwa97427**—Cisco UCS Manager release 4.0(4) and earlier have a limit on the size of an image that can be installed in BMC flash. This limit may cause a Cisco UCS B-Series M5 blade server to lose all management capabilities after upgrading from a Cisco UCS release 4.0(4m) or earlier to release 4.2(2c). To stop this issue from occurring, Cisco UCS Manager checks this condition and blocks the upgrade.

  Workaround—While upgrading any Cisco UCS M5 B-Series server from 4.0(4m) or an earlier release, perform a two-step upgrade.

  1. First upgrade the server to any 4.1 release. Cisco recommends latest 4.1(3) patch.
  2. Once the server is running the 4.1 release, upgrade to 4.2(2) release.

- **CSCwc99180**—Cisco UCS Manager may block an upgrade process when you try to upgrade B-bundle to release 4.2(2c) without first upgrading the infrastructure A-bundle to 4.2(2c).

  Workaround—Upgrade infrastructure A-bundle to 4.2(2c) first and then upgrade B-bundle.

Release 4.2(2a)

- **CSCwa36214**—If you downgrade an Intel® X710 card running version 1.826.0 using Cisco UCS Manager running version 4.2(2a), the adapter downgrades without any error, but the adapter does not get listed in the inventory in the next host reset operation and goes into the recovery mode. In another host reset, the adapter goes into unusable state.

  Workaround—If you wish to downgrade Intel® X710 card from version 1.826.0 to any lower version, it is recommended to perform outside from the Cisco UCS Manager scope to avoid damaging the card. For example, you can downgrade through HSU tool.

- **CSCvz71583** —Support of Precision Time Protocol (PTP) can be enabled only with one vNIC per Cisco UCS VIC 15428 adapter.

- **CSCwb64913**—In a setup equipped with Cisco UCS 6400 series FI, when a board controller or BIOS is in the process of activating for any Cisco UCS server, and if at the same time a vLAN configuration or any other non-distruptive change is taking place through a service profile association, then that server reboots even if user-ack for the maintenance policy is set.

  Workaround—Clear pending FlexFlash and board controller activation by resetting the FlexFlash controller:

  - **Equipment** > **Chassis** ***Number*** > **Servers** > **Server** ***Number*** > **Inventory** > **Storage** > **Reset FlexFlash Controller**

    OR

  - Clear the pending faults and activating state for the board controller and then apply the service profile association based non-distruptive change.

- **CSCvy34349**—In a setup equipped with Cisco B200 M6 servers and Cisco Boot Optimized M.2 RAID Controller, if VMD/Intel VROC is enabled, then BIOS may not display the RAID controller during POST.

  Workaround—Disable VMD/Intel VROC.

Release 4.2(1)

- Serial over LAN (SoL) configuration does not work on Cisco UCS M6 servers when serial port A is selected as console redirection in BIOS policy

  CSCvy05529—The Serial over LAN (SoL) policy set for Cisco UCS M6 platforms, does not work when serial port A is set as console redirection in the BIOS policy.

  Cisco UCS M6 platforms support only COM 0 for serial redirection. The serial redirection token has to be configured with COM 0 in the BIOS policy for the SoL configuration to work on M6 platforms.

- OCP Support for DWM on UCS Manager—Dual Wire Management (DWM) is not supported on Cisco UCS C225 M6 Server and Cisco UCS C245 M6 Server. Only Direct Attach and Single Wire Management are supported.

- CSCwe64267—Cisco UCS Manager does not support firmware upgrade for Intel® X710 card series if the infrastructure A bundle is in any 4.2(1) release and the server C bundle is in any 4.2(2) or later release.

  Workaround—Upgrade Cisco UCS Manager to 4.2(2) or higher release.

Related Documentation

For more information, you can access related documents from the following links:

- Release Bundle Contents for Cisco UCS Software
- Cisco UCS C-series Rack Server Integration Guides
- Cisco UCS C-series Software Release Notes
- Release Notes for Cisco Intersight Infrastructure Firmware

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2021 –2026 Cisco Systems, Inc. All rights reserved.