Release Notes for Cisco UCS Manager, Release 4.3

First Published: 2023-08-17

Last Modified: 2024-02-15

Cisco UCS Manager

Cisco UCS™ Manager, Release 4.3 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 4.3. This document also includes the following:

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

Revision History

Table 1: Release 4.3(3)

Release	Date	Description
4.3(3a)	March 08, 2024	Updated Cisco UCS NVMeoF Support Matrix for 3rd Party Storage Vendors, on page 26.
4.3(3a)	February 15, 2024	Created release notes for Cisco UCS Manager Release 4.3(3a).

Table 2: Release 4.3(2)

Release	Date	Description
4.3(2e)	January 23, 2024	Created release notes for Cisco UCS Manager Release 4.3(2e).
4.3(2c)	November 14, 2023	Created release notes for Cisco UCS Manager Release 4.3(2c).

Release	Date	Description
4.3(2b)	August 16, 2023	Created release notes for Cisco UCS Manager Release 4.3(2b).

Top Reasons to Move to Cisco UCS Manager Release 4.3

Release 4.3(3a)

Support for the following 5th Gen Intel® Xeon® Scalable Processors with Cisco X210c M7 servers:

- Intel® Xeon® Platinum 8558P Processor
- Intel® Xeon® Platinum 8562Y+ Processor
- Intel® Xeon® Platinum 8592+ Processor
- Intel® Xeon® Platinum 8568Y+ Processor
- Intel® Xeon® Platinum 8592V Processor
- Intel® Xeon® Platinum 8580 Processor
- Intel® Xeon® Gold 6542Y Processor
- Intel® Xeon® Gold 6544Y Processor
- Intel® Xeon® Gold 6530 Processor
- Intel® Xeon® Gold 6554S Processor
- Intel® Xeon® Gold 6548Y+ Processor
- Intel® Xeon® Gold 6526Y Processor
- Intel® Xeon® Gold 6534 Processor
- Intel® Xeon® Gold 6538Y+ Processor
- Intel® Xeon® Gold 6548N Processor

Support for the following 5th Gen Intel® Xeon® Scalable Processors with Cisco UCS C220 M7 and C240 M7 servers:

- Intel® Xeon® Platinum 8592V Processor
- Intel® Xeon® Platinum 8562Y+ Processor
- Intel® Xeon® Platinum 8568Y+ Processor
- Intel® Xeon® Platinum 8592+ Processor
- Intel® Xeon® Platinum 8558P Processor
- Intel® Xeon® Platinum 8580 Processor
- Intel® Xeon® Platinum 8558 Processor
- Intel® Xeon® Gold 6542Y Processor

- Intel® Xeon® Gold 6544Y Processor
- Intel® Xeon® Gold 6548Y+ Processor
- Intel® Xeon® Gold 6526Y Processor
- Intel® Xeon® Gold 6530 Processor
- Intel® Xeon® Gold 6534 Processor
- Intel® Xeon® Gold 6554S Processor
- Intel® Xeon® Gold 6538Y+ Processor
- Intel® Xeon® Gold 5515+ Processor
- Intel® Xeon® Gold 5520+ Processor
- Intel® Xeon® Gold 6548N Processor
- Intel® Xeon® Silver 4514Y Processor
- Intel® Xeon® Silver 4516Y+ Processor

Release 4.3(2c)

- Support for the following X-Series servers with Cisco UCSX-9508 Chassis:
  - Cisco UCS X410c M7 Compute Node
- Support for the following UCS VIC cards:
  - Cisco UCS VIC 15427 (Support with Secure Boot feature)
  - Cisco UCS VIC 15230 (Support with Secure Boot feature)
  - Cisco UCS VIC 15237 MLOM (Support with Secure Boot feature)

Release 4.3(2b)

- Support for the following rack servers:
  - Cisco UCS C240 M7 Server
  - Cisco UCS C220 M7 Server
- Support for Cisco UCSX-9508 Chassis
- Support for the following X-Series servers with Cisco UCSX-9508 Chassis:
  - Cisco UCS X210c M7 Compute Node
  - Cisco UCS X210c M6 Compute Node
- Support for the following Intelligent Fabric Modules with Cisco UCS X-Series Servers:
  - UCSX-I-9108-25G
  - UCSX-I-9108-100G

- Support for the following UCS VIC cards:
  - Cisco UCS VIC 15425(Support with Secure Boot feature)
  - Cisco UCS VIC 15235 (Support with Secure Boot feature)
  - Cisco UCS VIC 15231
  - Cisco UCS VIC 15420 (Support with Secure Boot feature)
  - Cisco UCS VIC 15422 (Support with Secure Boot feature)
  - Cisco UCS VIC 14425
  - Cisco UCS VIC 14825
- Support for Cisco UCS VIC Q-in-Q tunneling configuration. A Cisco UCS Manager based Q-in-Q (802.1Q-in-802.1Q) tunnel originating from Cisco UCS VIC allows to segregate the traffic in the Cisco UCS infrastructure, and helps to expand the VLAN space through the double-tagging of packets in hypervisor or non-hypervisor environments.

Supported Platforms and Release Compatibility Matrix

Supported Platforms in this Release

The following servers are supported in this release:

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

- Cisco UCS S3260 M5
- Cisco UCS C125 M5

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 3: 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
4.3(3)	4.3(3)	All M7, M6, and S3260 M5
	4.3(2)	All M7, M6, M5
4.3(2)	4.3(2)	All M7, M6, and M5
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

Cisco UCS Manager Release	C-Series Standalone Releases Included	C-Series Servers Supported by the C-Series Standalone Releases
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
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

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 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 4.3* provides detailed information about configuring the Intersight Device Connector.

Cisco UCS Central Integration

Cisco UCS Manager Release 4.3 can only be registered with Cisco UCS Central, Release 2.0(1o) 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.

Upgrade and Downgrade to Release 4.3(3)

1. You cannot downgrade any Cisco UCS C220 M7, C240 M7, and X210c server equipped with any 5th Gen Intel® Xeon® Scalable Processor listed in New Hardware in Release 4.3(3a), on page 14 to any release earlier than 4.3(3a).
2. If you are planing to install any 15000 series Cisco UCS VIC, first supported in any 4.3 release, then ensure that you first upgrade the servers to the minimum supported release and then install the adapters in the server.

   If you install the adapters into the server running an earlier release and then upgrade the servers to the supported release, the servers require A/C power cycle to recognize the adapters.

   For example, to install Cisco UCS VIC 15427 adapter, first upgrade to release 4.3(2c) or later and then install the adapter in the server.

3. If you are managing Cisco UCS X-Series chassis or Cisco UCS M7 servers after upgrading to any 4.3(3) release, then you must decommission the X-Series chassis and M7 servers before downgrading to any unsupported release.
4. Cisco UCS M4 servers are not supported by 4.3(2) and later releases. You must decommission Cisco UCS M4 servers before upgrading to release 4.3(3).
5. Once you upgrade to 4.3(3) or any later release and enable Netflow feature from Cisco UCS Manager GUI, then you cannot downgrade to any release earlier than 4.3(2). To downgrade to any release earlier than 4.3(2), you must first disable Netflow feature from Cisco UCS Manager GUI.
6. Once you upgrade Cisco UCS 6400 or 64108 FI to 4.3(3) or any later release and enable Q-in-Q feature from Cisco UCS Manager GUI, then you cannot downgrade to any release earlier than 4.3(2). To downgrade to any release earlier than 4.3(2), you must first disable Q-in-Q feature from Cisco UCS Manager GUI.
7. Once you upgrade to release 4.3(3) or later and enable **SMTP Authentication** under Call Home in Cisco UCS Manager GUI, then you cannot downgrade to any release earlier than 4.3(2). To downgrade to any release earlier than 4.3(2), you must first disable **SMTP Authentication** from Cisco UCS Manager GUI.
8. If you have installed any Cisco UCS VIC with secure boot feature, then you cannot downgrade to any release earlier than 4.3(2).
9. If Fibre Channel ports on UCS Fabric Interconnect are connected to non-Cisco products, ensure that these are operating as individual Fibre Channel links and not aggregated into a port channel. Fibre Channel port channels are not compatible with non-Cisco technology.

Infrastructure Upgrade and Downgrade to Release 4.3(2)

1. If you are planing to install any 15000 series Cisco UCS VIC, first supported in 4.3(2) release, then ensure that you first upgrade the servers to the supported release and then install the adapters in the server.

   If you install the adapters into the server running an earlier release and then upgrade the servers to the supported release, the servers require A/C power cycle to recognize the adapters.

   For example, to install Cisco UCS VIC 15427 adapter, first upgrade to release 4.3(2c) or later and then install the adapter in the server.
2. If you are managing Cisco UCS X-Series chassis or Cisco UCS M7 servers after upgrading to release 4.3(2), then you must decommission the X-Series chassis and M7 servers before downgrading.
3. Cisco UCS M4 servers are not supported by 4.3(2) and later releases. You must decommission Cisco UCS M4 servers before upgrading to release 4.3(2)
4. Once you upgrade to release 4.3(2) or later and enable Netflow feature from Cisco UCS Manager GUI, then you cannot downgrade to any previous release. To downgrade to any release earlier than 4.3(2), you must first disable Netflow feature from Cisco UCS Manager GUI.
5. Once you upgrade Cisco UCS 6400 or 64108 FI to release 4.3(2) 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 4.3(2), you must first disable Q-in-Q feature from Cisco UCS Manager GUI.
6. Once you upgrade to release 4.3(2) 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 4.3(2), you must first disable **SMTP Authentication** from Cisco UCS Manager GUI.
7. If you have installed any Cisco UCS VIC with secure boot feature, then you cannot dowgrade to any previous release.

8. If Fibre Channel ports on UCS Fabric Interconnect are connected to non-Cisco products, ensure that these are operating as individual Fibre Channel links and not aggregated into a port channel. Fibre Channel port channels are not compatible with non-Cisco technology.

Table 4: Upgrade Paths to Release 4.3(3)

Upgrade from Release	Recommended Upgrade Path
Upgrade from any 4.3(2) release	Direct upgrade to release 4.3(3).
Upgrade from any 4.2(2) or 4.2(3) release	Direct upgrade to release 4.3(3).
Upgrade from any 4.2(1) release	1. Upgrade from 4.2(1i) or later patch—Direct upgrade to release 4.3(3). 2. Upgrade from a patch earlier than 4.2(1i) — a. Upgrade to release 4.2(1i)A bundle and activate. **Note** Do not download release 4.3(3)A bundle before activating release 4.2(1i)A. b. Download and upgrade to release 4.3(3).
Upgrade from any 4.1(3) release	1. Upgrade from 4.1(3h) or later patch—Direct upgrade to release 4.3(3). 2. Upgrade from a patch earlier than 4.1(3h)— a. 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 4.3(3)A bundle before activating release 4.1(3h)A bundle or later infrastructure bundle in 4.1(3) release version.. b. Download and upgrade to release 4.3(3).

Upgrade from Release	Recommended Upgrade Path
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 4.3(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 4.3(3).
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 4.3(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 4.3(3).
Upgrade from any 4.0(4) 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 4.3(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 4.3(3).

Table 5: Upgrade Paths to Release 4.3(2)

Upgrade from Release	Recommended Upgrade Path
Upgrade from any 4.2(2) or 4.2(3) release	Direct upgrade to release 4.3(2).

Upgrade from Release	Recommended Upgrade Path
Upgrade from any 4.2(1) release	**1.** Upgrade from 4.2(1i) or later patch—Direct upgrade to release 4.3(2). **2.** Upgrade from a patch earlier than 4.2(1i) — **a.** Upgrade to release 4.2(1i)A bundle and activate. **Note** Do not download release 4.3(2)A bundle before activating release 4.2(1i)A. **b.** Download and upgrade to release 4.3(2).
Upgrade from any 4.1(3) release	**1.** Upgrade from 4.1(3h) or later patch—Direct upgrade to release 4.3(2). **2.** Upgrade from a patch earlier than 4.1(3h)— **a.** 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 4.3(2)A bundle before activating release 4.1(3h)A bundle or later infrastructure bundle in 4.1(3) release version.. **b.** Download and upgrade to release 4.3(2).
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 4.3(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 4.3(2).

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 4.3(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 4.3(2).
Upgrade from any 4.0(4) 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 4.3(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 4.3(2).

UCS Manager Health and Pre-Upgrade Check Tool

The UCS Manager Health and Pre-Upgrade Check Tool provides automated health and pre-upgrade checks that are designed to ensure your clusters are healthy before you upgrade. It is imperative that this healthcheck is not just performed, but that you take corrective action on any cluster that is found to be unhealthy. Correct all issues reported by the UCS Manager health check before continuing.

Default Open Ports

The following table lists the default open ports used in Cisco UCS Manager Release 4.3.

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

Port	Interface	Protocol	Traffic Type	Fabric Interconnect	Usage
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 4.3

Cisco UCS Manager, Release 4.3 is a unified software release for all supported UCS hardware platforms.

New Hardware Features

- New Hardware in Release 4.3(3a), on page 14
- New Hardware in Release 4.3(2e)—None
- New Hardware in Release 4.3(2c), on page 16
- New Hardware in Release 4.3(2b), on page 17

New Software Features

- New Software Feature in Release 4.3(3a)—None
- New Software Feature in Release 4.3(2e)—None
- New Software Feature in Release 4.3(2c)—None
- New Software Feature in Release 4.3(2b), on page 21

New Hardware in Release 4.3

New Hardware in Release 4.3(3a)

Support for 5th Gen Intel® Xeon® Scalable Processors

Support for the following 5th Gen Intel® Xeon® Scalable Processors with Cisco X210c M7 servers:

- Intel® Xeon® Platinum 8558P Processor
- Intel® Xeon® Platinum 8562Y+ Processor
- Intel® Xeon® Platinum 8592+ Processor
- Intel® Xeon® Platinum 8568Y+ Processor
- Intel® Xeon® Platinum 8592V Processor
- Intel® Xeon® Platinum 8580 Processor
- Intel® Xeon® Gold 6542Y Processor
- Intel® Xeon® Gold 6544Y Processor
- Intel® Xeon® Gold 6530 Processor
- Intel® Xeon® Gold 6554S Processor
- Intel® Xeon® Gold 6548Y+ Processor
- Intel® Xeon® Gold 6526Y Processor
- Intel® Xeon® Gold 6534 Processor
- Intel® Xeon® Gold 6538Y+ Processor
- Intel® Xeon® Gold 6548N Processor

Support for the following 5th Gen Intel® Xeon® Scalable Processors with Cisco UCS C220 M7 and C240 M7 servers:

- Intel® Xeon® Platinum 8592V Processor
- Intel® Xeon® Platinum 8562Y+ Processor
- Intel® Xeon® Platinum 8568Y+ Processor
- Intel® Xeon® Platinum 8592+ Processor
- Intel® Xeon® Platinum 8558P Processor
- Intel® Xeon® Platinum 8580 Processor
- Intel® Xeon® Platinum 8558 Processor
- Intel® Xeon® Gold 6542Y Processor
- Intel® Xeon® Gold 6544Y Processor
- Intel® Xeon® Gold 6548Y+ Processor

- Intel® Xeon® Gold 6526Y Processor
- Intel® Xeon® Gold 6530 Processor
- Intel® Xeon® Gold 6534 Processor
- Intel® Xeon® Gold 6554S Processor
- Intel® Xeon® Gold 6538Y+ Processor
- Intel® Xeon® Gold 5515+ Processor
- Intel® Xeon® Gold 5520+ Processor
- Intel® Xeon® Gold 6548N Processor
- Intel® Xeon® Silver 4514Y Processor
- Intel® Xeon® Silver 4516Y+ Processor

Support for 5600 DIMMs

Support for the following 5600 DIMMs with Cisco UCS X210c M7 servers:

- Samsung® 16GB 1Rx8 PC5-5600B-RD0-1010-XT (KR M321R2GA3PB0-CWMKH 2323)
- Samsung® 32GB 1Rx4 PC5-5600B-RC0-1010-XT (M321R4GA0PB0-CWM)
- Samsung® 64GB 2Rx4 PC5-5600B-RA0-1010-XT (KR M321R8GA0PB0-CWMCH 2326)
- Samsung® 96GB (M321RYGA0PB0-CWM)
- Hynix® 16GB 1Rx8 PC5-5600B-RD0-1010-XT (HMCG78AGBRA190N BB 307)
- Hynix® 32GB 1Rx4 PC5-5600B-RC0-1010-XT (HMCG84AGBRA190N BB 310)
- Hynix® 64GB 2Rx4 PC5-5600B-RA0-1010-XT (HMCG94AGBRA177N BB 327)
- Hynix® 96GB 96GB 2Rx4 PC5-5600B-RA0-1010-XT (HMCGM4MGBRB)
- Hynix® 128GB 2S2Rx4 PC5-5600B-RA0-1010-XT (HMCT04AGERA)

Support for the following 5600 DIMMs with Cisco UCS C240 M7 and C220 M7 servers:

- Hynix® 16GB 1Rx8 PC5-5600B-RD0-1010-XT (HMCG78AGBRA190N BB 307)
- Hynix® 32GB 1Rx4 PC5-5600B-RC0-1010-XT (HMCG84AGBRA190N BB 310)
- Hynix® 64GB 2Rx4 PC5-5600B-RA0-1010-XT (HMCG94AGBRA177N BB 327)
- Hynix® 96GB 96GB 2Rx4 PC5-5600B-RA0-1010-XT (HMCGM4MGBRB)
- Hynix® 128GB 2S2Rx4 PC5-5600B-RA0-1010-XT (HMCT04AGERA)
- Samsung® 16GB 1Rx8 PC5-5600B-RD0-1010-XT (KR M321R2GA3PB0-CWMKH 2323)
- Samsung® 32GB 1Rx4 PC5-5600B-RC0-1010-XT (M321R4GA0PB0-CWM)
- Samsung® 64GB 2Rx4 PC5-5600B-RA0-1010-XT (KR M321R8GA0PB0-CWMCH 2326)
- Micron® 96GB 2RX4 PC5-5600B-RA0-1010-XT (MTC40F204WS1RC56BB1 317)

Supported GPUs

Support for the following Intel® GPU cards with the CPUs listed here:

- Support for Intel® Data Center GPU Flex 170, FH-3/4L, 150W PCIe with Cisco UCS C240 M7 servers
- Support for Intel® Data Center GPU Flex 140, HHHL, 75W PCIe with Cisco UCS C220 M7 and C240 M7 servers

New Hardware in Release 4.3(2c)

Cisco UCS X410c M7 Compute Node

The Cisco UCS X410c M7 Compute Node is the first 4-socket 4th Gen Intel® Xeon® Scalable Processors computing device to integrate into the Cisco UCS X-Series Modular System. Up to four compute nodes or two compute nodes and two GPU nodes can reside in the 7-rack-unit (7RU) Cisco UCS X9508 Server Chassis, offering high performance and efficiency gains for a wide range of mission-critical enterprise applications, memory-intensive applications and bare-metal and virtualized workloads.

The Cisco UCS X410c M7 Compute Node provides these main features:

- CPU: Four 4th Gen Intel Xeon Scalable Processors with up to 60 cores per processor
- Memory: Up to 16TB of main memory with 64x 256 GB DDR5-4800 Memory DIMMs
- Storage: Up to six hot-pluggable solid-state drives (SSDs), or non-volatile memory express (NVMe) 2.5-inch drives with a choice of enterprise-class RAID or passthrough controllers, up to two M.2 SATA drives with optional hardware RAID
- mLOM virtual interface cards:
  - Cisco UCS VIC 15420 occupies the server's modular LAN on motherboard (mLOM) slot, enabling up to 50 Gbps of unified fabric connectivity to each of the chassis’s intelligent fabric modules (IFMs) for 100 Gbps connectivity per server.
  - Cisco UCS VIC 15231 occupies the server's modular LAN on motherboard (mLOM) slot, enabling up to 100 Gbps of unified fabric connectivity to each of the chassis’s intelligent fabric modules (IFMs) for 100 Gbps connectivity per server.
  - Cisco UCS VIC 15230 (with secure boot feature) occupies the server's modular LAN on motherboard (mLOM) slot, enabling up to 100 Gbps of unified fabric connectivity to each of the chassis’s intelligent fabric modules (IFMs) for 100 Gbps connectivity per server.
- Optional mezzanine card:
  - Cisco UCS 5th Gen VIC 15422 can occupy the server's mezzanine slot at the bottom rear of the chassis. This card's I/O connectors link to Cisco UCS X-Fabric technology. An included bridge card extends this VIC's 2x 50 Gbps of network connections through IFM connectors, bringing the total bandwidth to 100 Gbps per fabric (for a total of 200 Gbps per server).
  - Cisco UCS PCI Mezz card for Cisco UCS X-Fabric can occupy the server's mezzanine slot at the bottom rear of the chassis. This card's I/O connectors link to Cisco UCS X-Fabric modules and enable connectivity to the Cisco UCS X440p PCIe Node.
  - All VIC mezzanine cards also provide I/O connections from the X410c M7 compute node to the X440p PCIe node.

- Security: The server supports an optional trusted platform module (TPM). Additional features include a secure boot FPGA and ACT2 anti-counterfeit provisions.

Cisco UCS VIC Cards

Following Cisco UCS VIC Cards are supported from release 4.3(2c) onwards:

- Cisco UCS VIC 15427—The Cisco UCS VIC 15427 is a Quad Port CNA MLOM, 4 x 10/25/50G with Secure Boot for Cisco UCS C-Series M6 and M7 servers.
- Cisco UCS VIC 15230—The Cisco UCS VIC 15230 is a MLOM with Secure Boot for Cisco UCS X210c M6, X210c M7, and X410c M7 servers.
- Cisco UCS VIC 15237 MLOM—The Cisco UCS VIC 15237 MLOM is a MLOM, 2x40/100/200G with Secure Boot for Cisco UCS C-Series M6 and M7 servers.

New Hardware in Release 4.3(2b)

Cisco UCSX-9508 Chassis

The Cisco UCS® X-Series Modular System simplifies your data center, adapting to the unpredictable needs of modern applications while also providing for traditional scale-out and enterprise workloads. It reduces the number of server types to maintain, helping to improve operational efficiency and agility as it helps reduce complexity.

The Cisco UCS X-Series Modular System begins with the Cisco UCSX-9508 Chassis engineered to be adaptable and future ready. It is a standard, open system designed to deploy and automate faster in concert with a hybrid cloud environment.

With a midplane-free design, I/O connectivity for the X9508 chassis is accomplished with frontloading, vertically oriented compute nodes intersecting with horizontally oriented I/O connectivity modules in the rear of the chassis. A unified Ethernet fabric is supplied with the Cisco UCS 9108 Intelligent Fabric Modules. In the future, Cisco UCS X-Fabric Technology interconnects will supply other industry-standard protocols as standards emerge. Interconnections can be easily updated with new modules.

For more information, see Cisco UCS X9508 Chassis Data Sheet.

Cisco UCS X210c M7 Compute Node

The Cisco UCS X210c M7 Compute Node is the second generation of compute node to integrate into the Cisco UCS X-Series Modular System. It delivers performance, flexibility, and optimization for deployments in data centers, in the cloud, and at remote sites. This enterprise-class server offers market-leading performance, versatility, and density without compromise for workloads. Up to eight compute nodes can reside in the 7-rack-unit (7RU) Cisco UCSX-9508 Chassis, offering one of the highest densities of compute, I/O, and storage per rack unit in the industry.

The Cisco UCS X210c M7 Compute Node provides these main features:

- CPU: Up to 2x 4th Gen Intel® Xeon® Scalable Processors with up to 60 cores per processor and up to 2.625 MB Level 3 cache per core and up to 112.5 MB per CPU.
- Memory: Up to 8TB of main memory with 32x 256 GB DDR5-4800 DIMMs.
- Storage: Up to six hot-pluggable, solid-state drives (SSDs), or non-volatile memory express (NVMe) 2.5-inch drives with a choice of enterprise-class redundant array of independent disks (RAIDs) or passthrough controllers, up to two M.2 SATA and M.2 NVMe drives with optional hardware RAID.

- Optional front mezzanine GPU module: The Cisco UCS front mezzanine GPU module is a passive PCIe Gen 4.0 front mezzanine option with support for up to two U.2 NVMe drives and two HHHL GPUs.
- mLOM virtual interface cards:
  - Cisco UCS Virtual Interface Card (VIC) 15420 occupies the server's modular LAN on motherboard (mLOM) slot, enabling up to 50 Gbps of unified fabric connectivity to each of the chassis intelligent fabric modules (IFMs) for 100 Gbps connectivity per server.
  - ◦ Cisco UCS Virtual Interface Card (VIC) 15231 occupies the server's modular LAN on motherboard (mLOM) slot, enabling up to 100 Gbps of unified fabric connectivity to each of the chassis intelligent fabric modules (IFMs) for 100 Gbps connectivity per server.
- Optional mezzanine card:
  - Cisco UCS 5th Gen Virtual Interface Card (VIC) 15422 can occupy the server's mezzanine slot at the bottom rear of the chassis. This card's I/O connectors link to Cisco UCS X-Fabric technology. An included bridge card extends this VIC's 2x 50 Gbps of network connections through IFM connectors, bringing the total bandwidth to 100 Gbps per fabric (for a total of 200 Gbps per server).
  - Cisco UCS PCI Mezz card for X-Fabric can occupy the server's mezzanine slot at the bottom rear of the chassis. This card's I/O connectors link to Cisco UCS X-Fabric modules and enable connectivity to the Cisco UCS X440p PCIe Node.
  - All VIC mezzanine cards also provide I/O connections from the X210c M7 compute node to the X440p PCIe Node.
- Security: The server supports an optional trusted platform module (TPM). Additional features include a secure boot FPGA and ACT2 anti-counterfeit provisions.

Cisco UCS X210c M6 Compute Node

The Cisco UCS X210c M6 Compute Node is the first computing device to integrate into the Cisco UCS X-Series Modular System. Up to eight compute nodes can reside in the 7-Rack-Unit (7RU) Cisco UCS X9508 Chassis, offering one of the highest densities of compute, I/O, and storage per rack unit in the industry.

The Cisco UCS X210c M6 Compute Node provides these main features:

- CPU: Up to 2x 3rd Gen Intel® Xeon® Scalable Processors with up to 40 cores per processor and 1.5 MB Level 3 cache per core
- Memory: Up to 32x 256 GB DDR4-3200 DIMMs for up to 8 TB of main memory. Configuring up to 16x 512-GB Intel Optane™ persistent memory DIMMs can yield up to 12 TB of memory.
- Storage: Up to 6 hot-pluggable, solid-state drives (SSDs), or non-volatile memory express (NVMe) 2.5-inch drives with a choice of enterprise-class redundant array of independent disks (RAIDs) or pass-through controllers with four lanes each of PCIe Gen 4 connectivity and up to 2 M.2 SATA drives for flexible boot and local storage capabilities
- Optional front mezzanine GPU module: The Cisco UCS Front Mezzanine GPU module is a passive PCIe Gen 4 front mezzanine option with support for up to two U.2 NVMe drives and two GPUs.
- mLOM virtual interface cards:

- Cisco UCS Virtual Interface Card (VIC) 14425 occupies the server's modular LAN on motherboard (mLOM) slot, enabling up to 50 Gbps of unified fabric connectivity to each of the chassis intelligent fabric modules (IFMs) for 100 Gbps connectivity per server.
- Cisco UCS VIC 15231 occupies the server's modular LAN on motherboard (mLOM) slot, enabling up to 100 Gbps of unified fabric connectivity to each of the chassis intelligent fabric modules (IFMs) for 100 Gbps connectivity per server.
- Cisco UCS VIC 15420 occupies the server's modular LAN on motherboard (mLOM) slot, enabling up to 100 Gbps of unified fabric connectivity to each of the chassis intelligent fabric modules (IFMs) for 100 Gbps connectivity per server.

- Optional mezzanine card:
  - Cisco UCS VIC 14825 can occupy the server's mezzanine slot at the bottom rear of the chassis. This card's I/O connectors link to Cisco UCS X-Fabric technology. An included bridge card extends this VIC's 2x 50 Gbps of network connections through IFM connectors, bringing the total bandwidth to 100 Gbps per fabric (for a total of 200 Gbps per server).
  - Cisco UCS VIC 15422 X-Series mezz (UCSX-ME-V5Q50G) 4x25G can occupy the server's mezzanine slot at the bottom rear of the chassis. This card's I/O connectors link to Cisco UCS X-Fabric technology. An included bridge card extends this VIC's 2x 50 Gbps of network connections through IFM connectors, bringing the total bandwidth to 100 Gbps per fabric (for a total of 200 Gbps per server).
  - Cisco UCS PCI Mezz card for X-Fabric can occupy the server's mezzanine slot at the bottom rear of the chassis. This card's I/O connectors link to Cisco UCS X-Fabric modules and enable connectivity to the X440p PCIe Node.

- Security: The server supports an optional trusted platform module (TPM). Additional features include a secure boot FPGA and ACT2 anti-counterfeit provisions

Intelligent Fabric Module

The Intelligent Fabric Modules (IFMs) bring the unified fabric into the blade server enclosure, providing connectivity between the blade servers and the fabric interconnect, simplifying diagnostics, cabling, and management. Cisco UCS X-Series Servers support following IFMs:

- Cisco UCS 9108 25G IFMs (UCSX-I-9108-25G)
- Cisco UCS 9108 100G IFMs (UCSX-I-9108-100G)

Cisco UCS C240 M7 Server

The Cisco UCS C240 M7 Server is well-suited for a wide range of storage and I/O-intensive applications such as big data analytics, databases, collaboration, virtualization, consolidation, and high-performance computing in its two-socket, 2RU form factor. It incorporates the 4th Gen Intel® Xeon® Scalable Processors with up to 60 cores per socket.

In addition to the advanced features, the server is also equipped with the PCIe Gen 5.0 for high-speed I/O, a DDR5 memory bus, and expanded storage capabilities (up to 32 DDR5 DIMMs for up to 8 TB of capacity using 128 GB DIMMs (16 DIMMs per socket)) and delivers sigficant performance and efficiency gains that will improve your application performance.

You can deploy the Cisco UCS C-Series Rack Servers as standalone servers or as part of the Cisco Unified Computing System managed by Cisco Intersight or Intersight Managed Mode.

Cisco UCS C220 M7 Server

The Cisco UCS C220 M7 Server is a versatile general-purpose infrastructure and application server. This high-density, 1RU, 2-socket rack server delivers industry-leading performance and efficiency for a wide range of workloads, including virtualization, collaboration, and bare-metal applications. It incorporates the 4th Gen Intel® Xeon® Scalable Processors, with up to 52 cores per socket. With advanced features such as Intel Advanced Matrix Extensions (AMX), Data Streaming Accelerator (DSA), In-Memory Analytics Accelerator (IAA), and QuickAssist Technology (QAT), the server offers significant performance improvements.

In addition to the advanced features, the server is also equipped with the PCIe Gen 5.0 for high-speed I/O, a DDR5 memory bus, and expanded storage capabilities (up to 32 DDR5 DIMMs for up to 4 TB of capacity using 128 GB DIMMs (16 DIMMs per socket)).

You can deploy the Cisco UCS C-Series rack servers as standalone servers or as part of the Cisco Unified Computing System™ with the Cisco Intersight Infrastructure Service cloud-based management platform. These computing innovations help reduce Total Cost of Ownership (TCO) and increase their business agility. These improvements deliver significant performance and efficiency gains that improve your application performance.

Cisco UCS VIC Cards

Following Cisco UCS VIC Cards are supported from release 4.3(2) onwards:

- Cisco UCS VIC 15425—The Cisco UCS VIC 15425 is a quad-port small-form-factor pluggable (SFP+/SFP28/SFP56) PCIe card designed for Cisco UCS C-series M6/M7 rack servers. The card supports 10/25/50-Gbps Ethernet or FCoE. The card can present PCIe standards-compliant interfaces to the host, and these can be dynamically configured as either NICs or HBAs.
- Cisco UCS VIC 15235—The Cisco UCS VIC 15235 is a dual-port quad small-form-factor pluggable (QSFP/QSFP28/QSFP56) PCIe card designed for Cisco UCS C-series M6/M7 rack servers. The card supports 40/100/200-Gbps Ethernet or FCoE. The card can present PCIe standards-compliant interfaces to the host, and these can be dynamically configured as either NICs or HBAs.
- Cisco UCS VIC 15231—The Cisco UCS VIC 15231 is a 2x100-Gbps Ethernet/FCoE-capable modular LAN on motherboard (mLOM) designed exclusively for the Cisco UCS X210 Compute Node. The Cisco UCS VIC 15231 enables a policy-based, stateless, agile server infrastructure that can present to the host PCIe standards-compliant interfaces that can be dynamically configured as either NICs or HBAs.

  Cisco UCS VIC 15231 occupies the modular LAN on motherboard (mLOM) slot of the server, enabling up to 100 Gbps of unified fabric connectivity to each of the chassis intelligent fabric modules (IFMs) for 200 Gbps (2x 100G) connectivity per server.
- Cisco UCS VIC 15420—The Cisco UCS VIC 15420 is a 4x25-Gbps Ethernet/FCoE capable modular LAN On Motherboard (mLOM) designed exclusively for Cisco UCS X210c M6/M7 Compute Node. The Cisco UCS VIC 15420 enables a policy-based, stateless, agile server infrastructure that can present to the host PCIe standards-compliant interfaces that can be dynamically configured as either NICs or HBAs.

  Cisco UCS VIC 15420 card occupies the modular LAN on the motherboard (mLOM) slot of the server, enabling up to 50 Gbps of unified fabric connectivity to each of the chassis intelligent fabric modules (IFMs) for 100 Gbps connectivity per server.

- Cisco UCS VIC 15422—The Cisco UCS VIC 15422 is a 4x25-Gbps Ethernet/FCoE capable mezzanine card (mezz) designed exclusively for Cisco UCS X210c M6/M7 Compute Node. The card enables a policy-based, stateless, agile server infrastructure that can present PCIe standards-compliant interfaces to the host that can be dynamically configured as either NICs or HBAs.
- Cisco UCS VIC 14425—The Cisco UCS VIC 14425 is a 4x25-Gbps Ethernet/FCoE capable modular LAN On Motherboard (mLOM) designed exclusively for Cisco UCS X210c M6 Compute Node. The Cisco UCS VIC 14425 enables a policy-based, stateless, agile server infrastructure that can present to the host PCIe standards-compliant interfaces that can be dynamically configured as either NICs or HBAs.
- Cisco UCS VIC 14825—The Cisco UCS VIC 14825 is a 4x25-Gbps Ethernet/FCoE capable mezzanine card (mezz) designed exclusively for Cisco UCS X210c M6 Compute Node. Cisco UCS X The card enables a policy-based, stateless, agile server infrastructure that can present PCIe standards-compliant interfaces to the host that can be dynamically configured as either NICs or HBAs. The UCS VIC 14000 bridge connector is required with the mezz card to connect the UCS X-Series Blade Server to Intelligent Fabric Module UCSX-I-9108-25G.

Supported GPUs

Following table shows the new GPU support matrix:

GPU	Cisco UCS Blade Servers	Cisco UCS Rack Servers
NVIDIA H100-80 GPU	No	Yes
NVIDIA L40 GPU	No	Yes
NVIDIA L4 GPU	No	Yes
NVIDIA T4 GPU	Yes	No

Note The NVIDIA T4 GPU is supported on the front mezzanine GPU module and on the Cisco UCS X210c M6 Compute Node and Cisco UCS X210c M7 Compute Node only.

Other Peripherals

Support for Cisco UCSB-PSU-2500ACDV 2500 Watt Server AC Power Supply for Cisco UCS 5108 Chassis.

Cisco UCS Manager supports all the peripherals supported by Cisco UCS C240 M7 Server, Cisco UCS C220 M7 Server, Cisco UCS X210c M6 Compute Node, and Cisco UCS X210c M7 Compute Node. For complete list of supported peripherals for a server, see Cisco UCS C-Series Rack Servers Data Sheet and Spec Sheet and Cisco UCS X-Series Modular System Data Sheet and Spec Sheet.

New Software in Release 4.3

New Software Feature in Release 4.3(2b)

- Beginning with release 4.3(2b), Cisco UCS Manager introduces support for Secure Boot on the following Virtual Interface Cards (VIC) on Cisco UCS C-Series and X-Series servers:
  - Cisco UCS VIC 15420

- Cisco UCS VIC 15422
- Cisco UCS VIC 15235
- Cisco UCS VIC 15425

Secure Boot is a trustworthy technology that ensures the code running on Cisco hardware platforms is authentic, unmodified, and operational as intended. The Secure Boot uses a trust anchor module (TAm) in hardware to verify the bootloader code. It also protects the boot code in hardware and checks digitally signed images to verify that only genuine, unmodified code boots on a Cisco device.

- Added Windows NENIC Driver support to enable **Receive Side Scaling Version 2 (RSSv2)** for Cisco UCS VIC 15000 series adapters. When RSS is enabled on the VIC, multiple hardware receive queues can be configured on the Physical Function (PF). With RSSv2, the VIC adapters can now support up to 16 queues (4x). RSSv2 is supported on the following servers:
  - Cisco UCS B-Series and C-Series M6 servers
  - Cisco UCS C-Series and X-Series M7 servers
- Added support for NVMeOF using RDMA on Cisco UCS VIC 14000 series adapters.
- Support for Cisco UCS VIC Q-in-Q tunneling configuration. A Cisco UCS Manager based Q-in-Q (802.1Q-in-802.1Q) tunnel originating from Cisco UCS VIC allows to segregate the traffic in the Cisco UCS infrastructure, and helps to expand the VLAN space through the double-tagging of packets in hypervisor or non-hypervisor environments.
- Added support for migrating Cisco UCS 6400 Series Fabric Interconnect to Cisco UCS 6536 Fabric Interconnect:
  - Support for UCS-FI-6454 to UCS-FI-6536 migration
  - Support for UCS-FI-64108 to UCS-FI-6536 migration
  - Support for UCS-FI-6454 to UCS-FI-6536 migration with UCS Central
  - Support for UCS-FI-64108 to UCS-FI-6536 migration with UCS Central
- Cisco UCS Manager introduces Netflow Monitoring support for Cisco UCS 6400 and 6500 Series Fabric Interconnects.

  NetFlow monitoring includes both Host Receive and Transmit Direction Monitor. On Cisco UCS 6400 series and Cisco UCS 6536 Fabric Interconnects, NetFlow monitoring session applied to the Host Receive Direction Monitor will enable both transmit and receive monitoring, while NetFlow monitoring session applied to the Host transmit Direction Monitor is a NO-OP.
- Cisco UCS Manager introduces Policy Driven Chassis Group Cap for Cisco UCSX-9508 Chassis.
- SR-IOV support for ESXi on Cisco UCS VIC 15000 Series with Cisco UCS M6/M7 B-series, C-series and X-series servers and on Cisco UCS VIC 1400/14000 series for Cisco UCS M5/M6 B-series and C-series servers.
- QSFP - 100G SR 1.2 support with Cisco UCS VIC 1400 and 15000 Series.
- Cisco UCS Manager now supports soft check for IIS license.

  Cisco UCS X-Series Servers and Cisco M7 Servers require a valid Cisco Intersight license and a connection to Intersight to remain compliant. If Cisco UCS Manager 4.3(2) detects Cisco UCS X-Series or any M7

hardware, it checks to ensure that the domain is claimed with a Cisco Intersight instance (SaaS, Connected Virtual Appliance, or Private Virtual Appliance). If the domain is not claimed within Cisco Intersight (where the Cisco Intersight licenses are managed), Cisco UCS Manager displays a major fault to notify you of this requirement so that you can take necessary steps to move to a compliant deployment.

- Cisco UCS Manager also supports BMC Auto Upgrade functionality—If you migrate Cisco UCS X-Series Servers running Cisco IMC release lower than 4.3(2b) from IMM to Cisco UCS Manager managed mode, then Cisco UCS Manager auto upgrades Cisco IMC version to 4.3(2b).
- User Acknowledgment during Cisco UCS infra upgrade through Auto-Install is enhanced for better user experience:

```
Reboot Now

Are you sure you want to apply the changes immediately?
Acknowledging will cause a reboot of the Primary Fabric Interconnect.
Please make sure to validate (detailed info available in the Cisco UCS Manager
Firmware Management Guide) the below points to avoid unexpected network issues:

        • Dynamic vNIC (if any) are up and running
        • Ethernet/FIber channel date paths are operating as expected
        • No unexpected faults that may indicate a potential error, exist.

Click Yes to apply the pending changes.
```

Deprecated Hardware and Software in Cisco UCS Manager Release 4.3(2b)

- Beginning with Cisco UCS Manager Release 4.3(2b), all Cisco UCS M4 and older servers and their accessories are no longer supported on all platforms (6300 Series, and 6400 Series Fabric Interconnects).
- Beginning with Cisco UCS Manager Release 4.3(2b), Cisco UCS 6200 Series FI 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 6300, 6400 series and 6536 Fabric Interconnects:

Table 6: Mixed Cisco UCS Releases Supported on Cisco UCS 6300, 6400, 6536 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)	4.3(2)	4.3(3)
4.3(3)	—	—	—	—	—	—	—	—	—	6332, 6332-16UP, 6454, 64108, 6536	6332, 6332-16UP, 6454, 64108, 6536

	Infrastructure Versions (A Bundles)										
4.3(2)	—	—	—	—	—	—	—	—	—	6332, 6332-16UP, 6454, 64108, 6536	6332, 6332-16UP, 6454, 64108, 6536
4.2(3)	—	—	—	—	—	—	6200, 6332, 6332-16UP, 6454, 64108	6200, 6332, 6332-16UP, 6454, 64108	6200, 6332, 6332-16UP, 6454, 64108, 6536	6332, 6332-16UP, 6454, 64108, 6536	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	6332, 6332-16UP, 6454, 64108, 6536	6332, 6332-16UP, 6454, 64108, 6536
4.2(1)	—	—	—	—	—	—	6200, 6332, 6332-16UP, 6454, 64108	6200, 6332, 6332-16UP, 6454, 64108	6200, 6332, 6332-16UP, 6454, 64108	6332, 6332-16UP, 6454, 64108, 6536	6332, 6332-16UP, 6454, 64108, 6536
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	6332, 6332-16UP, 6454, 64108, 6536	6332, 6332-16UP, 6454, 64108, 6536
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	—	—
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 7: 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)	4.3(2)	4.3(3)
4.3(3)	—	—	—	—	—	—	—	—	—	6324	6324
4.3(2)	—	—	—	—	—	—	—	—	—	6324	6324
4.2(3)	—	—	—	—	—	—	6324	6324	6324	6324	6324
4.2(2)	—	—	—	—	—	—	6324	6324	6324	6324	6324
4.2(1)	—	—	—	—	—	—	6324	6324	6324	6324	6324
4.1(3)	—	—	—	6324	6324	6324	6324	6324	—	6324	6324
4.1(2)	—	—	—	6324	6324	6324	6324	6324	—	—	—
4.1(1)	—	—	—	6324	6324	6324	6324	6324	—	—	—
4.0(4)	6324	6324	6324	6324	6324	6324	—	—	—	—	—
4.0(2)	6324	6324	6324	6324	6324	6324	—	—	—	—	—
4.0(1)	6324	6324	6324	6324	6324	6324	—	—	—	—	—

The following table lists the mixed B, C bundles that are supported on all platforms with the 4.3(3)A bundle:

Table 8: Mixed B, C Bundles Supported on All Platforms with the 4.3(3)A Bundle

	Infrastructure Versions (A Bundles)			
Host FW Versions (B, C Bundles)	4.3(3)			
	6300	6324	6400	6500
	ucs-6300-k9-bundle-infra.4.3.3a.A.bin	ucs-mini-k9-bundle-infra.4.3.3a.A.bin	ucs-6400-k9-bundle-infra.4.3.3a.A.bin	ucs-6500-k9-bundle-infra.4.3.3a.A.bin:
4.3(3)	Yes	Yes	Yes	Yes
4.3(2)	Yes	Yes	Yes	Yes
4.2(3)	Yes	Yes	Yes	Yes
4.2(2)	Yes	Yes	Yes	Yes
4.2(1)	Yes	Yes	Yes	Yes
4.1(3)	Yes	Yes	Yes	Yes
4.1(2)	Yes	Yes	Yes	No
4.1(1)	Yes	Yes	Yes	No

	Infrastructure Versions (A Bundles)			
4.0(1), 4.0(4) (B, C Bundles)	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 9: 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 14000 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+. Refer https://hwu.netapp.com/ for latest Storage Array support details. A valid NetApp® account is required to access the compatibility information				
	NVMe-TCP	ONTAP 9.10 onwards	Cisco UCS 6400 Series Cisco UCS 6536	Cisco UCS 1400 Series Cisco UCS 14000 Series Cisco UCS 15000 Series	ESXi 7.0U3 +, ESXi 8.0 +, RHEL 9.0+, SLES 15SP3+
	Note Refer https://hwu.netapp.com/ for latest Storage Array support details. A valid NetApp® account is required to access the compatibility information				

Storage Vendor	Feature	Storage Array	Cisco UCS FI	Cisco UCS VIC	Operating System
Pure Storage, Inc.®	NVMe-FC	Purity//FA 6.1 onwards	Cisco UCS 6300 Series Cisco UCS 6400 Series Cisco UCS 6536	Cisco UCS 1300 Series Cisco UCS 1400 Series Cisco UCS 14000 Series Cisco UCS 15000 Series	ESXi 7.0U3 +, 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	Purity//FA 5.2 onwards	Cisco UCS 6300 Series Cisco UCS 6400 Series Cisco UCS 6536	Cisco UCS 1400 Series Cisco UCS 14000 Series Cisco UCS 15000 Series	RHEL 7.2 +, RHEL 8.0 +, RHEL 9.0+, SLES 15SP1 +
	NVMe-ROCEv2	Purity//FA 5.2 onwards	Cisco UCS 6400 Series Cisco UCS 6536	Cisco UCS 1400 Series Cisco UCS 14000 Series Cisco UCS 15000 Series	ESXi 7.0U3 and ESXI 8.0
	NVMe-TCP	Purity//FA 6.4.2 onwards	Cisco UCS 6300 Series Cisco UCS 6400 Series Cisco UCS 6536	Cisco UCS 1400 Series Cisco UCS 14000 Series Cisco UCS 15000 Series	ESXi 7.0U3 +, RHEL 9.0+ , SLES 15SP3 +

Storage Vendor	Feature	Storage Array	Cisco UCS FI	Cisco UCS VIC	Operating System
Dell Inc.®	NVMe-FC	PowerStore, PowerMax	Cisco UCS 6300 Series Cisco UCS 6400 Series Cisco UCS 6536	Cisco UCS 1400 Series Cisco UCS 14000 Series Cisco UCS 15000 Series	ESXi 7.0U3 +, RHEL 8.6 +, SLES 15SP3+
	NVMe-TCP	PowerStore	Cisco UCS 6300 Series Cisco UCS 6400 Series Cisco UCS 6536	Cisco UCS 1400 Series Cisco UCS 14000 Series Cisco UCS 15000 Series	ESXi 7.0U3 +, RHEL 9.0+ , SLES 15SP3 +
IBM® Information Technology	NVMe-FC	IBM FlashSystem 9500	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 15SP5+, UEK R6 U3+
		IBM FlashSystem 9200			
		IBM FlashSystem 9100			
		IBM FlashSystem 7300			
		IBM FlashSystem 7200			
		IBM FlashSystem 5200			
		IBM FlashSystem 5035			
		IBM FlashSystem 5015			

Note + under **OS Support** column refers to the newer release in that release train.

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, and 6332 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 10: Minimum Host Firmware Versions for Blade Servers

Servers	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 6324 Series FI UCS 6332, 6332-16UP FI UCS 6400 Series FI UCS 6536 Series FI
	UCS-IOM- 2204 UCS-IOM- 2208	UCS-IOM- 2304	UCS-IOM- 2304V2	UCS-IOM- 2204 UCS-IOM- 2208 UCS-IOM- 2408* UCSX-I-9108-25G	UCS-IOM- 2204 UCS-IOM- 2208 UCS-IOM- 2408* UCSX-I-9108-25G	UCS-IOM- 2304V1/V2 UCS-IOM- 2408 UCSX-I-9108-25G or UCSX-I-9108-100G	UCS-IOM-2204 UCS-IOM-2208 UCS-IOM-2408 UCS-IOM- 2304 UCS-IOM- 2304V2 UCSX-I-9108-25G or UCSX-I-9108-100G
	UCS-IOM-2408 support 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/UCS 6400 series FI. Cisco UCS M6 servers are not supported with 6200 series FI UCSX-I-9108-25G and UCSX-I-9108-100G are supported only with UCS X-Series Servers						
UCS X410c M7	—	—	—	4.3(2c)	4.3(2c)	4.3(2c)	4.3(3a) *
UCS X210c M7	—	—	—	4.3(2b)	4.3(2b)	4.3(2b)	4.3(3a)*

Servers	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 6324 Series FI UCS 6332, 6332-16UP FI UCS 6400 Series FI UCS 6536 Series FI
	UCS-IOM- 2204 UCS-IOM- 2208	UCS-IOM- 2304	UCS-IOM- 2304V2	UCS-IOM- 2204 UCS-IOM- 2208 UCS-IOM- 2408* UCSX-I-9108-25G	UCS-IOM- 2204 UCS-IOM- 2208 UCS-IOM- 2408* UCSX-I-9108-25G	UCS-IOM- 2304V1/V2 UCS-IOM- 2408 UCSX-I-9108-25G or UCSX-I-9108-100G	UCS-IOM-2204 UCS-IOM-2208 UCS-IOM-2408 UCS-IOM- 2304 UCS-IOM- 2304V2 UCSX-I-9108-25G or UCSX-I-9108-100G
	UCS-IOM-2408 support 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/UCS 6400 series FI. Cisco UCS M6 servers are not supported with 6200 series FI UCSX-I-9108-25G and UCSX-I-9108-100G are supported only with UCS X-Series Servers						
UCS X210c M6	—	—	—	4.3(2b)	4.3(2b)	4.3(2b)	4.3(3a)*
* Cisco UCS X-Series servers are supported only with Cisco UCS 6454, 64108, and 6536 FIs and are not supported with Cisco UCS 6324, UCS 6332, 6332-16UP FIs.							
B200 M6	4.2(1d)	4.2(1d)	4.2(1d)	4.2(1d)	4.2(1d)	4.2(3j)	4.3(3a)
B200 M5	3.2(1d)	3.2(1d)	4.0(4o)	4.0(1a)	4.1(1a)	4.2(3j)	4.3(3a)
B480 M5	3.2(2b)	3.2(2b)	4.0(4o)	4.0(1a)	4.1(1a)	4.2(3j)	4.3(3a)

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 11: Minimum Host Firmware Versions for Rack Servers

Servers	Minimum Software Version UCS 6332, 6332-16UP 2232 PP 2348	Minimum Software Version UCS 6454 2232 PP (10G) 2348 UPQ (10G) 93180YC-FX3 (25G server ports) 93180YC-FX3 (10G server ports)	Minimum Software Version UCS 64108 2232 PP (10G) 2348 UPQ (10G) 93180YC-FX3 (25G server ports) 93180YC-FX3 (10G server ports)	Minimum Software Version UCS 6536 93180YC-FX3 (25G server ports) 93180YC-FX3 (10G server ports) 2348 UPQ (10G server ports)	Suggested Software Version UCS 6332, 6332-16UP FI UCS 6400 Series FI UCS 6536
UCS C240 M7	—	4.3(2b)	4.3(2b)	4.3(2b)	4.3(3a)*
UCS C220 M7	—	4.3(2b)	4.3(2b)	4.3(2b)	4.3(3a)*
* Cisco UCS C-Series M7 Serves are supported only with Cisco UCS 6454, 64108, and 6536 FIs and are not supported with Cisco UCS UCS 6332, 6332-16UP FIs.					
C220 M6	4.2(1d)	4.2(1d)	4.2(1d)	4.2(3j)	4.3(3a)
C240 M6	4.2(1d)	4.2(1d)	4.2(1d)	4.2(3j)	4.3(3a)
C225 M6	4.2(1l)	4.2(1l)	4.2(1l)	4.2(3j)	4.3(3a)
C245 M6	4.2(1i)	4.2(1i)	4.2(1i)	4.2(3j)	4.3(3a)
C220 M5	3.2(1d)	4.0(1a)	4.1(1a)	4.2(3j)	4.3(3a)
C240 M5	3.2(1d)	4.0(1a)	4.1(1a)	4.2(3j)	4.3(3a)
C125 M5	4.0(1a)	4.0(1a)	4.1(1a)	4.2(3j)	4.3(3a)
S3260 M5	3.2(3a)	4.0(1a)	4.1(1a)	4.2(3j)	4.3(3a)
C480 M5 ML	4.0(2a)	4.0(2a)	4.1(1a)	4.2(3j)	4.3(3a)
C480 M5	3.2(2b)	4.0(1a)	4.1(1a)	4.2(3j)	4.3(3a)

Adapters

In the following table, the **Suggested Software Version** column does not provide FI, FEX/IOM, and adapter compatibility. Check the **Minimum Software Version** columns in the same table for compatibility information.

Table 12: Minimum Software Versions for Adapters

Adapters	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 6332, 6332-16UP FI UCS 6400 Series FI UCS 6500 Series FI
	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 (10/25G server ports) 2232 PP 2348 UPQ UCSX-I-9108-25G UCSX-I-9108-100G	UCS-IOM -2204 UCS-IOM -2208 UCS-IOM -2408* UCSX-I-9108-25G UCSX-I-9108-100G	UCS-IOM -2304 V1/V2 UCS-IOM -2408	93180YC -FX3 (10/25G server ports) 2348 UPQ (10G server ports) UCSX-I-9108-25G UCSX-I-9108-100G	UCS-IOM -2204 UCS-IOM -2208 UCS-IOM -2408* UCS-IOM- 2304 UCS-IOM- 2304V2
	Cisco UCS IOMs are applicable only for Cisco UCS B-Series Servers UCSX-I-9108-25G and UCSX-I-9108-100G are supported only with Cisco UCS X-Series Servers								
Cisco UCS VIC 15427	-	-	-	-	4.3(2c)	4.3(2c)	-	4.3(2c)	4.3(3a)
Cisco UCS VIC 15230	-	-	-	-	4.3(2c)	4.3(2c)	-	4.3(2c)	4.3(3a)
Cisco UCS VIC 15237 MLOM	-	-	-	-	4.3(2c)	4.3(2c)	-	4.3(2c)	4.3(3a)
UCSX-ML-V5D200G (Cisco UCS VIC 15231 Dual-port 100-G mLOM)	-	-	-	-	4.3(2b)	4.3(2b)	-	4.3(2b)	4.3(3a)
UCSX-ME-V5Q50G (Cisco UCS VIC 15422 Quad-port 25G mezzanine)	-	-	-	-	4.3(2b)	4.3(2b)	-	4.3(2b)	4.3(3a)
UCSX-ML-V5Q50G (Cisco UCS VIC 15420 Quad-port 25G mLOM)	-	-	-	-	4.3(2b)	4.3(2b)	-	4.3(2b)	4.3(3a)
UCSX-V4-Q25GML (Cisco UCS VIC 14425 Quad-port 25G mLOM)	-	-	-	-	4.3(2b)	4.3(2b)	-	4.3(2b)	4.3(3a)
UCSX-V4-Q25GME (Cisco VIC 14825 Quad-port 25G mezzanine)	-	-	-	-	4.3(2b)	4.3(2b)	-	4.3(2b)	4.3(3a)
UCSC-P-V5D200G (Cisco UCS VIC 15235 Dual-port 40/100/200-G PCIe\)	-	-	4.3(2b)	-	-	-	-	-	4.3(3a)
UCSC-P-V5Q50G (Cisco UCS VIC 15425 Quad-port 10/25/50-G PCIe	-	-	4.3(2b)	-	4.3(2b)	-	4.3(2b)	4.3(2b)	4.3(3a)
UCSC-M-V5Q50G (Cisco UCS VIC 15428 MLOM 4-port adapter)	-	-	4.2(1d)	-	4.2(1d)	-	-	4.2(3j)	4.3(3a)

Adapters	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 6332, 6332-16UP FI UCS 6400 Series FI UCS 6500 Series FI
	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 (10/25G server ports) 2232 PP 2348 UPQ UCSX-I-9108-25G UCSX-I-9108-100G	UCS-IOM -2204 UCS-IOM -2208 UCS-IOM -2408* UCSX-I-9108-25G UCSX-I-9108-100G	UCS-IOM -2304 V1/V2 UCS-IOM -2408	93180YC -FX3 (10/25G server ports) 2348 UPQ (10G server ports) UCSX-I-9108-25G UCSX-I-9108-100G	UCS-IOM -2204 UCS-IOM -2208 UCS-IOM -2408* UCS-IOM- 2304 UCS-IOM- 2304V2
	Cisco UCS IOMs are applicable only for Cisco UCS B-Series Servers UCSX-I-9108-25G and UCSX-I-9108-100G are supported only with Cisco UCS X-Series Servers								
UCSC-M-V5D200G (Cisco UCS VIC 15238 MLOM adapter) Direct Attached only	4.2(3j) Direct Attached only	4.2(3j) Direct Attached only	4.2(3j) Direct Attached only	-	-	-	4.2(3j) Direct Attached only (40/100G)	4.2(3j) Direct Attached only (40/100G)	4.3(3a)
UCSBMLV5Q 10G (Cisco VIC 15411)	4.2(1d)	4.2(1d)	-	4.2(1d)	-	4.2(1d)	4.2(3j)	-	4.3(3a)
UCSC-PCIE-C100 -04 (Cisco UCS VIC 1495)	4.0(2a) *	4.0(2a)	-	4.0(2a) *	-	4.0(2a) *	4.2(3j) Direct Attach only (40/100G)	4.2(3j) Direct Attach only (40/100G)	4.3(3a)
UCSC-MLOM-C100 -04 (Cisco UCS VIC 1497)	4.0(2a) *	4.0(2a) *	-	4.0(2a) *	-	4.0(2a) *	4.2(3j) Direct Attach only (40/100G)	4.2(3j) Direct Attach only (40/100G)	4.3(3a)
UCSB-MLOM- 40G-04 (UCS VIC 1440)	4.0(1a) *	4.0(1a) *	-	4.0(1a) *	-	4.1(1a) *	4.2(3j)	-	4.3(3a)
UCSCM- V25-04 (UCS VIC 1467)	-	-	4.2(1l)	-	4.2(1l)	-	-	4.2(3j)	4.3(3a)
UCSC-M-V100-04 (UCS VIC 1477)	4.2(1l)Direct Attached only			-	-	-	4.2(3j) Direct Attached only		4.3(3a)
UCSB-VIC- M84-4P (UCS VIC 1480)	4.0(1a) *	4.0(1a) *	-	4.0(1a) *	-	4.1(1a) *	4.2(3j)	-	4.3(3a)

Adapters	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 6332, 6332-16UP FI UCS 6400 Series FI UCS 6500 Series FI
	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 (10/25G server ports) 2232 PP 2348 UPQ ~~UCSX-I-9108-25G~~ ~~UCSX-I-9108-100G~~	UCS-IOM -2204 UCS-IOM -2208 UCS-IOM -2408* UCSX-I-9108-25G UCSX-I-9108-100G	UCS-IOM -2304 V1/V2 UCS-IOM -2408	93180YC -FX3 (10/25G server ports) 2348 UPQ (10G server ports) ~~UCSX-I-9108-25G~~ ~~UCSX-I-9108-100G~~	UCS-IOM -2204 UCS-IOM -2208 UCS-IOM -2408* UCS-IOM- 2304 UCS-IOM- 2304V2
	Cisco UCS IOMs are applicable only for Cisco UCS B-Series Servers UCSX-I-9108-25G and UCSX-I-9108-100G are supported only with Cisco UCS X-Series Servers								
UCSC-PCIE- C25Q-04 (UCS VIC 1455)	4.0(1a) *	4.0(1a) *	4.2(3j)	4.0(1a) *	4.2(3j)	4.1(1a) *	-	4.2(3j)	4.3(3a)
UCSC-MLOM- C25Q-04 (UCS VIC 1457)	4.0(1a) *	4.0(1a) *	4.2(3j)	4.0(1a) *	4.2(3j)	4.1(1a) *	-	4.2(3j)	4.3(3a)
UCSC-PCIE-C40Q -03 (UCS VIC 1385) UCSC-MLOM-C40Q -03 (UCS VIC 1387)	3.1(3a) *	3.1(3a) *	4.2(3j)	4.0(1a) *	4.2(3j)	4.1(1a) *	-	4.2(3j)	4.3(3a)
UCSB-MLOM- 40G-03 (UCS VIC 1340) UCSB-VIC- M83-8P (UCS VIC 1380)	3.1(3a) *	3.1(3a) *	-	4.0(1a) *	-	4.1(1a) *	4.2(3j)	-	4.3(3a)
UCSC-PCIE -BD16GF (Emulex LPe31002 Dual-Port 16G FC HBA)	3.2(3a) *	3.2(3a) *	-	4.0(1a) *	-	4.1(1a) *	-	-	4.3(3a)
UCSC-PCIE -ID40GF (Intel XL710 adapter)	3.2(3a) *	3.2(3a) *	-	4.0(1a) *	-	4.1(1a) *	-	-	4.3(3a)
UCSC-PCIE -IQ10GF (Intel X710-DA4 adapter)	3.2(3a) *	3.2(3a) *	-	4.0(1a) *	-	4.1(1a) *	-	-	4.3(3a)
UCSC-PCIE -ID10GF (Intel X710-DA2 adapter)	3.2(3a) *	3.2(3a) *	-	4.0(1a) *	-	4.1(1a) *	-	-	4.3(3a)

Adapters	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 6332, 6332-16UP FI UCS 6400 Series FI UCS 6500 Series FI
	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 (10/25G server ports) 2232 PP 2348 UPQ UCSX-I-9108-25G UCSX-I-9108-100G	UCS-IOM -2204 UCS-IOM -2208 UCS-IOM -2408* UCSX-I-9108-25G UCSX-I-9108-100G	UCS-IOM -2304 V1/V2 UCS-IOM -2408	93180YC -FX3 (10/25G server ports) 2348 UPQ (10G server ports) UCSX-I-9108-25G UCSX-I-9108-100G	UCS-IOM -2204 UCS-IOM -2208 UCS-IOM -2408* UCS-IOM- 2304 UCS-IOM- 2304V2
	Cisco UCS IOMs are applicable only for Cisco UCS B-Series Servers UCSX-I-9108-25G and UCSX-I-9108-100G are supported only with Cisco UCS X-Series Servers								
UCSC-PCIE -ID40GF: Intel XL710-QDA2 Dual port 40 Gigabit Ethernet PCIe adapter	3.2(3a) *	3.2(3a) *	-	4.0(1a) *	-	4.1(1a) *	-	-	4.3(3a)
UCSC-PCIE -ID25GF (Intel XXV710-DA2 Dual port 25 Gigabit Ethernet PCIe adapter)	3.2(3a) *	3.2(3a) *	-	4.0(1a) *	-	4.1(1a) *	-	-	4.3(3a)
UCSC-PCIE -ID10GC (Intel X550-T2 adapter)	3.2(3a) *	3.2(3a) *	-	4.0(1a) *	-	4.1(1a) *	-	-	4.3(3a)
N2XX-AIPCI01 (Intel X520 dual port adapter)	3.2(3a) *	3.2(3a) *	-	4.0(1a) *	-	4.1(1a) *	-	-	4.3(3a)
UCSC-PCIE-IRJ45: Intel Ethernet Server Adapter I350-T4	3.2(3a) *	3.2(3a) *	-	4.0(1a) *	-	4.1(1a) *	-	-	4.3(3a)
UCSC-MLOM-IRJ45: Intel Ethernet I350-mLOM 1 Gbps Network Controller	3.2(3a) *	3.2(3a) *	-	4.0(1a) *	-	4.1(1a) *	-	-	4.3(3a)
UCSC-PCIE -ID25GF (Intel X710 25Gb Dual-port BaseT)	3.2(3a) *	3.2(3a) *	-	4.0(1a) *	-	4.1(1a) *	-	-	4.3(3a)
UCSC-PCIE -IQ10GC (Intel X710-T4)	3.2(2b) *	3.2(2b) *	-	4.0(1a) *	-	4.1(1a) *	-	-	4.3(3a)
UCSC-PCIE -QD16GF (QLogic QLE2692-CSC)	3.2(1d) *	3.2(1d) *	-	4.0(1a) *	-	4.1(1a) *	-	-	4.3(3a)

Adapters	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 6332, 6332-16UP FI UCS 6400 Series FI UCS 6500 Series FI
	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 (10/25G server ports) 2232 PP 2348 UPQ ~~UCSX-I-9108-25G~~ ~~UCSX-I-9108-100G~~	UCS-IOM -2204 UCS-IOM -2208 UCS-IOM -2408* UCSX-I-9108-25G UCSX-I-9108-100G	UCS-IOM -2304 V1/V2 UCS-IOM -2408	93180YC -FX3 (10/25G server ports) 2348 UPQ (10G server ports) ~~UCSX-I-9108-25G~~ ~~UCSX-I-9108-100G~~	UCS-IOM -2204 UCS-IOM -2208 UCS-IOM -2408* UCS-IOM- 2304 UCS-IOM- 2304V2
	Cisco UCS IOMs are applicable only for Cisco UCS B-Series Servers UCSX-I-9108-25G and UCSX-I-9108-100G are supported only with Cisco UCS X-Series Servers								
UCSC-PCIE -IQ10GF (Intel X710-DA4 adapter) UCSC-PCIE -ID40GF (Intel XL710 adapter)	—	3.1(3a) *	-	4.0(1a) *	-	4.1(1a) *	-	-	4.3(3a)
UCSC-PCIE -BD32GF (Emulex LPe32002) UCSC-PCIE -BS32GF (Emulex LPe32000)	3.1(3a) *	3.1(3a) *	-	4.0(1a) *	-	4.1(1a) *	-	-	4.3(3a)
UCSC-PCIE -E16002 (Emulex LPe16002-M6 16G FC rack HBA)	3.2(1d) *	3.2(1d) *	-	4.0(1a) *	-	4.1(1a) *	-	-	4.3(3a)
UCSC-PCIE -ID10GC (Intel X550 Dual-port 10GBase-T NIC)	3.1(3a) *	3.1(3a) *	-	4.0(1a) *	-	4.1(1a) *	-	-	4.3(3a)
UCSC-O -ID25GF (Intel XXV710 - DA2 - OCP1 2x25/10GbE OCP 2.0 adapter)	4.0(1a) *	4.0(1a) *	-	4.0(1a) *	-	4.0(1a) *	-	-	4.3(3a)
UCSC-P -Q6D32GF (Cisco-QLogic QLE2772 2x32GFC Gen 6 Enhanced PCIe HBA)	4.2(1l)	4.2(1l)	-	4.2(1l)	-	4.2(1l)	-	-	4.3(3a)
UCSC-P -B7D32GF (Cisco-Emulex LPe35002-M2-2x32GFC Gen 7 PCIe HBA)	4.2(1l)	4.2(1l)	-	4.2(1l)	-	4.2(1l)	-	-	4.3(3a)

Adapters	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 6332, 6332-16UP FI UCS 6400 Series FI UCS 6500 Series FI
	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 (10/25G server ports) 2232 PP 2348 UPC UCSX-I-9108-25G UCSX-I-9108-100G	UCS-IOM -2204 UCS-IOM -2208 UCS-IOM -2408* UCSX-I-9108-25G UCSX-I-9108-100G	UCS-IOM -2304 V1/V2 UCS-IOM -2408	93180YC -FX3 (10/25G server ports) 2348 UPC (10G server ports) UCSX-I-9108-25G UCSX-I-9108-100G	UCS-IOM -2204 UCS-IOM -2208 UCS-IOM -2408* UCS-IOM- 2304 UCS-IOM- 2304V2
	Cisco UCS IOMs are applicable only for Cisco UCS B-Series Servers UCSX-I-9108-25G and UCSX-I-9108-100G are supported only with Cisco UCS X-Series Servers								
UCSC-P -I8D100GF(Cisco - Intel E810CQDA2 2x100 GbE QSFP28 PCIe NIC)	4.2(1l)	4.2(1l)	-	4.2(1l)	-	4.2(1l)	-	-	4.3(3a)
UCSC-P -I8Q25GF (Cisco - Intel E810XXVDA4 4x25/10 GbE SFP28 PCIe NIC)	4.2(1l)	4.2(1l)	-	4.2(1l)	-	4.2(1l)	-	-	4.3(3a)
UCSC-P -I8D25GF (Cisco - Intel E810XXVDA2 2x25/10 GbE SFP PCIe NIC)	4.2(1l)	4.2(1l)	-	4.2(1l)	-	4.2(1l)	-	-	4.3(3a)
UCSC-P -ID10GC (Cisco - Intel X710T2LG 2x10 GbE RJ45 PCIe NIC)	4.2(1l)	4.2(1l)	-	4.2(1l)	-	4.2(1l)	-	-	4.3(3a)
UCSC-O -ID10GC: Cisco(R) X710T2LG 2x10 GbE RJ45 OCP 3.0 NIC	4.2(1d)	4.2(1d)	4.2(1d)	4.2(1d)	4.2(1d)	4.2(1d)	4.2(1d)	4.2(1d)	4.3(3a)
UCSC-P -IQ1GC: Intel I710-T4L 4x1GBASE-T NIC	Cisco UCS Manager does not support UCSC-P -IQ1GC: Intel I710-T4L 4x1GBASE-T NIC card even if the server supports this card.								
UCSB-RAID12G-M6: Cisco FlexStorage 12G SAS RAID Controller	4.2(1d)	4.2(1d)	4.2(1d)	4.2(1d)	4.2(1d)	4.2(1d)	4.2(1d)	4.2(1d)	4.3(3a)
UCSC-SAS-M6T: Cisco M6 12G SAS HBA for (16 Drives)	4.2(1d)	4.2(1d)	4.2(1d)	4.2(1d)	4.2(1d)	4.2(1d)	4.2(1d)	4.2(1d)	4.3(3a)

Adapters	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 6332, 6332-16UP FI UCS 6400 Series FI UCS 6500 Series FI
	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 (10/25G server ports) 2232 PP 2348 UPQ UCSX-I-9108-25G UCSX-I-9108-100G	UCS-IOM -2204 UCS-IOM -2208 UCS-IOM -2408* UCSX-I-9108-25G UCSX-I-9108-100G	UCS-IOM -2304 V1/V2 UCS-IOM -2408	93180YC -FX3 (10/25G server ports) 2348 UPQ (10G server ports) UCSX-I-9108-25G UCSX-I-9108-100G	UCS-IOM -2204 UCS-IOM -2208 UCS-IOM -2408* UCS-IOM- 2304 UCS-IOM- 2304V2
	Cisco UCS IOMs are applicable only for Cisco UCS B-Series Servers UCSX-I-9108-25G and UCSX-I-9108-100G are supported only with Cisco UCS X-Series Servers								
UCSX-X10C-RAIDF: UCS X10c Compute RAID Controller	-	-	-	-	-	-	-	-	4.3(3a)
Cisco Mini Storage Carrier for M.2 SATA-SWRAID Mode	4.2(1d)	4.2(1d)	4.2(1d)	4.2(1d)	4.2(1d)	4.2(1d)	4.2(1d)	4.2(1d)	4.3(3a)

Note Cisco UCS Manager Infrastructure A Bundle only supports adapters running release 4.1(3) or later.

Cisco UCS Fabric Interconnect Server Compatibility Matrix - Release 4.3(3a)

Cisco UCS 6536 FI

Table 13: Cisco UCS 6536 FI - Cisco UCS Rack Servers

Cisco VIC	Direct Attach (40/100G)	Direct Attach (4x25G or 25G QSA28)	FEX		
			93180YC-FX3 (25G server ports)	93180YC-FX3 (10G server ports)	2348 UPQ (10G server ports)
15427 (UCSC-M-V5Q50GV2)	Not Supported	All Cisco UCS C-Series M6 and M7 servers **Note** Reverse breakout is not supported.	All Cisco UCS C-Series M6 and M7 servers	SFP-10G-SR/SR-S only	All Cisco UCS C-Series M6 and M7 servers
15237 (UCSC-M-V5D200GV2)	All Cisco UCS C-Series M6 and M7 servers	Not Supported	Not Supported	Not Supported	Not Supported

Cisco VIC	Direct Attach (40/100G)	Direct Attach (4x25G or 25G QSA28)	FEX		
			93180YC-FX3 (25G server ports)	93180YC-FX3 (10G server ports)	2348 UPQ (10G server ports)
15235 (UCSC-P-V5D200G)	All Cisco UCS C-Series M6 and M7 servers	Not Supported	Not Supported	Not Supported	Not Supported
15238 (UCSC-M-V5D200G)	All Cisco UCS C-Series M6 and M7 servers	Not Supported	Not Supported	Not Supported	Not Supported
15425 (UCSC-P-V5Q50G)	Not Supported	All Cisco UCS C-Series M6 and M7 servers **Note** No reverse breakout supported	All Cisco UCS C-Series M6 and M7 servers	SFP-10G-SR/SR-S only	All Cisco UCS C-Series M6 and M7 servers
15428 (UCSC-M-V5Q50G)	Not Supported	All Cisco UCS C-Series M6 and M7 servers **Note** No reverse breakout supported	All Cisco UCS C-Series M6 and M7 servers	SFP-10G-SR/SR-S only	All Cisco UCS C-Series M6 and M7 servers
1497-40G/100G (UCSC-MLOMC100-04)	All Cisco UCS C-series M5 servers	Not Supported	Not Supported	Not Supported	Not Supported
1495-40G/100G (UCSC-PCIEC100-04)	All Cisco UCS C-Series M6, C-Series M5, and S-series M5 servers	Not Supported	Not Supported	Not Supported	Not Supported
1477-40G/100G (UCSC-MV100-04)	All Cisco UCS C-series M6 servers	Not Supported	Not Supported	Not Supported	Not Supported
1467-10G/25G (UCSC-MV25-04)	Not Supported	All Cisco UCS C-Series M6 servers	All Cisco UCS C-Series M6 servers	SFP-10G-SR/SR-S only	All Cisco UCS C-Series M6 servers
1457-10G/25G (UCSC-MLOMC25Q-04)	Not Supported	Cisco UCS C220 M5 and C240 M5	Cisco UCS C220 M5 and C240 M5	SFP-10G-SR/SR-S only	Cisco UCS C220 M5 and C240 M5
1455-10G/25G (UCSC-PCIEC25Q-04)	Not Supported	All Cisco UCS C-Series M5 and M6 servers and S-series M5 servers	All Cisco UCS C-Series M5 and M6 servers and S-series M5 servers	SFP-10G-SR/SR-S only	All Cisco UCS C-Series M5 and M6 servers and S-series M5 servers
1387 - 40G (UCSC-MLOM-C40Q-03)	All Cisco UCS C-Series M5 Servers (40G)	Not Supported	Not Supported	With QSA and SFP-10G-SR only	All Cisco UCS C-Series M5 servers (QSA at adapter)
1385 - 40G (UCSC-PCIE-C40Q-03)	All Cisco UCS C-Series M5 Servers (40G)	Not Supported	Not Supported	With QSA and SFP-10G-SR only	All Cisco UCS C-Series M5 servers (QSA at adapter)

Table 14: Cisco UCS 6536 FI - Cisco UCS Blade Servers

Cisco VIC	IOM	
	2304v1/v2 & /2408	UCSX-I-9108-25G or UCSX-I-9108-100G
15230 (UCSX-ML-V5D200GV2)	-	Cisco UCS X210c M6, X210c M7, and X410c M7
15420 + UCS VIC 15000 bridge connector (UCSX-V5-BRIDGE+) + 15422 (UCSX-ME-V5Q50G)	-	Cisco UCS X210c M6, X210c M7, and X410c M7
15420 (UCSX-ML-V5Q50G)	-	Cisco UCS X210c M6, X210c M7, and X410c M7
15231 (UCSX-ML-V5D200G)	-	Cisco UCS X210c M6, X210c M7, and X410c M7
14425 + UCS VIC 14000 bridge connector (UCSX-V4-BRIDGE) + 14825 (UCSX-V4-Q25GME)	-	Cisco UCS X210c M6
14425 (UCSX-V4-Q25GML)	-	Cisco UCS X210c M6
15411 + Port Expander (UCSB-ML-V5Q10G + UCSB-MLOM-PT-01)	Cisco UCS B200 M6	-
15411 (UCSB-ML-V5Q10G)	Cisco UCS B200 M6	-
1440 + 1480 + Port Expander (UCSB-MLOM-40G-04 + UCSB-VIC-M84-4P) + UCSB-MLOM-PT-01	Cisco UCS B480 M5	-
1440 + 1480 + 1480 (UCSB-MLOM-40G-04 + UCSB-VIC-M84-4P +UCSB-VIC-M84-4P)	Cisco UCS B480 M5	-
1440 + 1480 (UCSB-MLOM-40G-04 + UCSB-VIC-M84-4P)	Cisco UCS B200 M6, B200 M5, B480 M5	-
1440 + Port Expander (UCSB-MLOM-40G-04 + UCSB-MLOM-PT-01)	Cisco UCS B200 M6, B200 M5, B480 M5	-
1440 (UCSB-MLOM-40G-04)	Cisco UCS B200 M6, B200 M5, B480 M5	-
1340 + 1380 + Port Expander	Cisco UCS B480 M5	-
1340 + 1380 + 1380	Cisco UCS B480 M5	-
1340 + 1380 (UCSB-MLOM-40G-03 + UCSB-VIC-M83-8P)	Cisco UCS B200 M5 and B480 M5	-

Cisco VIC	IOM	
	2304v1/v2 & /2408	UCSX-I-9108-25G or UCSX-I-9108-100G
1340 + Port Expander - 10G/40G (UCSB-MLOM-40G-03 + UCSB-MLOM-PT-01)	Cisco UCS B200 M5 and B480 M5	-
1340 - 10G/40G (UCSB-MLOM-40G-03)	Cisco UCS B200 M5 and B480 M5	-

Cisco UCS 6400 and 64108 FIs

Table 15: Cisco UCS 6400 and 64108 FIs - Cisco UCS Rack Servers

Cisco VIC	Direct Attach (10G/25G)	Direct Attach (4x10G/4x25)	Direct Attach (40G/100G)	FEX		
				2232 PP (10G)	93180YC-FX3 (25G server ports)	93180YC-FX3 (10G server ports)
15427 (UCSC-M-V5Q50GV2)	All Cisco UCS C-Series M6 and M7 servers	All Cisco UCS C-Series M6 and M7 servers	Not Supported	Not Supported	All Cisco UCS C-Series M6 and M7 servers	SFP-10G-SR/SR-S only
15237 (UCSC-M-V5D200GV2)	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported
15235 (UCSC-P-V5D200G)	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported
15238 (UCSC-M-V5D200G)	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported
15425 (UCSC-P-V5Q50G)	All Cisco UCS C-Series M6 and M7 servers	All Cisco UCS C-Series M6 and M7 servers	Not Supported	Not Supported	All Cisco UCS C-Series M6 and M7 servers	SFP-10G-SR/SR-S only
15428 (UCSC-M-V5Q50G)	All Cisco UCS C-Series M6 and M7 servers	All Cisco UCS C-Series M6 and M7 servers	Not Supported	Not Supported	All Cisco UCS C-Series M6 and M7 servers	SFP-10G-SR/SR-S only
Note Break-out is supported (6400 side QSFP, on adapter side two ports can be connected to 1 VIC (like ports 1 and 2) Reverse-breakout : Not supported						
1495-40G/100G (UCSC-PCIEC100-04)	Not Supported	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	Not Supported

Cisco VIC	Direct Attach (10G/25G)	Direct Attach (4x10G/4x25)	Direct Attach (40G/100G)	FEX		
				2232 PP (10G)	93180YC-FX3 (25G server ports)	93180YC-FX3 (10G server ports)
1477-40G/100G (UCSC-MV100 -04)	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported
1467-10G/25G (UCSC -MV25-04)	All Cisco UCS C-Series M6 servers	All Cisco UCS C-Series M6 servers	Not Supported	All Cisco UCS C-Series M6 servers	All Cisco UCS C-Series M6 servers	SFP-10G-SR/SR-S only
1457-10G/25G (UCSC-MLOM C25Q-04)	Cisco UCS C220 M5, C240 M5	Cisco UCS C220 M5, C240 M5	Not Supported	Cisco UCS C220 M5, C240 M5	Cisco UCS C220 M5, C240 M5	SFP-10G-SR/SR-S only
1455-10G/25G (UCSC-PCIEC 25Q-04)	All Cisco UCS C-Series M5 and M6 servers, and S-Series M5 servers	All Cisco UCS C-Series M5 and M6 servers, and S-Series M5 servers	Not Supported	All Cisco UCS C-Series M5 and M6 servers, and S-Series M5 servers	All Cisco UCS C-Series M5 and M6 servers, and S-Series M5 servers	SFP-10G-SR/SR-S only
1387 - 40G (UCSC-MLOM -C40Q-03)	All Cisco UCS C-Series M5 servers QSA at adapter)	Not Supported	Not Supported	All Cisco UCS C-Series M5 servers QSA at adapter)	Not Supported	With QSA and SFP-10G-SR only
1385 - 40G (UCSC-PCIE -C40Q-03)	All Cisco UCS C-Series M5 and S-Series M5 servers (Except C125 M5) QSA at adapter)	Not Supported	Not Supported	All Cisco UCS C-Series M5 and S-Series M5 servers (Except C125 M5) QSA at adapter)	Not Supported	With QSA and SFP-10G-SR only

Table 16: Cisco UCS 6400 and 64108 FIs - Cisco UCS Blade Servers

Cisco VIC	IOM	
	2204/2208/2408	UCSX-I-9108-25G
15230 (UCSX-ML-V5D200GV2)	Not Supported	Cisco UCS X210c M6, X210c M7, and X410c M7
15420 + UCS VIC 15000 bridge connector (UCSX-V5-BRIDGE+) + 15422 (UCSX-ME-V5Q50G)	Not Supported	Cisco UCS X210c M6, X210c M7, and X410c M7
15420 (UCSX-ML-V5Q50G)	Not Supported	Cisco UCS X210c M6 and X210c M7 servers

Cisco VIC	IOM	
	2204/2208/2408	UCSX-I-9108-25G
15231 (UCSX-ML-V5D200G)	Not Supported	Cisco UCS X210c M6 and X210c M7 servers
14425 + UCS VIC 14000 bridge connector (UCSX-V4-BRIDGE) + 14825 (UCSX-V4-Q25GME)	Not Supported	Cisco UCS X210c M6
14425 (UCSX-V4-Q25GML)	Not Supported	Cisco UCS X210c M6
15411 + Port Expander (UCSB-ML -V5Q10G + UCSB-MLOM -PT-01)	B200 M6	Not Supported
15411 (UCSB-ML -V5Q10G)	B200 M6	Not Supported
1440 + 1480 + 1480 (UCSB-MLOM-40G-04 + UCSB-VIC-M84-4P + UCSB-VIC-M84-4P)	Cisco UCS B480 M5	Not Supported
1440 + 1480 + Port Expander (UCSB-MLOM-40G-04 + UCSB-VIC- M84-4P) + UCSB-MLOM-PT-01	Cisco UCS B480 M5	Not Supported
1440 + 1480 (UCSB-MLOM-40G-04 + UCSB-VIC-M84-4P)	Cisco UCS B200 M6, B200 M5, B480 M5	Not Supported
1440 + Port Expander (UCSB-MLOM-40G-04 + UCSB-MLOM-PT-01)	Cisco UCS B200 M6, B200 M5, B480 M5	Not Supported
1440 (UCSB-MLOM-40G-04)	Cisco UCS B200 M6, B200 M5, B480 M5	Not Supported
1340 + 1380 + 1380	Cisco UCS B480 M5	Not Supported

Cisco VIC	IOM	
	2204/2208/2408	UCSX-I-9108-25G
1340 + 1380 + Port Expander	Cisco UCS B480 M5	Not Supported
1340 + Port Expander - 10G/40G (UCSB-MLOM-40G-03 + UCSB-MLOM-PT-01)	Cisco UCS B200 M5 and B480 M5	Not Supported
1340 + 1380 (UCSB-MLOM-40G-03 + UCSB-VIC-M83-8P)	Cisco UCS B200 M5 and B480 M5	Not Supported
1340 - 10G/40G (UCSB-MLOM-40G-03)	Cisco UCS B200 M5 and B480 M5	Not Supported

Cisco UCS 6300 FI

Table 17: Cisco UCS 6300 FI - Cisco UCS Rack Servers

Cisco VIC	Direct Attach	Direct Attach (Break-out)	FEX	
			2232 PP	2348
15427 (UCSC-M-V5Q50GV2)	All Cisco UCS C-Series M6 servers	All Cisco UCS C-Series M6 servers	Not Supported	All Cisco UCS C-Series M6 servers
15237 (UCSC-M-V5D200GV2)	All Cisco UCS C-Series M6 servers	Not Supported	Not Supported	Not Supported
15235 (UCSC-P-V5D200G)	All Cisco UCS C-Series M6 servers	Not Supported	Not Supported	Not Supported
15425 (UCSC-P-V5Q50G)	All Cisco UCS C-Series M6 servers	All Cisco UCS C-Series M6 servers	Not Supported	All Cisco UCS C-Series M6 servers
15428 (UCSC-M-V5Q50G)	All Cisco UCS C-Series M6 servers	All Cisco UCS C-Series M6 servers	Not Supported	All Cisco UCS C-Series M6 servers
15238 (UCSC-M-V5D200G)	All Cisco UCS C-Series M6 servers	Not Supported	Not Supported	Not Supported
1497-40G/100G (UCSC-MLOMC100-04)	Cisco UCS C220 M5, C240 M5 servers	Not Supported	Not Supported	Not Supported
1495-40G/100G (UCSC-PCIEC100-04)	All Cisco UCS C-Series M5 and M6 servers and S-Series M5 servers	Not Supported	Not Supported	Not Supported

Cisco VIC	Direct Attach	Direct Attach (Break-out)	FEX	
			2232 PP	2348
1477-40G/100G (UCSC-MV100-04)	All Cisco UCS C-Series M6 servers	Not Supported	Not Supported	Not Supported
1467-10G/25G (UCSC-MV25-04)	All Cisco UCS C-Series M6 servers (10G speed with 6332-16UP)	All Cisco UCS C-Series M6 servers	All Cisco UCS C-Series M6 servers	All Cisco UCS C-Series M6 servers
1457-10G/25G (UCSC-MLOMC25Q-04)	Cisco UCS C220 M5 and C240 M5 (10G speed with 6332-16UP)	Cisco UCS C220 M5 and C240 M5	Cisco UCS C220 M5 and C240 M5	Cisco UCS C220 M5 and C240 M5
1455-10G/25G (UCSC-PCIEC25Q-04)	All Cisco UCS C-Series M5 and M6 servers and S-Series M5 servers (10G speed with 6332-16UP)	All Cisco UCS C-Series M5 and M6 servers and S-Series M5 servers	All Cisco UCS C-Series M5 and M6 servers and S-Series M5 servers	All Cisco UCS C-Series M5 and M6 servers and S-Series M5 servers
1387 - 40G (UCSC-MLOM-C40Q-03)	All Cisco UCS C-Series M5 servers (40G or 10G using QSA)	Not Supported	All Cisco UCS C-Series M5 servers (QSA at adapter)	All Cisco UCS C-Series M5 servers (QSA at adapter)
1385 - 40G (UCSC-PCIE-C40Q-03)	All Cisco UCS C-Series M5 servers (except UCS C125 M5) and S-Series M5 servers (40G or 10G using QSA)	Not Supported	All Cisco UCS C-Series M5 servers (except UCS C125 M5) and S-Series M5 servers (40G or 10G using QSA)	All Cisco UCS C-Series M5 servers (except UCS C125 M5) and S-Series M5 servers (40G or 10G using QSA)

Table 18: Cisco UCS 6300 FI - Cisco UCS Blade Servers

Cisco VIC	IOM
	2304v1/v2 2204/2208
15411 + Port Expander (UCSB-ML-V5Q10G + UCSB-MLOM-PT-01)	Cisco UCS B200 M6
15411 (UCSB-ML-V5Q10G)	Cisco UCS B200 M6
1440 + 1480 + 1480	Cisco UCS B480 M5
1440 + 1480 + Port Expander (UCSB-MLOM-40G-04 + UCSB-VIC-M84-4P) + UCSB-MLOM-PT-01	Cisco UCS B480 M5
1440 + 1480 (UCSB-MLOM-40G-04 + UCSB-VIC-M84-4P)	Cisco UCS B200 M5, B480 M5 and B200 M6 servers
1440 + Port Expander (UCSB-MLOM-40G-04 + UCSB-MLOM-PT-01)	Cisco UCS B200 M5, B480 M5 and B200 M6 servers

Cisco VIC	IOM
	2304v1/v2 2204/2208
1440 (UCSB-MLOM-40G-04)	Cisco UCS B200 M5, B480 M5 and B200 M6 servers
1340 + 1380 + 1380	Cisco UCS B480 M5
1340 + 1380 + Port Expander	Cisco UCS B480 M5
1340 + Port Expander - 10G/40G (UCSB-MLOM-40G-03 + UCSB-MLOM-PT-01)	Cisco UCS B200 M5 and B480 M5 servers
1340 + 1380 (UCSB-MLOM-40G-03 + UCSB-VIC-M83-8P)	Cisco UCS B200 M5 and B480 M5 servers
1340 - 10G/40G (UCSB-MLOM-40G-03)	Cisco UCS B200 M5 and B480 M5 servers

Cisco UCS 6324 FI

Table 19: Cisco UCS 6324 FI - Cisco UCS Rack Servers

Cisco VIC	Direct Attach (10G)	Direct Attach (Break-out)
15428 (UCSC-M-V5Q50G)	Not Supported	Not Supported
15238 (UCSC-M-V5D200G)	Not Supported	Not Supported
1497-40G/100G (UCSC-MLOMC100-04)	Not Supported	Not Supported
1495-40G/100G (UCSC-PCIEC100-04)	Not Supported	Not Supported
1477-40G/100G (UCSC-MV100-04)	Not Supported	Not Supported
1467-10G/25G (UCSC-MV25-04)	Not Supported	Not Supported
1457-10G/25G (UCSC-MLOMC25Q-04)	Cisco UCS C220 M5 and C240 M5 servers	Cisco UCS C220 M5 and C240 M5 servers
1455-10G/25G (UCSC-PCIEC25Q-04)	All Cisco UCS C-Series and S-Series M5 servers	All Cisco UCS C-Series and S-Series M5 servers
1387 - 40G (UCSC-MLOM-C40Q-03)	All Cisco UCS C-Series M5 servers (QSA at the adapter)	Not Supported
1385 - 40G (UCSC-PCIE-C40Q-03)	All Cisco UCS C-Series M5 servers (QSA at the adapter)	Not Supported

Table 20: Cisco UCS 6324 FI - Cisco UCS Blade Servers

Cisco VIC	IOM	6324
	2204/2208	(Primary Chassis)
15411 (UCSB-ML-V5Q10G)	Not Supported	Not Supported
15411 + Port Expander (UCSB-ML-V5Q10G + UCSB-MLOM-PT-01)	Not Supported	Not Supported
1440 + 1480 + 1480 (UCSB-MLOM-40G-04 + UCSB-VIC-M84-4P +UCSB-VIC-M84-4P)	Not Supported	Cisco UCS B480 M5
1440 + 1480 + Port Expander (UCSB-MLOM-40G-04 + UCSB-VIC-M84-4P) + UCSB-MLOM-PT-01	Not Supported	Cisco UCS B480 M5
1440 + 1480 (UCSB-MLOM-40G-04 + UCSB-VIC-M84-4P)	Not Supported	Cisco UCS B200 M5 and B480 M5
1440 + Port Expander (UCSB-MLOM-40G-04 + UCSB-MLOM-PT-01)	Not Supported	Cisco UCS B200 M5 and B480 M5
1440 (UCSB-MLOM-40G-04)	Not Supported	Cisco UCS B200 M5 and B480 M5
1340 + 1380 + 1380	Cisco UCS B480 M5	Cisco UCS B480 M5
1340 + 1380 + Port Expander	Cisco UCS B480 M5	Cisco UCS B480 M5
1340 + 1380 (UCSB-MLOM-40G-03 + UCSB-VIC-M83-8P)	Cisco UCS B200 M5 and B480 M5	Cisco UCS B200 M5 and B480 M5
1340 + Port Expander - 10G/40G (UCSB-MLOM-40G-03 + UCSB-MLOM-PT-01)	Cisco UCS B200 M5 and B480 M5	Cisco UCS B200 M5 and B480 M5
1340 - 10G/40G (UCSB-MLOM-40G-03)	Cisco UCS B200 M5 and B480 M5	Cisco UCS B200 M5 and B480 M5

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 23. The following is the list of other supported hardware:

Table 21: Supported Hardware for UCS 6500 Series Fabric Interconnects

Type	Details
Chassis	UCSB-5108-AC2 UCSB-5108-DC2 Cisco UCSX-9508 Chassis (For Cisco UCS X-Series Servers)
Fabric Interconnects	UCS 6500
Fabric Extenders	93180YC-FX3 (25G server ports) 93180YC-FX3 (10G server ports) 2348 UPQ (10G server ports) 2304v1/v2 & /2408 UCSX-I-9108-25G or UCSX-I-9108-100G (Supported with Cisco UCS X-Series Servers)
Power Supplies	UCS-PSU-6536-AC UCSX-PSU-2800AC (For Cisco UCSX-9508 Chassis)

Table 22: 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 Cisco UCSX-9508 Chassis (For Cisco UCS X-Series Servers)
Fabric Interconnects	UCS 64108 UCS 6454
Fabric Extenders	2232 PP (10G) 93180YC-FX3 (25G server ports) 93180YC-FX3 (10G server ports) 2204/2208/2408 UCSX-I-9108-25G

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

Table 23: 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	2232 PP 2348 2304v1/v2 2204/2208
Power Supplies	UCS-PSU-6332-AC UCS-PSU-6332-DC

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

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 24: 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
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 CVR-QSFP28-SFP25G 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 **Note** FET-40G is supported only between FI and IOM/FEX QSFP-40G-ACU10M QSFP-40G-SR-BD QSFP-100G40G-BIDI **Note** QSFP-100G40G-BIDI is supported only on border ports/uplink ports in 40G mode.

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 between FI and I9108-100G IOM/N9K-C93180YC-FX3 FEX/border ports in 100G mode. 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 QSFP-4SFP25G-CU1M QSFP-4SFP25G-CU2M QSFP-4SFP25G-CU3M QSFP-4SFP25G-CU5M

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 QSFP-4SFP10G-CU1M QSFP-4SFP10G-CU3M QSFP-4SFP10G-CU5M QSFP-4X10G-AC7M QSFP-4X10G-AC10M QSFP-4X10G-AOC1M QSFP-4X10G-AOC3M QSFP-4X10G-AOC5M QSFP-4X10G-AOC7M

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 SFP-10/25G-LR-S SFP-10/25G-CSR-S
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 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 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 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 25: Minimum Software Versions for UCS Mini Chassis

Chassis	Minimum Software Version	Suggested Software Version
UCSB-5108-AC2	3.0(1e)	4.3(3a)
UCSB-5108-DC2	3.0(2c)	4.3(3a)

UCS Mini Supported Blade and Rack Servers

Table 26: Minimum Host Firmware Versions for Blade and Rack Servers on UCS Mini

Servers	Minimum Software Version	Suggested Software Version
B200 M6	4.2(1d)	4.3(3a)
B200 M5	4.2(1d)	4.3(3a)
B480 M5	4.2(1d)	4.3(3a)
C220 M5	4.2(1d)	4.3(3a)
C240 M5	4.2(1d)	4.3(3a)
C480 M5	4.2(1d)	4.3(3a)

UCS Mini Supported Adapters

Adapters	Minimum Software Version	Suggested Software Version
UCSC-PCIE-C25Q-04 (UCS VIC 1455)	4.2(2a)	4.3(3a)
UCSC-MLOM-C25Q-04 (UCS VIC 1457)	4.2(2a)	4.3(3a)
UCSB-VIC-M84-4P (UCS VIC 1480)	4.2(2a)	4.3(3a)

Adapters	Minimum Software Version	Suggested Software Version
UCSB-MLOM-40G-04 (UCS VIC 1440)	4.2(2a)	4.3(3a)
UCSC-PCIE-C40Q-03 (UCS VIC 1385) UCSC-MLOM-C40Q-03 (UCS VIC 1387)	3.1(3a)	4.3(3a)
UCSB-MLOM-40G-03 (UCS VIC 1340) UCSB-VIC-M83-8P (UCS VIC 1380)	3.1(3a)	4.3(3a)

UCS Mini Supported Fabric Interconnects

Fabric Interconnects	Minimum Software Version	Suggested Software Version
Cisco UCS 6324	3.1(3a)	4.3(3a)

UCS Mini Supported Fabric Extenders for Secondary Chassis

Fabric Extenders	Minimum Software Version	Suggested Software Version
UCS 2204 XP	3.1(3a)	4.3(3a)
UCS 2208 XP	3.1(3a)	4.3(3a)

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)	4.3(3a)

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

Gb Connector Modules	Transceivers Modules and Cables
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
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 27: Version Mapping

UCS Release	Catalog File Name	Additional PIDs in this Release
4.3(3a)	ucs-catalog.4.3.3a.T.bin	

UCS Release	Catalog File Name	Additional PIDs in this Release
		CPUs for Cisco UCS X210c M7 Compute Node: • UCSX-CPU-I8562Y+ • UCSX-CPU-I6542Y • UCSX-CPU-I6544Y • UCSX-CPU-I8558P • UCSX-CPU-I6530 • UCSX-CPU-I6554S • UCSX-CPU-I8592+ • UCSX-CPU-I8568Y+ • UCSX-CPU-I8592V • UCSX-CPU-I6548Y+ • UCSX-CPU-I6526Y • UCSX-CPU-I8580 • UCSX-CPU-I6534 • UCSX-CPU-I6538Y+ • UCSX-CPU-I6548N CPUs for Cisco UCS C220 M7 and C240 M7 servers: • UCS-CPU-I6542Y • UCS-CPU-I6544Y • UCS-CPU-I6548Y+ • UCS-CPU-I6526Y • UCS-CPU-I6530 • UCS-CPU-I8562Y+ • UCS-CPU-I8568Y+ • UCS-CPU-I8592+ • UCS-CPU-I8558P • UCS-CPU-I6534 • UCS-CPU-I6554S • UCS-CPU-I6538Y+ • UCS-CPU-I4514Y • UCS-CPU-I8580 • UCS-CPU-I8592V • UCS-CPU-I5515+ • UCS-CPU-I5520+ • UCS-CPU-I4516Y+

UCS Release	Catalog File Name	Additional PIDs in this Release
		• UCS-CPU-I8558 • UCS-CPU-I6548N DIMMs for Cisco UCS C220 M7 and C240 M7 servers: • UCS-MRX16G1RE3 • UCS-MRX32G1RE3 • UCS-MRX64G2RE3 • UCS-MRX96G2RF3 • UCS-MR128G4RE3 DIMMs for Cisco UCS X210c M7 Compute Node: • UCSX-MRX16G1RE3 • UCSX-MRX32G1RE3 • UCSX-MRX64G2RE3 • UCSX-MRX96G2RF3 • UCSX-MR128G4RE3
4.3(2e)	ucs-catalog.4.3.2e.T.bin	—
4.3(2c)	ucs-catalog.4.3.2c.T.bin	Cisco UCS X410c M7 Compute Node: • UCSX-410C-M7 • UCSX-410C-M7-U Cisco UCS VIC: • UCSC-M-V5Q50GV2 • UCSC-M-V5Q50GV2D • UCSX-ML-V5D200GV2 • UCSX-ML-V5D200GV2D • UCSC-M-V5D200GV2 • UCSC-M-V5D200GV2D

UCS Release	Catalog File Name	Additional PIDs in this Release
4.3(2b)	ucs-catalog.4.3.2b.T.bin	Cisco UCSX-9508 Chassis M7: • UCSX-M7-MLB • UCSX-9508-D= • UCSX-9508-D-U • UCSX-9508-D-CH Cisco UCS X210c M7 Compute Node: • UCSX-210C-M7 • UCSX-210C-M7-U Cisco UCS X210c M6 Compute Node: • UCSX-210C-M6 • UCSX-210C-M6-U Cisco UCS C240 M7 Server: • UCSC-C240-M7SX • UCSC-C240-M7SN Cisco UCS C220 M7 Server: • UCSC-C220-M7S • UCSC-C220-M7N Intelligent Fabric Module: • UCSX-I-9108-25G • UCSX-I-9108-100G Cisco UCS VIC: • UCSC-P-V5Q50G • UCSC-P-V5D200G • UCSX-ML-V5D200G-D • UCSX-ML-V5Q50G-D • UCSX-ME-V5Q50G-D • UCSX-V4-Q25GML • UCSX-V4-Q25GME NVIDIA GPU: • UCSC-GPU-T4-16 PSU: • UCSB-PSU-2500ACDV

Security Fixes

Security Fixes in Release 4.3(3a)

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.

CSCwi20282

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

- CVE-2007-2768—OpenSSH, when using OPIE (One-Time Passwords in Everything) for PAM, allows remote attackers to determine the existence of certain user accounts, which displays a different response if the user account exists and is configured to use one-time passwords (OTP), a similar issue to CVE-2007-2243.
- CVE-2008-3844—Certain Red Hat Enterprise Linux (RHEL) 4 and 5 packages for OpenSSH, as signed in August 2008 using a legitimate Red Hat GPG key, contain an externally introduced modification (Trojan Horse) that allows the package authors to have an unknown impact.
- CVE-2016-20012—OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session.
- 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-2018-20685—In OpenSSH 7.9, **`scp.c`** in the scp client allows remote SSH servers to bypass intended access restrictions via the filename of **`.`** or an empty filename. The impact is modifying the permissions of the target directory on the client side.
- CVE-2019-6109—An issue was discovered in OpenSSH 7.9. Due to missing character encoding in the progress display, a malicious server (or Man-in-The-Middle attacker) can employ crafted object names to manipulate the client output, for example, by using ANSI control codes to hide additional files being transferred. This affects **`refresh_progress_meter()`** in **`progressmeter.c`**.
- CVE-2019-6110—In OpenSSH 7.9, due to accepting and displaying arbitrary stderr output from the server, a malicious server (or Man-in-The-Middle attacker) can manipulate the client output, for example, to use ANSI control codes to hide additional files being transferred.

- 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).
- CVE-2020-14145—The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client).
- CVE-2020-15778—scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument.
- CVE-2021-28041—ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.
- CVE-2021-36368—An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf.
- CVE-2021-41617—sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.
- 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 4.3(2e)

CSCwh23927

Cisco UCS C225 M6 and C245 M6 servers with certain AMD® CPUs are affected by vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) ID:

- CVE-2023-20569—A side channel vulnerability on some of the AMD® CPUs may allow an attacker to influence the return address prediction. This may result in speculative execution at an attacker-controlled address, potentially leading to information disclosure.

CSCwh43415

Cisco UCS C225 M6 and C245 M6 servers with AMD® CPUs are affected by vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) IDs:

- CVE-2021-26345—Failure to validate the value in APCB may allow a privileged attacker to tamper with the APCB token to force an out-of-bounds memory read potentially resulting in a denial of service.
- CVE-2022-23830—SMM configuration may not be immutable, as intended, when SNP is enabled resulting in a potential limited loss of guest memory integrity.
- CVE-2021-46774—Insufficient DRAM address validation in System Management Unit (SMU) may allow an attacker to read/write from/to an invalid DRAM address, potentially resulting in denial-of-service.
- CVE-2023-20519—A Use-After-Free vulnerability in the management of an SNP guest context page may allow a malicious hypervisor to masquerade as the guest's migration agent resulting in a potential loss of guest integrity.
- CVE-2023-20566—Improper address validation in ASP with SNP enabled may potentially allow an attacker to compromise guest memory integrity.

CSCwh68315

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

- CVE-2023-23583—Sequence of processor instructions leads to unexpected behavior for some Intel® Processors may allow an authenticated user to potentially enable escalation of privilege and/or information disclosure and/or denial of service via local access.

Security Fixes in Release 4.3(2c)

CSCwh46667

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

- CVE-2022-0778—The BN_mod_sqrt() function, which computes a modular square root, contains a bug that can cause it to loop forever for non-prime moduli. This function is used when parsing certificates that contain elliptic curve public keys in compressed form or explicit elliptic curve parameters with a base point encoded in compressed form.

  It is possible to trigger the infinite loop by crafting a certificate that has invalid explicit curve parameters. Certificate parsing happens prior to verification of the certificate signature, and hence, any process that parses an externally supplied certificate may thus be subject to a denial of service attack.

  The infinite loop can also be reached when parsing crafted private keys as they can contain explicit elliptic curve parameters. Vulnerable situations include:

  - TLS clients consuming server certificates
  - TLS servers consuming client certificates
  - Hosting providers taking certificates or private keys from customers
  - Certificate authorities parsing certification requests from subscribers
  - Anything else which parses ASN.1 elliptic curve parameters
  - Also any other applications that use the BN_mod_sqrt() where the attacker can control the parameter values are vulnerable to this DoS issue

In the OpenSSL 1.0.2 version the public key is not parsed during initial parsing of the certificate which makes it slightly harder to trigger the infinite loop. However, any operation which requires the public key from the certificate triggers the infinite loop. In particular the attacker can use a self-signed certificate to trigger the loop during verification of the certificate signature. This issue affects OpenSSL versions 1.0.2, 1.1.1 and 3.0. It was addressed in the releases of 1.1.1n and 3.0.2 on the 15th March 2022. Fixed in OpenSSL 3.0.2 (Affected 3.0.0,3.0.1). Fixed in OpenSSL 1.1.1n (Affected 1.1.1-1.1.1m). Fixed in OpenSSL 1.0.2zd (Affected 1.0.2-1.0.2zc).

The affected third-party software component is 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 4.3(2b)

CSCwc01592

Cisco UCS Manager feature if affected by the following Common Vulnerability and Exposures (CVE) ID:

- CVE-2023-20016—A vulnerability in the backup configuration feature of Cisco UCS Manager and in the configuration export feature of Cisco FXOS 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.
- For more information see Cisco FXOS Software and UCS Manager Software Configuration Backup Static Key Vulnerability

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.

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.

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.

Note You must have a Cisco.com account to log in and access the Cisco Bug Search Tool. If you do not have one, you can register for an account.

For more information about the Cisco Bug Search Tool, see the Bug Search Tool Help & FAQ.

Resolved Caveats in Release 4.3(3a)

The following caveats are resolved in Release 4.3(3a):

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCwi31115	Cisco UCS 6454 FI does not detect the NX-OS on the active FI after replacement. This issue is resolved.	4.2(1n)A	4.3(3a)A
CSCwh37590	Cisco UCS Manager displays error while changing the Power Save Policy. This issue is resolved.	4.3(2c)A	4.3(3a)A
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	4.3(3a)A

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCwh75796	SCP backup on Linux host server fails due to MOD message. This issue is resolved.	4.2(3h)C	4.3(3a)C
CSCwh26280	In a setup equipped with Cisco UCS X210c M7 servers, when IPMI tool sends a query to the out-of-band (OOB) IP address for the server, it takes more than 30 seconds to receive a response. This delay causes monitoring tools to display an error because the expected response time in less than 30 seconds. This issue is resolved.	4.3(2c)A	4.3(3a)A

Resolved Caveats in Release 4.3(2e)

The following caveats are resolved in Release 4.3(2e):

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCwe95417	Cisco UCS 5108 AC2 chassis shows incorrect power chart after upgrading to release 4.3(2c)A bundle. This issue is resolved.	4.3(2c)A	4.3(2e)A

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCwh26280	In a setup equipped with Cisco UCS X210c M7 servers, when IPMI tool sends a query to the out-of-band (OOB) IP address for the server, it takes more than 30 seconds to receive a response. This delay causes monitoring tools to display an error because the expected response time in less than 30 seconds. This issue is resolved.	4.3(2c)A	4.3(2e)A
CSCwh31644	Cisco UCS Manager fails to discover any Chassis or rack servers. This issue is resolved.	4.2(3e)A	4.3(2e)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	4.3(2e)A

Resolved Caveats in Release 4.3(2c)

The following caveats are resolved in Release 4.3(2c):

Defect ID	Symptom	First Bundle Affected	Resolved in Release
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	4.3(2c)A

Defect ID	Symptom	First Bundle Affected	Resolved in Release
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	4.3(2c)A
CSCwf56305	Cisco UCS VIC 1455 shows incorrect Port enumeration. This issue is resolved.	4.2(2a)A	4.3(2c)A

CSCwh60769	DIMMs with M321R8GA0BB0-CQKDS OEM part number (Samsung 64gb DIMMs 4800MHz) display the following fault:
	`Severity: Warning`
	`Code: F0502`
	`ID: 327373`
	`Status: None`
	`Description: DIMM DIMM_PX_X1 on server 1/6 has an invalid FRU`
	`Affected Object: sys/chassis-X/blade-X/board/memarray-X/mem-X`
	`Name: Memory Unit Identity Unestablishable`
	`Cause: Identity Unestablishable`
	This issue is resolved.
		4.3(2b)A	4.3(2c)A

CSCwf91291	The RAID controller in Cisco UCS X210c servers may read incorrect voltage value and mark the battery as dead. This results in the following error: `Battery Backup unit IMM/chassis-x/server-y/controller-1/ BBU is marked bad and needs to be replaced` This issue is resolved.	4.3(2b)A	4.3(2c)A

Defect ID	Symptom	First Bundle Affected	Resolved in Release
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	4.3(2c)A
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	4.3(2c)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	4.3(2c)A

Resolved Caveats in Release 4.3(2b)

The following caveats are resolved in Release 4.3(2b):

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCvy59090	In a rare event when all the fans are **Inoperable** and a thermal even occurs, the IOM CMC may shutdown the entire chassis. This issue is resolved.	4.0(4a)A	4.3(2b)A

Defect ID	Symptom	First Bundle Affected	Resolved in Release
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. This issue is resolved.	4.2(3b)	4.3(2b)
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	4.3(2b)B
CSCvh04298	The IOMs connected to an FI no longer reboot unexpectedly due to software-controlled resets. This issue is resolved.	3.1(3c)A	4.3(2b)A

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCwf00940	Broadcom Inc.® AERO RAID Controller (Cisco UCS X210c RAID module) power good response is high when host is powered on. This issue is resolved. Broadcom Inc.® released new Vision PSOC image to improve AERO RAID Controller board power good response.	4.3(2b)A	4.3(2b)A
CSCwf18625	Few UCS-HD1T7K12N and UCS-HD2T7K12N running firmware version CN05 may experience timeouts and go offline. This issue is resolved.	4.1(3j)C	4.3(2b)C

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.

Note You must have a Cisco.com account to log in and access the Cisco Bug Search Tool. If you do not have one, you can register for an account.

For more information about the Cisco Bug Search Tool, see the Bug Search Tool Help & FAQ.

Open Caveats for Release 4.3(3a)

The following caveats are open in Release 4.3(3a):

Defect ID	Symptom	Workaround	First Bundle Affected
CSCwi70964	In a setup up equipped with Cisco UCS M7 servers (with Intel® Xeon® Platinum 8558P Processor) and Nvidia® H100 GPU adapter, RHEL/Ubuntu installation or bootup fail with kernal panic.	Perform one of the following: • Update BIOS settings MMIO High Granularity to 1024GB from **Advanced** > **Socket Config** > **Uncore Config** > **Uncore General Config** • Disable QAT setting for all processors in BIOS settings from **Advanced** > **Socket Confg** > **IIO Config** > **IOAT Config** > **Sck0 IOAT Config**. Disable CPM. Perform these for all the sockets in the processor.	4.3(3a)B and C
CSCwi84495	Cisco UCS M7 Blade servers equipped with Intel® Xeon® Platinum 8558P Processor and Intel Flex 170 GPU adapter fail to boot and gets into continuous reset loop.	Disable QAT setting for all processors in BIOS settings from **Advanced** > **Socket Confg** > **IIO Config** > **IOAT Config** > **Sck0 IOAT Config**. Disable CPM. Perform these for all the sockets in the processor.	4.3(3a)B and C

Defect ID	Symptom	Workaround	First Bundle Affected
CSCwi01267	In a setup up equipped with Cisco UCS M7 Blade servers and Intel® Flex 170, 140 GPU adapters, RHEL/Ubuntu installation or bootup fail with kernal panic.	Update BIOS following MMIO High settings from **Advanced** > **Socket Config** > **Uncore Config** > **Uncore General Config** • MMIO High Granularity to 1024 GB • MMIO High Base to 56T • Disable **Limit CPU PA to 46 bits**	4.3(3a)B and C

Open Caveats for Release 4.3(2e)

There are no open caveats in Release 4.3(2e).

Open Caveats for Release 4.3(2c)

There are no open caveats in Release 4.3(2c).

Open Caveats for Release 4.3(2b)

The following caveats are open in Release 4.3(2b):

Defect ID	Symptom	Workaround	First Bundle Affected

CSCwe09048	If you install ESXi OS on SAN LUN on Cisco UCS X210 M6 server and same service profile is associated with Cisco UCS X210 M7 server, the OS results in PSOD boot error.	1. Press **Shift** + **O** to enter boot option.
		2. Execute the following command to get the recovery_key:
		`esxcli system settings encryption recovery list`
		3. Provide this TPM recovery key as a boot option during Cisco UCS X210 M7 boot.
		`encryptionRecoveryKey=recovery_key`
			4.3(2b)

Defect ID	Symptom	Workaround	First Bundle Affected
CSCwf53294	In a setup with Cisco UCS M7 servers, RHEL 8.7 does not boot up when VMD is enabled in the BIOS. Server boots to a blank screen or boot halts with the following message: `DMAR: DRHD: handling fault status reg 2 DMAR: [INTR-REMAP] Request device [c2:00.5] fault index 0x8000 [fault reason 0x25] Blocked a compatibility format interrupt request.`	Perform one of the following: 1. Cisco recommends that you should upgrade to RHEL release 8.8 2. For existing RHEL 8.7 installation, perform the following: a. Upgrade the kernel to 4.18.0-425.13.1.el8_7 or later. b. Remove boot parameter intremap=off if used before c. Update BIOS to release 4.3(2b) 3. For new RHEL 8.7 installation, perform the following: a. Disable VMD. b. Install RHEL version 8.7 c. Update kernel to 4.18.0-425.13.1.el8_7 or later. d. Reboot and Enable VMD in the BIOS.	4.3(2b)
CSCwf44478	In a setup equipped with Cisco UCS C-Series and X-Series M7 servers, running RHEL OS versions 8.6 or 9.0, Micron 7450 NVMe drives do not get detected after hot-plug.	For RHEL version 8.6, update kernel to version 4.18.0-425.13.1.el8_7 or later For RHEL version 9.0, update kernel to version 5.14.0-162.6.1.el9_1 or later	4.3(2b)

Defect ID	Symptom	Workaround	First Bundle Affected
CSCwe95482	While moving Cisco UCS X-Series server managed by Cisco UCS X9508 Chassis from IMM to UCS Manager manged mode, it may take about 10 minutes for the Discovery FSM to show. This happens when the servers are in CIMC version 5.1.1.x or earlier.	Wait for 10 minutes after inserting the blade in the chassis. The discovery FSM status should show up. If it does not, upgrade the server to CIMC 5.1.1.x or later version before inserting the server to a UCS Manager managed chassis.	4.3(2b)
CSCwb76030	After decommissioning and recommissioning, server discovery fails with the following error message: `no connection to MC endpoint`	Wait for at least 30 seconds after decommissioning is completed before performing recommission.	4.3(2b)
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)
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)
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
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)
CSCwf21977	Cisco UCS Manager CLI interface does not support manual control over day light saving time settings.	There is no known workaround.	4.2(1l)

Known Behavior and Limitations in Release 4.3

Known Behavior and Limitations in Release 4.3(3a)

There are no known behavior and limitations in Release 4.3(3a).

Known Behavior and Limitations in Release 4.3(2e)

There are no known behavior and limitations in Release 4.3(2e).

Known Behavior and Limitations in Release 4.3(2c)

There are no known behavior and limitations in Release 4.3(2c).

Known Behavior and Limitations in Release 4.3(2b)

Defect ID	Symptom	Workaround	First Bundle Affected
CSCwd82136	In a setup equipped with Cisco UCS 6400 Series FI connecting using passive copper cables to Cisco UCS C-Series servers with Cisco UCS VIC1457/1455/1467, ports on the FI may to error-disabled state with the following reason after a link flap or after a server is decommissioned and recommissioned: `errDisabledExcessportIn`	Flap the Fabric Interconnect (FI) port connected to the Cisco UCS C-Series server.	4.3(2b)

Defect ID	Symptom	Workaround	First Bundle Affected
CSCwe98830	If Cisco UCS S3260 chassis is equipped with Cisco UCS B-Series server, the firmware details are not displayed for Cisco UCS VIC card.	There is no known workaround.	4.3(2b)
CSCwe48563	In a setup equipped with Cisco UCS 6400 Series or 6536 FIs, logical configuration from any 4.2(3) patch release to 4.2(3b) succeeds instead of failing due to enhancement in the security.	There is no known workaround.	4.3(2b)
CSCwe32091	Under the following conditions Cisco UCS VIC support MAX LUN values above 1024: • UCS Manager with release 4.2(3d) or later. • Cisco UCS VIC firmware version 5.2.3c.230101 or earlier for 14XX series or 4.5.3b.230101 or earlier for 13XX series.	There is no known workaround. Update Cisco UCS VIC firmware version.	4.3(2b)

Defect ID	Symptom	Workaround	First Bundle Affected
CSCwf61445	Cisco recommends the below screen resolutions for launching the UCS Manager for the best experience. • 1920 x 1080 • 1600 x 900 • 1440 x 900 • 1360 x 768 • 1280 x 768 • 1280 x 720 Cisco UCS Manager does not support browser full screen mode. Hence, use the recommended resolutions only.	There is no known workaround.	4.3(2b)
CSCvp31928	UCS Manager allows you to delete security without any warning. Set-up continues to function normally without security.	This issue does not have any functionality impact.	4.3(2b)
CSCvh60768	In a setup running ESXi OS, when vNICs are removed in Service Profile while CDN (Consistent Device Naming) is enabled, the vNICs are re-orederd from the vNIC, which was removed.	Manually assign vmNIC number in /etc/vmware/esx.conf file and reboot.	3.2(2)B
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

Defect ID	Symptom	Workaround	First Bundle Affected
CSCvp38564	NMPTU in AD mode hangs or goes into infinite loop when DCPMM in AppDirect mode.	If DCPMM is detected in system, BIOS does not load NMPTU to prevent hang/infinite loop.	4.0(3)
CSCvp37389	DCPMM clock stop may cause DCPMM media to go into disable state.	There is no known workaround.	4.0(3)
CSCva74263	Cisco UCS 6324 In a setup equipped with Cisco UCS 6324 FI (Cisco UCS Mini FI), QoS buffers get full and do not drain out. As a result, all packets get dropped on the FI and there are no Tx on the uplink ports.	Reboot the FI to clear this cnodition.	3.1(1e)
CSCvh17760	IOM reboots without core.	There is no known workaround.	3.(1g)
CSCvs83647	Cisco UCS 6454 FI reboots with the following error mssage: `Security Daemon hap reset`	There is no known workaround.	4.0(4d)A
CSCwh22856	UCS Manager does not allow creation of same VSAN ID in both SAN cloud and storage cloud from release 4.3(2b). However, if you were already using the same VSAN for both SAN cloud and storage cloud, then you cannot modify the duplicate VSAN configuration after upgrading to release 4.3(2b).	There is no known workaround.	4.3(2b)

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