

Release Notes for Cisco Intersight Managed Mode Infrastructure Firmware, Release 6.0

First Published: 2025-08-05

Last Modified: 2026-10-26

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

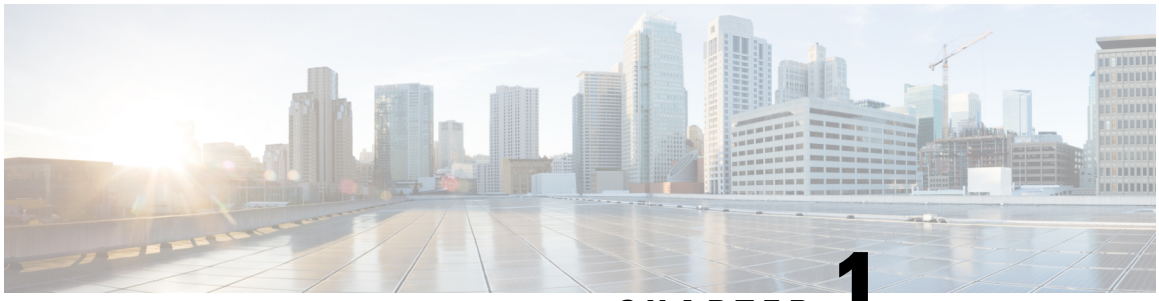
Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual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

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

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

© 2025–2026 Cisco Systems, Inc. All rights reserved.



CHAPTER 1

Cisco Intersight Managed Mode Infrastructure Firmware, Release 6.0

- Cisco Intersight Managed Mode Infrastructure Firmware, Release 6.0, on page 1
- Firmware Version Equivalency Between Cisco Intersight, Cisco IMC, and Cisco UCS Manager, on page 1
- Revision History, on page 2

Cisco Intersight Managed Mode Infrastructure Firmware, Release 6.0

Firmware upgrades in Intersight include server firmware upgrades and infrastructure firmware upgrades. Infrastructure firmware upgrades in Intersight Managed mode is supported on Cisco UCS Fabric Interconnects Series 6600, 6500, 6400, and Cisco UCS X-Series Direct Fabric Interconnects. To manage the Cisco UCS infrastructure firmware, see Upgrading Fabric Interconnect Firmware in IMM. This feature is available with a Cisco Intersight Essentials or Advanced license tier.

In Intersight, infrastructure and server firmware upgrades can be done independently. That is, you do not need to upgrade infrastructure firmware to use the latest server firmware and vice versa. For more information on compatibility between infrastructure firmware and server firmware, see Cross Version Firmware Support. For more information on server firmware updates, see Release Notes for Cisco Intersight Managed Mode Server Firmware.

Firmware Version Equivalency Between Cisco Intersight, Cisco IMC, and Cisco UCS Manager

For more information, see Cisco UCS Equivalency Matrix for Cisco Intersight, Cisco IMC, and Cisco UCS Manager.

To view the complete matrix in PDF format, click here.

Revision History

The following table includes the change history for this document.

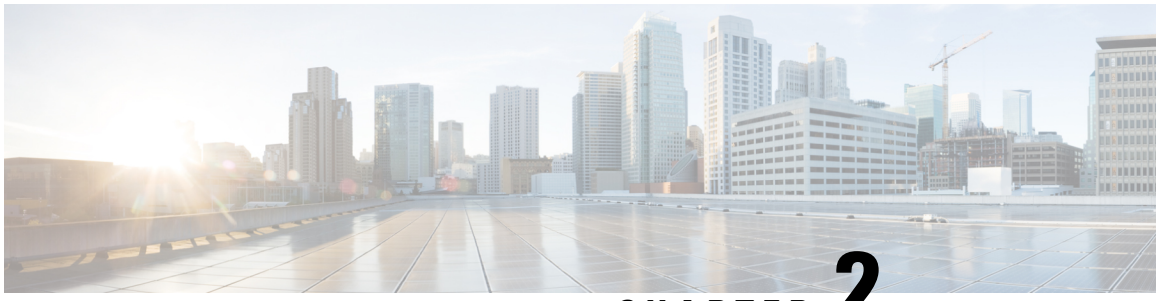
Table 1: Release 6.0

Revision Date	Description
October 26, 2026	Cisco UCS C-Series C220 M8 and C240 M8 6.0(2.260236) Server Firmware version has been released. There is no corresponding Infrastructure Firmware release.
October 09, 2026	Added **Security Hardening Updates** to Security fixes in Release 6.0(2.260080).
September 23, 2026	Updated release notes for Cisco UCS 6600, 6500, and 6400 Series Fabric Interconnect and Cisco UCS X-Series Direct Fabric Interconnect Infrastructure Firmware version 6.0(2.260080). This release includes updates to: • Resolved issues in Release 6.0(2.260080) It does not include any new hardware support, security fixes, or open issues.
August 17, 2026	Cisco UCS X-Series M8, M7 6.0(2.260180) and Cisco UCS C-Series M8, M7 6.0(2.260180) Server Firmware versions have been released. There is no corresponding Infrastructure Firmware release.
July 14, 2026	Cisco UCS B-Series M5 6.0(1.260031) Server Firmware version has been released. There is no corresponding Infrastructure Firmware release.
June 25, 2026	Updated release notes for Cisco UCS 6600, 6500, and 6400 Series Fabric Interconnect and Cisco UCS X-Series Direct Fabric Interconnect Infrastructure Firmware version 6.0(2.260067). This release includes updates to: • Resolved issues in Release 6.0(2.260067) It does not include any new hardware support, security fixes, or open issues.

Revision Date	Description
April 23, 2026	Updated release notes for Cisco UCS 6600, 6500, and 6400 Series Fabric Interconnect and Cisco UCS X-Series Direct Fabric Interconnect Infrastructure Firmware version 6.0(2.260055). It does not include any new hardware features, security fixes, resolved issues, or open issues. Corresponding server firmware release notes have been updated for the following versions: X-Series M8, M7, M6 6.0(2.260069), C-Series M8, M7, M6 6.0(2.260069), and B-Series M6 6.0(2.260069). Cisco UCS X580p PCIe Node firmware version 6.0(2.260069) and Cisco UCS X9508 Chassis firmware version 6.0(2.260069) have been released.
March 27, 2026	Updated release notes for Cisco UCS 6600, 6500, and 6400 Series Fabric Interconnect and Cisco UCS X-Series Direct Fabric Interconnect Infrastructure Firmware version 6.0(1.260006). This release includes updates to: • Resolved issues in Release 6.0(1.260006) It does not include any new hardware support, security fixes, or open issues.
March 16, 2026	Cisco UCS B-Series M5 6.0(1.260012) Server Firmware version has been released. There is no corresponding Infrastructure Firmware release.
March 16, 2026	Updated release notes for Cisco UCS 6600, 6500, 6400 Series FI and Cisco UCS X-Series Direct FI Infrastructure Firmware version 6.0(2.260045). This release includes updates to: • New hardware features in 6.0(2.260045) • Resolved issues in Release 6.0(2.260045) • Open issues in Release 6.0(2.260045) • Known issues in Release 6.0(2.260045) It does not include any security fixes.
March 02, 2026	Included CSCwt36346 in Open issues in Release 6.0(1.250198)

Revision Date	Description
February 06, 2026	Updated release notes for Cisco UCS 6600, 6500, and 6400 Series Fabric Interconnect Infrastructure firmware release 6.0(1.260003) and Cisco UCS X-Series Direct Fabric Interconnect Infrastructure Firmware version 6.0(1.260003). This release includes updates to: • Resolved issues in Release 6.0(1.260003) It does not include any new hardware support, security fixes, or open issues.
January 14, 2026	Cisco UCS C-Series M8 6.0(1.250194) Server Firmware version has been released. There is no corresponding Infrastructure Firmware release.
December 18, 2025	Updated release notes for Cisco UCS 6600, 6500, and 6400 Series Fabric Interconnect Infrastructure firmware release 6.0(1.250243) and Cisco UCS X-Series Direct Fabric Interconnect Infrastructure Firmware version 6.0(1.250243). It does not include any new hardware feature, security fixes, resolved issues, or open issues. Corresponding server firmware release notes have been updated for the following versions: Cisco UCS X-Series M8 6.0(1.252114), M7, M6 6.0(1.250179), Cisco UCS B-Series M6, M5 6.0(1.250169), and Cisco UCS C-Series M8, M7, M6 6.0(1.250192). Cisco UCS X580p PCIe Node firmware version 6.0(1.252050) and Cisco UCS X9508 Chassis firmware version 6.0(1.252050) have been released.
December 12, 2025	Updated the following sections: • New hardware features in 6.0(1.250229) to include support for Cisco UCS X580p PCIe Node and Cisco UCS X9516 X-Fabric. • Open issues in Release 6.0(1.250229) to include CSCwr31737.
November 21, 2025	Cisco UCS X-Series M8 6.0(1.252039) Server Firmware version has been released. There is no corresponding Infrastructure Firmware release.

Revision Date	Description
November 12, 2025	Updated release notes for Cisco UCS 6600, 6500, and 6400 Series Fabric Interconnect Infrastructure firmware release 6.0(1.250229) and Cisco UCS X-Series Direct Fabric Interconnect Infrastructure Firmware version 6.0(1.250229). It does not include any new hardware feature, security fixes, resolved issues, or open issues. Corresponding server firmware release notes have been updated for the following versions: Cisco UCS X-Series M8, M7, M6 6.0(1.250162), Cisco UCS B-Series M6, M5 6.0(1.250157), and Cisco UCS C-Series M8, M7, M6 6.0(1.250174).
November 07, 2025	Added information on deprecated hardware.
October 09, 2025	Cisco UCS X-Series M8, M7, M6 6.0(1.250122), Cisco UCS B-Series M6, M5 6.0(1.250127), and Cisco UCS C-Series M8, M7, M6 6.0(1.250131) Server Firmware versions have been released. There is no corresponding Infrastructure Firmware release.
September 09, 2025	Added Cisco UCS NVMeoF Support Matrix for 3rd Party Storage Vendors matrix.
September 02, 2025	Created release notes for Cisco UCS 6600, 6500, and 6400 Series Fabric Interconnect Infrastructure firmware 6.0(1.250198) and Cisco UCS X-Series Direct Fabric Interconnect Infrastructure firmware 6.0(1.250198). This release includes updates to: • New hardware features in 6.0(1.250198) • Open issues in Release 6.0(1.250198) It does not include any security fixes or resolved issues.



CHAPTER 2

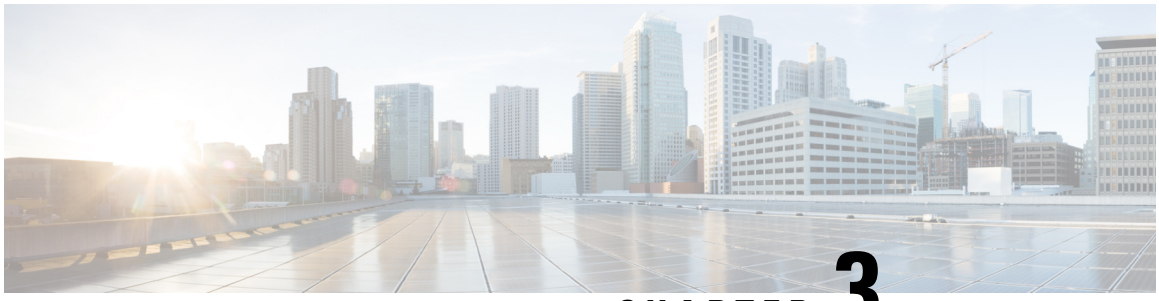
New software features

• New software features, on page 7

New software features

Intersight software features may not align with the Intersight firmware release schedule. To know more about the latest software features, see the What's New section in Intersight Help Center.

New software features



CHAPTER 3

New hardware features

- New hardware features in Infrastructure Firmware Release 6.0(2.260080) — None, on page 9
- New hardware features in Infrastructure Firmware Release 6.0(2.260067) — None, on page 9
- New hardware features in Infrastructure Firmware Release 6.0(1.260006) — None, on page 9
- New hardware features in Infrastructure Firmware Release 6.0(2.260045), on page 9
- New hardware features in Infrastructure Firmware Release 6.0(1.260003) — None, on page 10
- New Hardware Features in Infrastructure Firmware Release 6.0(1.250229), on page 10
- New hardware features in Infrastructure Firmware Release 6.0(1.250198), on page 11

New hardware features in Infrastructure Firmware Release 6.0(2.260080) — None

New hardware features in Infrastructure Firmware Release 6.0(2.260067) — None

New hardware features in Infrastructure Firmware Release 6.0(1.260006) — None

New hardware features in Infrastructure Firmware Release 6.0(2.260045)

Cisco UCS 6652 Fabric Interconnect

The Cisco UCS 6652 fabric interconnect is a 1-rack-unit (1-RU), fixed-port system designed for top-of-rack deployment in data centers with a total of 52 ports.

The Cisco UCS 6652 fabric interconnect supports an array of Gigabit Ethernet (GbE), Fibre Channel (FC), and Fibre Channel over Ethernet (FCoE) ports to provide connectivity to peer data center devices. The system offers the following ports and capabilities:

- 48 ZSFP ports (ports 1–48) that support 10G, 25G, and 50G Ethernet speeds.
- 4 QSFP-DD uplink ports (ports 49–52) that support 40G, 100G, and 400G Ethernet speeds.
- Breakout capability is supported only on QSFP-DD ports.
- 16 unified ports (ports 17–32) that support either:
  - 10/25/50 Gbps Ethernet or FCoE, or
  - 16/32/64 Gbps Fibre Channel.
- Unified ports provide full retimer and MACsec support.
- All Ethernet ports support Fibre Channel over Ethernet (FCoE).
- The fabric interconnect includes management, console, USB, and high-availability L1/L2 ports.
- The architecture supports low-latency, deterministic, line-rate switching.

For more information, see the Cisco UCS 6600 Series Fabric Interconnects Data Sheet.

Note The Cisco UCS 6652 FI supports these components:

- Cisco UCSX-9508 chassis that support Cisco UCSX-I-9108-25G Intelligent Fabric Modules (IFM) and Cisco UCS X-series blade servers with Cisco UCS VIC 14,000 or 15,000 series adapters
- Cisco UCS 5108 chassis with IOM 2408
- Cisco UCS C-series servers with Cisco UCS VIC 1400 or 15,000 series adapters, and
- Cisco UCS C-series servers using Nexus 93180YC-FX3 in Fabric Extender (FEX) mode.

New hardware features in Infrastructure Firmware Release 6.0(1.260003) — None

New Hardware Features in Infrastructure Firmware Release 6.0(1.250229)

This section provides a brief description of the new hardware features.

Cisco UCS X580p PCIe Node

The Cisco UCS X580p PCIe Node is the latest PCIe resource node for the UCS X-Series Modular System. It delivers high-performance GPU support for workloads such as generative and agentic AI fine-tuning, inference, and other applications that require GPU acceleration.

The Cisco UCS X580p PCIe Node supports up to four PCIe GPUs. It can be paired with the Cisco UCS X210c M8 server (with Intel® Xeon® processors) or the UCS X215c M8 server (with EPYC processors). The X580p uses Cisco UCS X-Fabric technology for GPU connectivity.

The X580p occupies two node slots in the X-Series chassis and allows assignment of up to four GPUs per node. Each 7RU Cisco UCS X9508 chassis supports up to two PCIe Nodes, with each node pairing with one or two servers.

For more information, see Cisco UCS X580p PCIe Node Installation and Service Guide and Cisco UCS X580p PCIe Node Spec Sheet.

Cisco UCS X9516 X-Fabric

The Cisco UCS X9516 X-Fabric is the second-generation X-Fabric module for the UCS X9508 chassis. It provides ultra-low-latency PCIe Gen5 switching and SmartNIC support, enabling flexible and composable IT resources. Managed via Cisco Intersight®, the UCS X9516 X-Fabric allows GPUs and NICs to be dynamically provisioned across servers using policy-based management.

Paired with the UCS X580p PCIe Node, the X9516 X-Fabric supports up to four dual-slot GPUs per node with NVLink Bridge support, serving as the control point for modular GPU composability in AI-driven environments.

For more information, see Cisco UCS X9516 X-Fabric Data Sheet.

Minimum Firmware Requirements to Support Cisco UCS X580p PCIe Node and Cisco UCS X9516 X-Fabric

- X580p PCIe Node Firmware: 6.0(1.252044)
- X9508 Chassis Firmware: 6.0(1.252044)
- Cisco UCS X-Series M8 Server Firmware: 6.0(1.252039)
- Fabric Interconnect Infrastructure Firmware: 6.0(1.250229)

Note The X580p PCIe Node firmware 6.0(1.252044) and X9508 Chassis firmware 6.0(1.252044) are available as separate bundles.

New hardware features in Infrastructure Firmware Release 6.0(1.250198)

This section provides a brief description of the new hardware features.

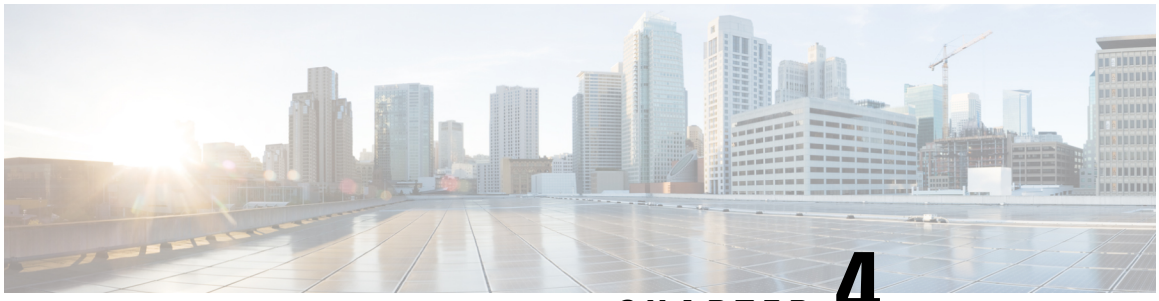
Cisco UCS 6664 Fabric Interconnect

The Cisco UCS 6664 Fabric Interconnect is a 2-rack unit (RU), fixed-port system designed for Top-of-Rack deployment in data centers. It reduces cabling complexity for the Cisco UCS® X-Series Modular System and Cisco UCS C-Series Rack Servers.

The Fabric Interconnect supports an array of Gigabit Ethernet (GbE), Fibre Channel (FC), and Fibre Channel over Ethernet (FCoE) ports to offer connectivity to peer data center devices. For more information, see Cisco UCS 6600 Series Fabric Interconnects Data Sheet.

Note

- Cisco UCS 6664 Fabric Interconnect (FI) is supported with the UCSX-9508 chassis using the UCSX-I-9108-25G and UCSX-I-9108-100G Intelligent Fabric Modules (IFMs).
- Cisco UCS 6664 FI supports the UCS IOM 2408 when used with the Cisco UCS 5108 chassis.



CHAPTER 4

Security fixes

You can view the open issues, resolved issues, and security fixes using the Cisco Bug Search Tool.

- Security fixes in Release 6.0(2.260080), on page 13
- Security fixes in Release 6.0(2.260067) — None, on page 14
- Security fixes in Release 6.0(1.260006) — None, on page 14
- Security fixes in Release 6.0(2.260045) — None, on page 14
- Security fixes in Release 6.0(1.260003) — None, on page 14
- Security fixes in Release 6.0(1.250229) — None, on page 14
- Security fixes in Release 6.0(1.250198) — None, on page 14

Security fixes in Release 6.0(2.260080)

Security Hardening Updates

Cisco NX-OS Software updates include security hardening to address multiple vulnerabilities identified during internal testing. Cisco is not aware of these vulnerabilities being actively exploited. Related issues are grouped by Common Weakness Enumeration (CWE) and associated with a single Common Vulnerabilities and Exposures (CVE) identifier to support customer remediation and disclosure.

Cisco has released software updates that address these vulnerabilities. There are no workarounds that address these vulnerabilities.

CVE ID	Description
CVE-2026-76453	Improper neutralization (covers command, OS, and argument injection)
CVE-2026-76455	Improper access control (covers authorization, authentication, privileges, and bypasses)
CVE-2026-76456	Improper input validation (covers input validation, path traversal, and external path control)
CVE-2026-76457	Out-of-bounds read (covers buffer over-read and exposure of sensitive information)
CVE-2026-76458	Improper handling of exceptional conditions (covers uncaught exceptions and reachable assertions)

CVE ID	Description
CVE-2026-76459	Out-of-bounds write (covers stack-based buffer overflow, heap-based buffer overflow, classic buffer overflow, and incorrect buffer size calculation)

This advisory is available at the following link:

Cisco NX-OS Software Security Hardening Release: October 2026

Security fixes in Release 6.0(2.260067) — None

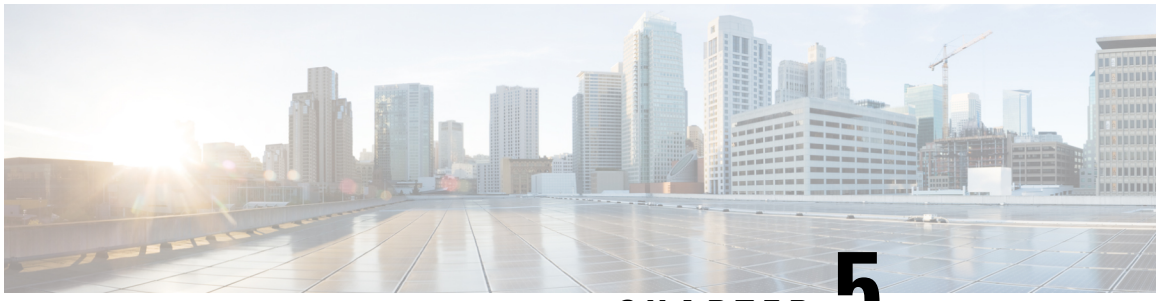
Security fixes in Release 6.0(1.260006) — None

Security fixes in Release 6.0(2.260045) — None

Security fixes in Release 6.0(1.260003) — None

Security fixes in Release 6.0(1.250229) — None

Security fixes in Release 6.0(1.250198) — None



CHAPTER 5

Resolved issues

You can view the open issues, resolved issues, and security fixes using the Cisco Bug Search Tool.

- Resolved issues in Release 6.0(2.260080), on page 15
- Resolved issues in Release 6.0(2.260067), on page 16
- Resolved issues in Release 6.0(1.260006), on page 16
- Resolved issues in Release 6.0(2.260045), on page 17
- Resolved issues in Release 6.0(1.260003), on page 18
- Resolved issues in Release 6.0(1.250229) — None, on page 19
- Resolved issues in Release 6.0(1.250198) — None, on page 19

Resolved issues in Release 6.0(2.260080)

This section provides a brief description of the resolved issues.

Defect ID	Description	First Version Affected	Resolved in Release
CSCwt48678	On Cisco UCS X-Series chassis with UCSX-I-9108-100G Intelligent Fabric Modules (IFM), after running the factory reset command `debug platform software cmcctrl factory` to securely erase the embedded MultiMediaCard (eMMC) of an IFM, the IFM may become non-operational immediately following the reboot. When this condition occurs, the IFM becomes offline and no LED indicators are visible, but the chassis Power Supply Unit (PSU) and fans remain operational. There is no workaround after the IFM becomes non-operational. It is recommended to contact Cisco TAC for assistance. This issue is resolved.	4.3(6.250048)	6.0(2.260080)

Resolved issues in Release 6.0(2.260067)

This section provides a brief description of the resolved issues.

Defect ID	Description	First Version Affected	Resolved in Release
CSCwt42965	On Cisco UCS X9508 chassis connected to Cisco Intersight Virtual Appliance, chassis profile deployment may fail when a Simple Network Management Protocol (SNMP) policy is attached to the profile. When this condition occurs, the device SNMP policy deployment fails, and the chassis profile does not fully deploy in Cisco Intersight. This issue is resolved.	4.3(6.250048)	6.0(2.260067) 4.3(6.260036)

Resolved issues in Release 6.0(1.260006)

This section provides a brief description of the resolved issues.

Defect ID	Description	First Version Affected	Resolved in Release
CSCwt36346	On Cisco UCS 6500 Series and 6400 Series Fabric Interconnects, when the allowed VLAN string on the vEth interface exceeds 900 characters, data corruption occurs over time. This eventually causes both Fabric Interconnects to perform a hard reboot. The generic error message `Reset Requested due to Fatal Module Error` is displayed when the `show system reset-reason` command is run. This issue is resolved.	6.0(1.250198)	6.0(1.260006) 6.0(2.260045)
CSCwn65484	Cisco UCS Fabric Interconnects (6400, 6500, 6600 Series, and Cisco UCS X-Series Direct UCS 9108 100G) may generate a missing FCOE_NPV_PKG license warning. The warning message is: %LICMGR-2-LOG_LIC_MISSING_WARNING. Despite this warning, the FCoE feature continues to operate normally under honor-based licensing. This issue is resolved.	4.3(3.240007)	6.0(1.260006)

Resolved issues in Release 6.0(2.260045)

This section provides a brief description of the resolved issues.

Defect ID	Description	First Version Affected	Resolved in Release
CSCwt36346	On Cisco UCS 6500 Series and 6400 Series Fabric Interconnects, when the allowed VLAN string on the vEth interface exceeds 900 characters, data corruption occurs over time. This eventually causes both Fabric Interconnects to perform a hard reboot. The generic error message `Reset Requested due to Fatal Module Error` is displayed when the `show system reset-reason` command is run. This issue is resolved.	6.0(1.250198)	6.0(2.260045) 6.0(1.260006)
CSCwq30478	On Cisco UCS 6400 Fabric Interconnects, the svc_samc_proxy process may repeatedly log dead thread messages in the proxy log. Despite these messages, communication continues without interruption. This issue is resolved.	4.2(3h)	6.0(2.260045)
CSCws79311	When adding multiple UCS domains to Cisco Nexus Dashboard Fabric Controller (NDFC), some Fabric-B names in certain domains appear with the first character missing. This issue affects the display of the Fabric-B name and causes the model column to show only Cisco instead of the full model name. This issue is resolved.	4.3(6.260002)	6.0(2.260045)
CSCwq80370	On Cisco UCS X chassis, the PSU firmware version reported under the Power Subsystem in the Redfish API may show incorrect or inconsistent values compared to the Firmware Inventory or PSUFWUPDATE information. This discrepancy can occur after an ESU firmware update, where the Redfish interface displays outdated or partial firmware versions, while the actual primary and secondary firmware versions differ. This issue is resolved.	6.0(1.250229)	6.0(2.260045)

Defect ID	Description	First Version Affected	Resolved in Release
CSCws91466	IOMs in UCS domain report a CMCLowMem warning related to high usage of the /var/volatile/wtmp file, which grows due to repeated FI connections triggering rlogin. The wtmp file consumes about 1.4 GB of space, but no other service impact is observed. This issue is resolved.	4.3(6.250048)	6.0(2.260045) 4.3(6.260026)
CSCwr55882	After performing an FI upgrade, fabric evacuation on IOM backplane ports may not turn off because some servers remain in a rediscovery state. This causes affected backplane ports to stay down, while others in the domain may come up normally. The issue typically occurs when fabric evacuation is manually enabled before the upgrade and after the first Fabric Interconnect completes the upgrade. This issue is resolved.	4.3(5.240032)	6.0(2.260045)
CSCwt11034	Cisco UCS 6400 series FIs show a warning about missing identity files and prompt for a user password when remote users connect to the peer fabric NXOS. The warning indicates that the SSH identity file is not accessible. This issue is resolved.	6.0(1.260003)	6.0(2.260045)

Resolved issues in Release 6.0(1.260003)

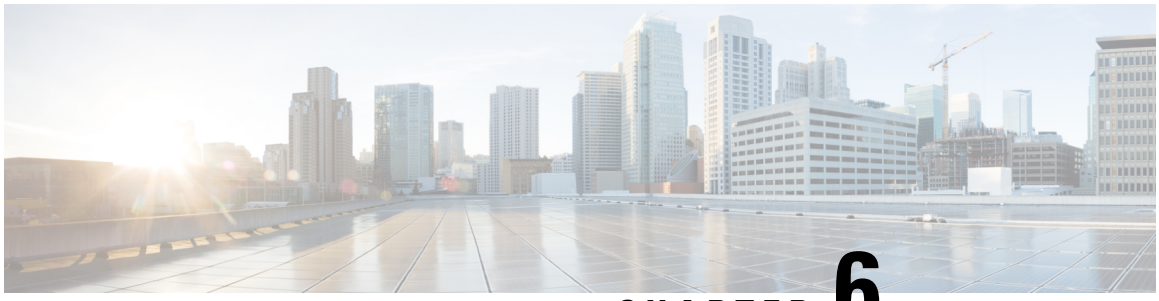
This section provides a brief description of the resolved issues.

Defect ID	Description	First Version Affected	Resolved in Release
CSCws83445	On Cisco UCS 6664 Fabric Interconnects, certain unified ports failed to come up. This issue occurred on devices reporting a hardware changes bit value of 0x0 in the supervisor SPROM. Only ports 1/25, 1/28, 1/29, 1/36, 1/37, and 1/40 will be operational; all other ports might not link-up or encounter issues even when up and should be disabled until the device is upgraded to 6.0(1.260003) or later. This issue affects both Ethernet and Fibre Channel ports and is not resolved by RMA, as hardware replacement without a firmware update will not correct the problem.	6.0(2.250085)	6.0(1.260003)

Resolved issues in Release 6.0(1.250229) — None

Resolved issues in Release 6.0(1.250198) — None

Resolved issues in Release 6.0(1.250198) — None



CHAPTER 6

Open issues

You can view the open issues, resolved issues, and security fixes using the Cisco Bug Search Tool.

- Open issues in Release 6.0(2.260080) — None, on page 21
- Open issues in Release 6.0(2.260067) — None, on page 21
- Open issues in Release 6.0(1.260006) — None , on page 21
- Open issues in Release 6.0(2.260045), on page 21
- Open issues in Release 6.0(1.260003) — None, on page 23
- Open issues in Release 6.0(1.250229), on page 23
- Open issues in Release 6.0(1.250198), on page 23

Open issues in Release 6.0(2.260080) — None

Open issues in Release 6.0(2.260067) — None

Open issues in Release 6.0(1.260006) — None

Open issues in Release 6.0(2.260045)

This section provides a brief description of the open issues.

Defect ID	Description	Workaround	First Version Affected
CSCwp18495	On Cisco UCS X-Direct Fabric Interconnects, tech support collection is slower than on other platforms and may take over one hour when initiated through Intersight. This is due to the bundling of NXOS and CMC tech supports for both Fabric Interconnects, as well as slower memory access on the CPU compared to the 6500, 6400, and 6600 series FIs. Other Fabric Interconnect platforms are not affected. There is no functional impact due to this issue.	There is no workaround.	6.0(2.260045)
CSCwt15440	Fabric Interconnect (FI) ports using 64G Fibre Channel (FC) SFPs may experience incrementing input discards and errors, leading to `errDisabled` state due to high bit error rates when configured at 16G speed in FC Switch mode. Additionally, FC Name Server (FCNS) entries for targets connected to MDS switches may show empty vendor names on the FI. This issue occurs when FC ports on Cisco UCS 6652 FI use 64G FC SFPs but are set to operate at 16G speed while sending FCoE traffic across multiple VSANs.	Use 16G or 32G SFP.	6.0(2.260045)

Open issues in Release 6.0(1.260003) — None

Open issues in Release 6.0(1.250229)

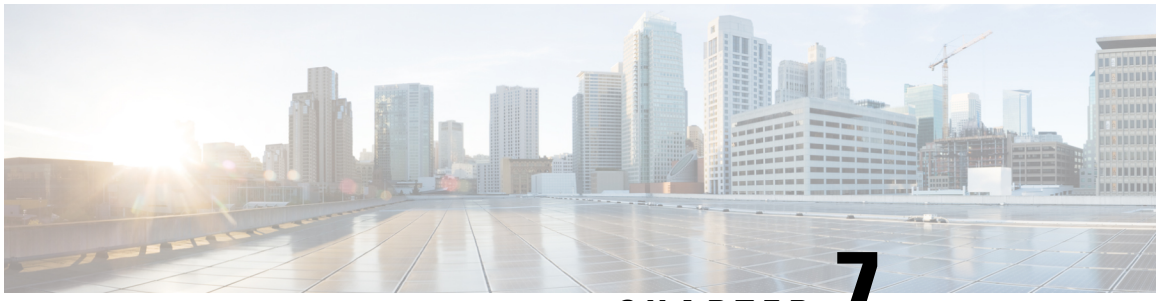
This section provides a brief description of the open issues.

Defect ID	Description	Workaround	First Version Affected
CSCwr31737	On Cisco UCSX-9508 chassis configured with a Cisco UCS X580p PCIe Node, changing from a higher to a lower available power policy can cause one or more servers or GPUs to receive insufficient or no power. This may result in affected servers or GPUs shutting down, or the system becoming oversubscribed and at risk of a chassis brownout. Additionally, GPUs may continue to stay 'On' even when power is not allocated to the paired Cisco UCS X-Series server or the GPU server. This can lead to inaccurate status reporting and potential operational issues.	1. Do not change the power policy from a higher available power setting to a lower one. 2. If the policy is changed accidentally, revert to the original setting.	6.0(1.250229)

Open issues in Release 6.0(1.250198)

This section provides a brief description of the open issues.

Defect ID	Description	Workaround	First Version Affected
CSCwt36346	On Cisco UCS 6500 Series and 6400 Series Fabric Interconnects, when the allowed VLAN string on the vEth interface exceeds 900 characters, data corruption occurs over time. This eventually causes both Fabric Interconnects to perform a hard reboot. The generic error message `Reset Requested due to Fatal Module Error` is displayed when the `show system reset-reason` command is run.	Configure all vEth interfaces so that their allowed VLAN string length is 900 characters or less.	6.0(1.250198)
CSCwo44245	On UCS FI 6664, Fibre Channel (FC) ports using 64G SFP modules may go into an error-disabled state due to high bit error rates when configured at 16G speed.	Use 16G or 32G SFP modules instead of 64G SFP when configuring the port at 16G speed.	6.0(1.250071)



CHAPTER 7

Known issues

- Known issues in Release 6.0(2.260080) — None, on page 25
- Known issues in Release 6.0(2.260067) — None, on page 25
- Known issues in Release 6.0(1.260006) — None, on page 25
- Known issues in Release 6.0(2.260045), on page 25
- Known issues in Release 6.0(1.260003) — None, on page 26

Known issues in Release 6.0(2.260080) — None

Known issues in Release 6.0(2.260067) — None

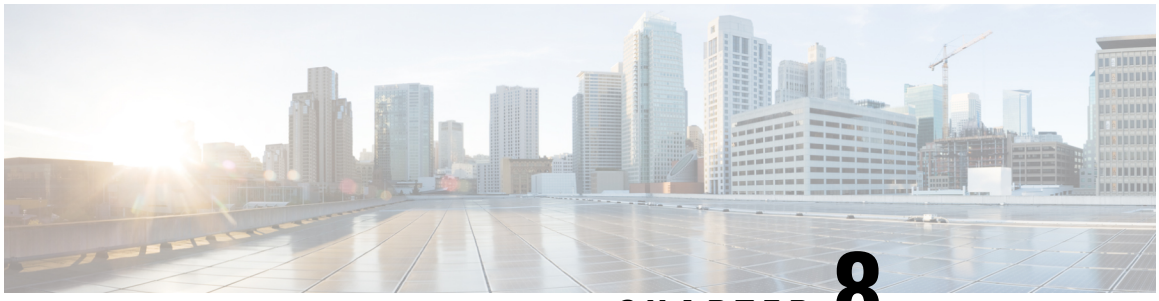
Known issues in Release 6.0(1.260006) — None

Known issues in Release 6.0(2.260045)

This section provides a brief description of the known issues.

Defect ID	Description	Workaround	First Version Affected
CSCwr50750	On Cisco UCS Fabric Interconnects Series 6600, 6500, 6400, and X-Series Direct Fabric Interconnects, when the management interface is configured with IPv6, a syslog message is displayed if the device receives a Router Advertisement (RA) packet containing an ICMPv6 MTU option greater than 1500 bytes. This message indicates an MTU mismatch but does not impact functionality.	No workaround is required; the syslog message can be safely ignored.	6.0(1.250223)

Known issues in Release 6.0(1.260003) — None



CHAPTER 8

Compatibility

- Cross-Version Firmware Support, on page 27
- Cisco UCS NVMeoF Support Matrix for Third-Party Storage Vendors, on page 30
- Compatibility and Support Matrix for Cisco Fabric Interconnects and MDS Switches, on page 33
- Compatibility and Support Matrix for Cisco Fabric Interconnects and Nexus Switches, on page 34
- Compatibility and Support Matrix for Cisco Fabric Interconnects and Brocade Switches, on page 34
- Support Matrix for Cisco Fabric Interconnects Appliance Ports, on page 35
- Deprecated Hardware, on page 35

Cross-Version Firmware Support

Note The three-part version number format, such as 4.3(6) or 6.0(1), represents a general version series. For example, 4.3(6) indicates all firmware versions that start with 4.3(6), encompassing detailed subversions such as 4.3(6.260058) and 4.3(6.260054). Similarly, 6.0(1) indicates all firmware versions that start with 6.0(1), encompassing detailed subversions such as 6.0(1.260003) and 6.0(1.250127). For detailed information about specific firmware versions and their equivalencies across Cisco Intersight, Cisco Integrated Management Controller (Cisco IMC), and Cisco UCS Manager, see the Cisco UCS Equivalency Matrix.

X-Series Server Firmware Version	Infrastructure Firmware Version										
	4.1(3)	4.2(1)	4.2(2)	4.2(3)	4.3(2)	4.3(3)	4.3(4)	4.3(5)	4.3(6)	6.0(1)	6.0(2)
6.0(2)	N/A	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
6.0(1)	N/A	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
5.4(0)	N/A	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
5.3(0)	N/A	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
5.2(2)	N/A	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
5.2(1)	N/A	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

5.2(0)	N/A	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
5.1(1)	N/A	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
5.1(0)	N/A	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
5.0(4)	N/A	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
5.0(2)	N/A	Yes	Yes	Yes	No	No	No	No	No	No	No
5.0(1)	N/A	Yes	Yes	Yes	No	No	No	No	No	No	No

C-Series Server Firmware Version	**Infrastructure Firmware Version**										
	4.1(3)	**4.2(1)**	**4.2(2)**	**4.2(3)**	**4.3(2)**	**4.3(3)**	**4.3(4)**	**4.3(5)**	**4.3(6)**	**6.0(1)**	**6.0(2)**
6.0(2)	No	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
6.0(1)	No	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
4.3(6)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
4.3(5)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
4.3(4)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
4.3(3)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
4.3(2)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
4.3(1)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
4.2(3)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
4.2(2)	Yes	Yes	Yes	Yes	No	No	No	No	No	No	No
4.2(1)	Yes	Yes	Yes	Yes	No	No	No	No	No	No	No
4.1(3)	Yes	Yes	Yes	Yes	No	No	No	No	No	No	No

B-Series Server Firmware Version	**Infrastructure Firmware Version**										
	4.1(3)	**4.2(1)**	**4.2(2)**	**4.2(3)**	**4.3(2)**	**4.3(3)**	**4.3(4)**	**4.3(5)**	**4.3(6)**	**6.0(1)**	**6.0(2)**
6.0(2)	No	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
6.0(1)	No	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
5.4(0)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
5.3(0)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
5.2(2)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

5.2(1)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
5.2(0)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
5.1(0)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
4.3(3)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
4.3(2)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
4.2(3)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
4.2(2)	Yes	Yes	Yes	Yes	No	No	No	No	No	No	No
4.2(1)	Yes	Yes	Yes	Yes	No	No	No	No	No	No	No
4.1(3)	Yes	Yes	Yes	Yes	No	No	No	No	No	No	No

Cisco UCS NVMeoF Support Matrix for Third-Party Storage Vendors

Storage Vendor	Feature	Storage Array	Cisco UCS FI	Cisco UCS VIC	Operating System
NetApp Inc.®	NVMe-FC	ONTAP 9.16 onwards	Cisco UCS 6664 FI, Cisco UCS 6652 FI	15000, 14000	ESXi 8.0 U3+, ESXi 9.0+, RHEL 9.6+, RHEL 10+, SLES 15SP5+
		ONTAP 9.15 onwards	Cisco UCS 6400 series, Cisco UCS 6536 FI	1400/14000, 15000	ESXi 8.0 U3+, ESXi 9.0+, RHEL 9.6+, RHEL 10+, SLES 15SP5+
		ONTAP 9.15 onwards	Cisco UCS X-Direct	15000	ESXi 8.0 U3+, ESXi 9.0+, RHEL 9.6+, RHEL 10+, SLES 15SP5+
	NVMe-TCP	ONTAP 9.16 onwards	Cisco UCS 6664 FI, Cisco UCS 6652 FI	15000, 14000	ESXi 8.0 U3+, ESXi 9.0+, RHEL 9.6+, RHEL 10+, SLES 15SP5+
		ONTAP 9.15 onwards	Cisco UCS 6400 series, Cisco UCS 6536 FI	1400/14000/15000	ESXi 8.0 U3+, ESXi 9.0+, RHEL 9.6+, RHEL 10+, SLES 15SP5+
		ONTAP 9.15 onwards	Cisco UCS X-Direct	15000	ESXi 8.0 U3+, ESXi 9.0+, RHEL 9.6+, RHEL 10+, SLES 15SP5+

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	FlashArray//C, FlashArray//X, FlashArray//XL	Cisco UCS 6652 FI Cisco UCS 6664 FI	15000, 14000	ESXi 8.0 U3+, ESXi 9.0+, RHEL 9.6+, RHEL 10+, SLES 15SP5+
		FlashArray//C, FlashArray//X, FlashArray//XL	Cisco UCS 6400 series, Cisco UCS 6536 FI	1400/14000, 15000	ESXi 8.0 U3+, ESXi 9.0+, RHEL 9.6+, RHEL 10+, SLES 15SP5+
		FlashArray//C, FlashArray//X, FlashArray//XL	Cisco UCS X-Direct	15000	ESXi 8.0 U3+, ESXi 9.0+, RHEL 9.6+, RHEL 10+, SLES 15SP5+
	NVMe-ROCEv2	FlashArray//C, FlashArray//X, FlashArray//XL	Cisco UCS 6652 FI	15000, 14000	ESXi 8.0 U3+, ESXi 9.0+, RHEL 9.6+, RHEL 10+
		FlashArray//C, FlashArray//X, FlashArray//XL	Cisco UCS 6664 FI	15000, 14000	ESXi 8.0 U3+, ESXi 9.0+, RHEL 9.6+, RHEL 10+
		FlashArray//C, FlashArray//X, FlashArray//XL	Cisco UCS 6400 series, Cisco UCS 6536 FI	1400/14000, 15000	ESXi 8.0 U3+, ESXi 9.0+, RHEL 9.6+, RHEL 10+
		FlashArray//C, FlashArray//X, FlashArray//XL	Cisco UCS X-Direct	15000	ESXi 8.0 U3+, ESXi 9.0+, RHEL 9.6+, RHEL 10+
	NVMe-TCP	FlashArray//C, FlashArray//X, FlashArray//XL	Cisco UCS 6652 FI	15000, 14000	ESXi 8.0 U3+, ESXi 9.0+, RHEL 9.6+, RHEL 10+, SLES 15SP5+
		FlashArray//C, FlashArray//X, FlashArray//XL	Cisco UCS 6664 FI	15000, 14000	ESXi 8.0 U3+, ESXi 9.0+, RHEL 9.6+, RHEL 10+, SLES 15SP5+

Storage Vendor	Feature	Storage Array	Cisco UCS FI	Cisco UCS VIC	Operating System
		FlashArray//C, FlashArray//X, FlashArray//XL	Cisco UCS 6400 series, Cisco UCS 6536 FI	1400/14000, 15000	ESXi 8.0 U3+, ESXi 9.0+, RHEL 9.6+, RHEL 10+, SLES 15SP5+
		FlashArray//C, FlashArray//X, FlashArray//XL	Cisco UCS X-Direct	15000	ESXi 8.0 U3+, ESXi 9.0+, RHEL 9.6+, RHEL 10+, SLES 15SP5+
Dell Inc.®	NVMe-FC	PowerStore, PowerMax	Cisco UCS 6664 FI, Cisco UCS 6652 FI	15000, 14000	ESXi 8.0 U3+, ESXi 9.0+, RHEL 9.6+, RHEL 10+, SLES 15SP5+
		PowerStore, PowerMax	Cisco UCS 6400 series, Cisco UCS 6536 FI	1400/14000, 15000	ESXi 8.0 U3+, ESXi 9.0+, RHEL 9.6+, RHEL 10+, SLES 15SP5+
		PowerStore, PowerMax	Cisco UCS X-Direct	15000	ESXi 8.0 U3+, ESXi 9.0+, RHEL 9.6+, RHEL 10+, SLES 15SP5+
	NVMe-TCP	PowerStore, PowerMax	Cisco UCS 6664 FI, Cisco UCS 6652 FI	15000, 14000	ESXi 8.0 U3+, ESXi 9.0+, RHEL 9.6+, RHEL 10+, SLES 15SP5+
		PowerStore, PowerMax	Cisco UCS 6400 series, Cisco UCS 6536 FI	1400/14000, 15000	ESXi 8.0 U3+, ESXi 9.0+, RHEL 9.6+, RHEL 10+, SLES 15SP5+
		PowerStore, PowerMax	Cisco UCS X-Direct	15000	ESXi 8.0 U3+, ESXi 9.0+, RHEL 9.6+, RHEL 10+, SLES 15SP5+

Storage Vendor	Feature	Storage Array	Cisco UCS FI	Cisco UCS VIC	Operating System
Hitachi, Ltd. ®	NVMe-TCP	Hitachi VSP One Block 85	UCSX S9108 (EHM)	15000	ESXI 9.0+
	NVMe-TCP	Hitachi VSP One Block 24			
	NVMe-TCP	Hitachi VSP One Block 26			
	NVMe-TCP	Hitachi VSP One Block 28			

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

Compatibility and Support Matrix for Cisco Fabric Interconnects and MDS Switches

Fabric Interconnect and MDS Support Matrix

Fabric Interconnect	Older Supported Release of MDS	Recommended release of MDS
UCS-FI-6652	9.2	9.4
UCS-FI-6664	9.2	9.4
UCS-FI-6536	9.2	9.4
UCS-FI-6454	9.2	9.4
UCS-FI-64108	9.2	9.4
UCSX-S9108-100G	—	9.4

Note For older supported release only MDS recommended minor version are supported. For more information, see Recommended Releases for Cisco MDS 9000 Series Switches.

Compatibility and Support Matrix for Cisco Fabric Interconnects and Nexus Switches

Fabric Interconnect and Nexus Switch Support Matrix

Fabric Interconnect	Older Supported Release of NX-OS	Recommended release of NX-OS
UCS-FI-6652	—	10.5(x)
UCS-FI-6664	—	10.5(x)
UCS-FI-6536	—	10.5(x)
UCS-FI-6454	—	10.5(x)
UCS-FI-64108	—	10.5(x)
UCSX-S9108-100G	—	10.5(x)

Compatibility and Support Matrix for Cisco Fabric Interconnects and Brocade Switches

Fabric Interconnect and Brocade Switch Support Matrix

Cisco UCS Fabric Interconnect	Older Supported Release of Brocade	Recommended release of Brocade
UCS-FI-6652	—	9.2
UCS-FI-6664	—	9.2
UCS-FI-6536	—	9.2
UCS-FI-6454	—	9.2
UCS-FI-64108	—	9.2
UCSX-S9108-100G	—	9.2

Support Matrix for Cisco Fabric Interconnects Appliance Ports

Fabric Interconnect Appliance Port Support Matrix

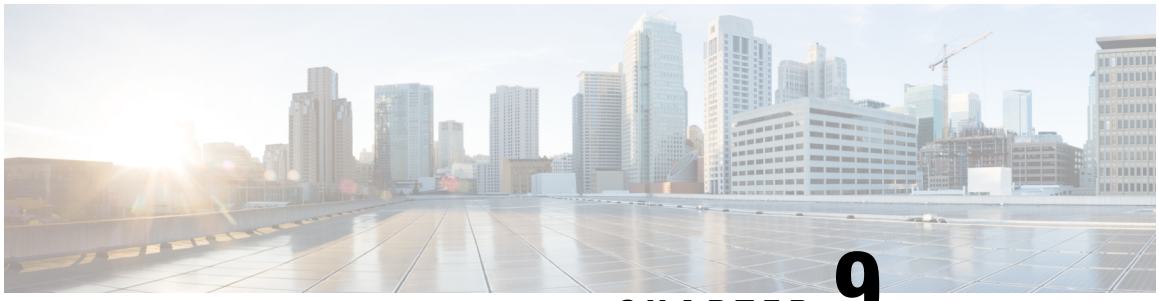
Protocol	Partner	Partner Support	Cisco Support
NVMe-TCP	NetApp (ONTAP)	Supported	Supported
	DELL EMC	Supported	Supported
	Pure	Supported	Supported
RoCE v2	NetApp (ONTAP)	Not Supported	Not Supported
	DELL EMC	Not Supported	Not Supported
	Pure	Not Supported	Not Supported
iSCSI	NetApp (ONTAP)	Supported	Supported
	DELL EMC	Supported	Supported
	Pure	Supported	Supported

Deprecated Hardware

Release 6.0(1)

Beginning with Intersight Infrastructure Firmware Release 6.0(1), the following hardware is no longer supported:

- IOM Models:
  - UCS-IOM-2208XP
  - UCS-IOM-2204XP
  - UCS-IOM-2304
  - UCS-IOM-2304V2
- FEX Models:
  - N2K-C2232PP-10GE



CHAPTER 9

Related resources

- Related resources, on page 37

Related resources

- Release Notes and Release Bundles for Cisco Intersight
- Cisco UCS Equivalency Matrix for Cisco Intersight, Cisco IMC, and Cisco UCS Manager
- Release Notes for Cisco UCS Manager
- Release Notes for Cisco UCS Rack Server Software
- Cisco Baseboard Management Controller Release Notes for Cisco UCS C885A M8 Rack Server
- Cisco UCS Manager and Intersight Release Strategy

Related resources

© 2025–2026 Cisco Systems, Inc. All rights reserved.