Release Notes for Cisco UCS Manager, Release 4.3

First Published: 2023-08-17

Last Modified: 2026-08-17

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

Deprecation Notice

Deprecated Releases 4.3(4a), 4.3(4b), 4.3(4c), and 4.3(4d)

Releases 4.3(4a), 4.3(4b), 4.3(4c), and 4.3(4d) are deprecated and firmware files are no longer available.

Cisco recommends that you upgrade to release 4.3(4e) or later. For more information, refer to the Deferral Notices:

- https://www.cisco.com/c/en/us/support/docs/field-notices/742/fn74201.html
- https://www.cisco.com/c/en/us/support/docs/field-notices/742/fn74209.html

Revision History

Table 1: Release 4.3(6)

Release	Date	Description
4.3(6i)	August 17, 2026	Created release notes for Cisco UCS Manager Release 4.3(6i).

Release	Date	Description
4.3(6h)	June 25, 2026	Created release notes for Cisco UCS Manager Release 4.3(6h).
4.3(6g)	May 4, 2026	Created release notes for Cisco UCS Manager Release 4.3(6g).
4.3(6f)	March 26, 2026	Updated Security Fixes in Release 4.3(6f), on page 33.
4.3(6f)	February 23, 2026	Created release notes for Cisco UCS Manager Release 4.3(6f).
4.3(6e)	January 14, 2026	Created release notes for Cisco UCS Manager Release 4.3(6e).
4.3(6c)	December 09, 2025	Added CSCws30219 under Open Caveats for Release 4.3(6c), on page 99.
4.3(6d)	October 28, 2025	Created release notes for Cisco UCS Manager Release 4.3(6d).
4.3(6c)	August 28, 2025	Updated Cisco UCS NVMeoF Support Matrix for 3rd Party Storage Vendors, on page 138.
4.3(6c)	July 07, 2025	Created release notes for Cisco UCS Manager Release 4.3(6c).
4.3(6b)	May 22, 2025	Created release notes for Cisco UCS Manager Release 4.3(6b).
4.3(6a)	April 30, 2025	Created release notes for Cisco UCS Manager Release 4.3(6a).

Table 2: Release 4.3(5)

Release	Date	Description
4.3(5c)	April 02, 2025	Updated Security Fixes in Release 4.3(5c), on page 40.
4.3(5d)	March 25, 2025	Created release notes for Cisco UCS Manager Release 4.3(5d).
4.3(5c)	February 21, 2025	Added Compatibility and Support Matrix for Cisco Fabric Interconnects and Nexus Switches, on page 144.
4.3(5c)	January 16, 2025	Created release notes for Cisco UCS Manager Release 4.3(5c).

Release	Date	Description
4.3(5a)	October 22, 2024	Created release notes for Cisco UCS Manager Release 4.3(5a).

Table 3: Release 4.3(4)

Release	Date	Description
4.3(4f)	December 16, 2024	Created release notes for Cisco UCS Manager Release 4.3(4f).
4.3(4e)	November 13, 2024	Deprecated releases 4.3(4a), 4.3(4b), 4.3(4c), and 4.3(4d).
4.3(4e)	October 28, 2024	Created release notes for Cisco UCS Manager Release 4.3(4e).
4.3(4d)	October 07, 2024	Created release notes for Cisco UCS Manager Release 4.3(4d).
4.3(4c)	September 01, 2024	Created release notes for Cisco UCS Manager Release 4.3(4c).
4.3(4b)	July 25, 2024	Cisco UCS Manager introduces support for Cisco UCS X-Series Direct.
4.3(4a)	July 03, 2024	Added CSCwd35712 under Resolved Caveats in Release 4.3(4a), on page 85.
4.3(4b)	June 25, 2024	Created release notes for Cisco UCS Manager Release 4.3(4b).
4.3(4a)	June 05, 2024	Created release notes for Cisco UCS Manager Release 4.3(4a).

Table 4: Release 4.3(3)

Release	Date	Description
4.3(3a)	May 08, 2024	Updated New Hardware in Release 4.3(3a), on page 20.
4.3(3c)	April 22, 2024	Created release notes for Cisco UCS Manager Release 4.3(3c).
4.3(3a)	March 08, 2024	Updated Cisco UCS NVMeoF Support Matrix for 3rd Party Storage Vendors, on page 138.

Release	Date	Description
4.3(3a)	February 15, 2024	Created release notes for Cisco UCS Manager Release 4.3(3a).

Table 5: Release 4.3(2)

Release	Date	Description
4.3(2f)	October 23, 2024	Created release notes for Cisco UCS Manager Release 4.3(2f).
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).
4.3(2b)	August 16, 2023	Created release notes for Cisco UCS Manager Release 4.3(2b).

What's New

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(6i), on page 6
- New Hardware in Release 4.3(6g)—None
- New Hardware in Release 4.3(6f)—None
- New Hardware in Release 4.3(6e)—None
- New Hardware in Release 4.3(6d)—None
- New Hardware in Release 4.3(6c), on page 7
- New Hardware in Release 4.3(6b)—None
- New Hardware in Release 4.3(6a), on page 7
- New Hardware in Release 4.3(5d)—None
- New Hardware in Release 4.3(5c), on page 13
- New Hardware in Release 4.3(5a), on page 15
- New Hardware in Release 4.3(4f)—None
- New Hardware in Release 4.3(4e)—None
- New Hardware in Release 4.3(4d)—None
- New Hardware in Release 4.3(4c)—None

- New Hardware in Release 4.3(4b), on page 18
- New Hardware in Release 4.3(4a), on page 19
- New Hardware in Release 4.3(3c)—None
- New Hardware in Release 4.3(3a), on page 20
- New Hardware in Release 4.3(2f)—None
- New Hardware in Release 4.3(2e)—None
- New Hardware in Release 4.3(2c), on page 23
- New Hardware in Release 4.3(2b), on page 24

New Software Features

- New Software in Release 4.3(6i)—None
- New Software in Release 4.3(6h)—None
- New Software in Release 4.3(6g)—None
- New Software in Release 4.3(6f)—None
- New Software in Release 4.3(6e)—None
- New Software in Release 4.3(6d)—None
- New Software in Release 4.3(6c)—None
- New Software in Release 4.3(6b)—None
- New Software Feature in Release 4.3(6a), on page 29
- New Software Feature in Release 4.3(5d), on page 29
- New Software Feature in Release 4.3(5c), on page 29
- New Software Feature in Release 4.3(5a), on page 30
- New Software in Release 4.3(4f)—None
- New Software in Release 4.3(4e)—None
- New Software in Release 4.3(4d)—None
- New Software in Release 4.3(4c)—None
- New Software Feature in Release 4.3(4b)—None
- New Software Feature in Release 4.3(4a), on page 30
- New Software Feature in Release 4.3(3c), on page 31
- New Software Feature in Release 4.3(3a)—None
- New Software in Release 4.3(2f)—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 32

New Hardware in Release 4.3

New Hardware in Release 4.3(6i)

Added support for the following DIMMs:

Model	Description	Cisco PID
MDRR448QDBC2	16GB 1Rx8 DDR5-6400 RDIMM	UCS-MRX16G1RE5
MDRR544QDBC2	32GB DDR5-6400 RDIMM 1Rx4 (16Gb)	UCS-MRX32G1RE5
MDRR644QDBC2	64GB 2Rx4 DDR5-6400 RDIMM	UCS-MRX64G2RE5
MDRRWM4QDBC2	96GB 2Rx4 DDR5-6400 RDIMM	UCS-MRX96G2RF5
M321RAJA0MB2-CCP	128GB 2Rx4 DDR5-6400 RDIMM	UCS-MR128G2RG5
M321R2GA3PB2-CCP	16GB 1Rx8 DDR5-6400 RDIMM	UCS-MRX16G1RE5
M321R4GA0PB2-CCP	32GB 1Rx4 DDR5-6400 RDIMM	UCS-MRX32G1RE5
M321R8GA0PB2-CCP	64GB 2Rx4 DDR5-6400 RDIMM	UCS-MRX64G2RE5
M321RYGA0PB2-CCP	96GB 2Rx4 DDR5-6400 RDIMM	UCS-MRX96G2RF5
HMCG78AHBRA	16GB 1Rx8 DDR5-6400 RDIMM	UCS-MRX16G1RE5
HMCG84AHBRA	32GB 1Rx4 DDR5-6400 RDIMM	UCS-MRX32G1RE5
HMCG94AHBRA	64GB 2Rx4 DDR5-6400 RDIMM	UCS-MRX64G2RE5
HMCGM4BHBRB	96GB DDR5-6400 RDIMM 2Rx4 (24Gb)	UCS-MRX96G2RF5
HMCT04MHBRC	128GB 2Rx4 DDR5-6400 RDIMM	UCS-MR128G2RG5
HMCG78CHBRA	16GB DDR5-6400 RDIMM	UCS-MRX16G1RE5
HMCG84CHBRA	32GB DDR5-6400 RDIMM	UCS-MRX32G1RE5
HMCG94CHBRA	64GB DDR5-6400 RDIMM	UCS-MRX64G2RE5
HMCGM4MHBRB	96GB 2Rx4 DDR5-6400 RDIMM	UCS-MRX96G2RF5
MTC10F1084S1RC64BD2	16GB 1Rx8 DDR5-6400 RDIMM	UCS-MRX16G1RE5
MTC20F1045S1RC64BD2	32GB 1Rx4 DDR5-6400 RDIMM	UCS-MRX32G1RE5
MTC40F2046S1RC64BD2	64GB 2Rx4 DDR5-6400 RDIMM	UCS-MRX64G2RE5

Model	Description	Cisco PID
MTC40F204WS1RC64BC1	96GB 2Rx4 DDR5-6400 RDIMM	UCS-MRX96G2RF5
MTC40F2047S1RC64BB1	128GB 2Rx4 DDR5-6400 RDIMM	UCS-MR128G2RG5
MTC10F1084S1RC64BH1	16GB 1Rx8 DDR5-6400 RDIMM	UCS-MRX16G1RE5
MTC20F1045S1RC64BH1	32GB 1Rx4 DDR5-6400 RDIMM	UCS-MRX32G1RE5
MTC40F2046S1RC64BH1	64GB 2Rx4 DDR5-6400 RDIMM	UCS-MRX64G2RE5

New Hardware in Release 4.3(6c)

Added support for NVIDIA H200-NVL GPU (UCSC-GPU-H200-NVL) on Cisco UCS C240 M8 servers.

Cisco UCS Manager introduces dual support for the Cisco Tri-Mode M1 24G RAID (UCSC-RAID-M1L16) controllers on Cisco UCS C245 M8 Servers, enabling independent configuration and management of two controllers within the same server environment.

New Hardware in Release 4.3(6a)

Cisco UCS C240 M8 Server

The 2RU, 2-socket Cisco UCS C240 M8 Rack Server offers I/O flexibility and larger storage capacity. It combines the fastest Intel® processors and is a versatile general-purpose application and infrastructure server delivering leading performance and efficiency for a wide range of workloads, including AI, big-data analytics, databases, collaboration, virtualization, and high-performance computing.

The Cisco UCS C240 M8 Server extends the capabilities of the Cisco UCS rack server portfolio by incorporating Intel Xeon® 6 CPUs. It improves security, performance, and efficiency while helping you achieve your sustainability goals with built-in accelerators such as Intel Trust Domain Extensions (TDX), Intel Data Streaming Accelerator (DSA), Intel QuickAssist Technology (QAT), Intel Advanced Matrix Extensions (AMX), and Intel In-Memory Analytics Accelerator (IAA).

You are able to decrease server Operating Expenses (OpEx) for power and cooling, management, and maintenance by consolidating older servers onto the latest generation of Cisco UCS C240 M8 Server.

The Cisco UCS C240 M8 Server offers the following:

- Processors: Up to 2x Intel Xeon 6700P or 6500P processors (1 or 2)
- Memory
  - 32 DIMM slots (16 DIMMS per CPU): 16, 32, 48, 64, 96, 128, 256GB DDR5 at up to 6400 MT/s for up to 8TB of memory
  - 32, 64GB MRDIMMs at up to 8000 MT/s
- PCIe expansion: Up to 8 PCIe 5.0 slots plus 1 dedicated 24-Gbps RAID controller slot and 1 dedicated mLOM/OCP 3.0 slot
- RAID controllers:
  - Cisco 24-Gbps modular tri-mode RAID controller supports SAS 4 or NVMe hardware RAID
  - Cisco 24-Gbps modular tri-mode SAS Host Bus Adapter (HBA)

- Internal storage:
  - Backplane options: Up to 28 SFF SAS/SATA/U.3 NVMe drives through SAS4 tri-mode RAID or HBA controller, with optional up to eight direct-attach U.2/U.3 NVMe drives
  - Up to 36 E3.S 1T direct-attach NVMe drives
  - Up to 16 LFF SAS HDDs plus optional 4 rear SFF HDD/SSDs
- mLOM/OCP 3.0:
  - One dedicated PCIe Gen5x16 slot that can be used to add an mLOM or OCP 3.0 card for additional rear-panel connectivity
  - mLOM slot can flexibly accommodate 10/25/50 and 40/100/200 Gbps Cisco VIC adapters
  - OCP 3.0 slot features full out-of-band manageability that supports Intel X710 OCP Dual 10GBase-T via mLOM interposer
- Power supplies: Hot-pluggable, redundant platinum and titanium options:
  - Platinum: 1050W DC and 1600W AC
  - Titanium: 1200W AC and 2300W AC
- Other storage:
  - Dedicated Baseboard Management Controller (BMC) FlexMMC for utilities (on board)
  - Dual M.2 SATA SSDs (internal or hot-swappable) with HW RAID support
- GPU: Up to three double-wide or eight single-wide GPUs supported

Cisco UCS Manager supports all the peripherals supported by Cisco UCS C240 M8 Server. For complete list of supported peripherals for Cisco UCS C240 M8 Server, see Cisco UCS C240 M8 SFF Rack Server.

Note Cisco UCS C240 M8 Server supports only Cisco UCS 15000 series secure boot adapters.

Cisco UCS C220 M8 Server

The 1RU, 2-socket Cisco UCS C220 M8 Rack Server is designed to meet the needs of customers that choose to deploy high density rack-mount servers. It combines the latest Intel® processors and is a versatile general-purpose application and infrastructure server delivering leading performance and efficiency for a wide range of workloads, including virtualization, collaboration, and bare-metal applications.

The Cisco UCS C220 M8 Server extends the capabilities of the Cisco UCS rack server portfolio incorporating Intel Xeon® 6 CPUs. It improves security, performance, and efficiency while helping achieve sustainability goals with built-in accelerators the such as Intel Trust Domain Extensions (TDX), Intel Data Streaming Accelerator (DSA), Intel QuickAssist Technology (QAT), Intel Advanced Matrix Extensions (AMX), and Intel In-Memory Analytics Accelerator (IAA).

Operating Expenses (OpEx) for power and cooling, management, and maintenance can be decreased by consolidating older servers onto the latest generation of Cisco UCS C220 M8 Rack Servers.

The Cisco UCS C220 M8 Server is a dense, fault-tolerant server that provides value, performance, and flexibility for both commercial and enterprise customers.

The Cisco UCS C220 M8 Server offers the following:

- Processors: Up to 2x Intel Xeon 6700P or 6500P processors (1 or 2)
- Memory:
  - 32 DIMM slots (16 DIMMS per CPU): 16, 32, 48, 64, 96, 128GB DDR5 at up to 6400 MT/s for up to 4TB of memory
  - 32, 64GB MRDIMMs at up to 8000 MT/s
- PCIe expansion: Up to 3 PCIe 5.0 half-height slots or up to 2 PCIe 5.0 full-height slots plus 1 dedicated 24-Gbps RAID controller slot and 1 dedicated mLOM/OCP 3.0 slot
- RAID controllers:
  - Cisco® 24-Gbps modular tri-mode RAID controller supports SAS 4 or NVMe hardware RAID
  - Cisco 24-Gbps modular tri-mode SAS Host Bus Adapter (HBA)
- Internal storage:
  - Backplane options: Up to 10 SFF SAS/SATA/U.3 NVMe drives through SAS4 tri-mode RAID or HBA controller, with optional up to eight direct-attach U.2/U.3 NVMe drives
  - Up to 16 E3.S 1T direct-attach NVMe drives at PCIe Gen5 x4 each
- mLOM/OCP 3.0:
  - One dedicated PCIe Gen5x16 slot that can be used to add an mLOM or OCP 3.0 card for additional rear-panel connectivity
  - mLOM slot can flexibly accommodate 10/25/50 and 40/100/200 Gbps Cisco VIC adapters
  - OCP 3.0 slot features full out-of-band manageability that supports Intel X710 OCP dual 10GBase-T through mLOM interposer
- Power supplies: Hot-pluggable, redundant platinum, and titanium options:
  - Platinum: 1050W DC and 1600W AC
  - Titanium: 1200W AC and 2300W AC
- Other storage:
  - Dedicated Baseboard Management Controller (BMC) FlexMMC for utilities (on board)
  - Dual M.2 SATA SSDs (internal or hot-swappable) with HW RAID support
- GPU: Up to three single-wide GPUs supported

Cisco UCS Manager supports all the peripherals supported by Cisco UCS C220 M8 Server. For complete list of supported peripherals for Cisco UCS C220 M8 Server, see Cisco UCS C220 M8 SFF Rack Server Spec Sheet.



Note Cisco UCS C220 M8 Server supports only Cisco UCS 15000 series secure boot adapters.

Cisco UCS X210c M8 Compute Node

The Cisco UCS X210c M8 Compute Node is the third 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 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 M8 Compute Node provides these main features:

- Processors: Up to 2x Intel Xeon 6 Scalable Processors (1 or 2)
- Memory: Up to 32 DDR5 DIMM slots (up to 16 DIMMS per CPU)
  - 16, 32, 64, 128, 256GB RDIMM at up to 6400 MT/s
  - Support of 32, 64GB MRDIMM at up to 8000 MT/s
- mLOM: mLOM slot for Cisco UCS VIC 15420 or Cisco VIC 15230
- Mezzanine adapter (rear): Cisco UCS 15422 mezzanine card with UCS VIC 15000 bridge connector compatible with Cisco UCS VIC 15420
- Mezzanine Module (front)
  - EDSFF E3.S NVMe passthrough controller
  - NVMe passthrough controller (for U.2 and U.3 NVMe drives only)
  - RAID controller with 4GB cache (for SSD and mix of SSD and NVMe)
  - GPU front mezzanine
  - No front mezzanine
- Internal storage and GPU
  - Front mezzanine storage options:
    - Up to 9x EDSFF E3.S NVMe drives
    - Up to 6x 2.5-inch SAS and SATA RAID-compatible SSDs
    - Up to 6x 2.5-inch NVMe PCIe drives
    - A mixture of up to six SAS/SATA or NVMe drives
  - Note: Drives require a RAID or passthrough controller in the front mezzanine module slot.
  - Boot drive options:
    - Mini storage module with 2x M.2 (up to 960GB per drive) SATA drives with Hardware RAID

- Mini storage module with 2x M.2 (up to 960GB per drive) NVMe drives in pass-through mode
- GPU options: GPU front mezzanine module with 2x 2.5-inch NVMe drives and 2x GPUs

Cisco UCS Manager supports all the peripherals supported by Cisco UCS X210c M8 Compute Node. For complete list of supported peripherals for Cisco UCS X210c M8 Compute Node, see Cisco UCS X210c M8 Compute Node Spec Sheet.

GPU Support

Extended support for the following existing GPUs:

GPU	Server
NVIDIA A16 GPU on X440p: PCIE 250W 4X16GB, FHFL (UCSX-GPU-A16) (with PCIe Node)	Cisco UCS X210c M8 Compute Node
Intel GPU Flex 140, Gen4x8, HHHL, 75W PCIe (Front Mezz) (UCSX-GPU-FLX140MZ)	
NVIDIA H100-NVL GPU 400W, 94GB, 2-slot FHFL (UCSX-GPU-H100-NVL)	
Intel GPU Flex 140, Gen4x8, HHHL, 75W PCIe (UCSX-GPU-FLEX140)	
Intel GPU Flex 170, Gen4x16, HHFL, 150W PCIe (UCSX-GPU-FLEX170)	
NVIDIA L4 Tensor Core, 70W, 24GB (UCSX-GPU-L4)	
NVIDIA L40S: 350W, 48GB, 2-slot FHFL GPU (UCSX-GPU-L40S) (with PCIe Node)	
NVIDIA H100-NVL GPU 400W, 94GB, 2-slot FHFL (UCSC-GPU-H100-NVL)	Cisco UCS C240 M8 Server
Intel GPU Flex 140, Gen4x8, HHHL, 75W PCIe (UCSC-GPU-FLEX140)	
NVIDIA TESLA A16 PCIE 250W 4X16GB (UCSC-GPU-A16)	
NVIDIA L40S: 350W, 48GB, 2-slot FHFL GPU (UCSC-GPU-L40S)	
NVIDIA L4:70W, 24GB, 1-slot HHHL GPU (UCSC-GPU-L4)	

GPU	Server
Intel GPU Flex 140, Gen4x8, HHHL, 75W PCIe (UCSC-GPU-FLEX140)	Cisco UCS C220 M8 Server
NVIDIA L4:70W, 24GB, 1-slot HHHL GPU (UCSC-GPU-L4)	

Support for the following new GPU:

- AMD MI210 GPU; 300W 64GB, 2 slot FHFL (UCSX-GPU-MI210) with Cisco UCS X215c M8 Compute Node.

Controller Support

Support for the following controllers with Cisco UCS X210c M8 Compute Node:

- 24G Tri-Mode M1 RAID Controller w/4GB FBWC 6Drv (UCSX-RAID-M1L6)
- UCS X10c Compute Pass Through Controller for E3.S (Front) (UCSX-X10C-PTE3)
- UCSX Front UCSX Front panel w/M.2 RAID controller Included for SATA drvpanel with M.2 RAID controller for SATA drives (UCSX-M2I-HWRD-FPS)

Third-Party Adapters

Support for the following NVIDIA OEM adapters with Cisco UCS C220 M8 and C240 M8 servers:

- NVIDIA OEM MCX623436AC-CDAB CX6Dx 2x100G QSFP56 x16 OCP NIC (UCSC-O-N6CD100GFO)
- NVIDIA OEM MCX623106AC-CDAT 2x100 GbE QSFP56 PCIe Crypto Enabled (UCSC-P-M6CD100GFO)
- NVIDIA OEM MCX623106AS-CDAT 2x100 GbE QSFP56 PCIe Crypto Disabled (UCSC-P-M6DD100GFO)
- NVIDIA OEM MCX631432AC-ADAB CX6Lx 2x25G SFP28 x8 OCP NIC (UCSC-O-N6CD25GFO)
- NVIDIA OEM MCX755106AS-HEAT 2x200GbE QSFP112 Gen5x16, PCIe VPI NIC; No Crypto (UCSC-P-N7D200GFO)
- NVIDIA OEM MCX713104AS-ADAT CX-7 4x25GbE SFP56 Gen4 x16 PCIe NIC (UCSC-P-N7Q25GFO)
- NVIDIA OEM MCX715105AS-WEAT CX-7 1x400GbE QSFP112 PCIe Gen5 x16 VPI NIC (UCSC-P-N7S400GFO)
- NVIDIA OEM MCX631102AS-ADAT CX6Lx 2x25GbE SFP28 x8 PCIe NIC (UCSC-P-N6D25GFO)

Support for the following BlueField adapters with Cisco UCS C220 M8 and C240 M8 servers:

- NVIDIA BlueField-3 B3210E DPU 2x100G QSFP112, PCIe Gen5.0 x16, Crypto Disabled (900-9D3B6-00CC-EA0)
- NVIDIA BlueField-3 B3220L SuperNIC 2x200G QSFP112, PCIe Gen5.0 x16, Crypto Disabled (UCSC-P-N3220L)

New Hardware in Release 4.3(5c)

Support for 5th Gen AMD® EPYC® Processors

Support for the following 5th Gen AMD® EPYC® Processors with Cisco UCS C245 M8 servers:

- AMD 9655 2.6GHz 400W 96C/384MB Cache DDR5 6000MT/s (UCS-CPU-A9655)
- AMD 9575F 3.3GHz 400W 64C/256MB Cache DDR5 6000MT/s (UCS-CPU-A9575F)
- AMD 9555 3.2GHz 360W 64C/256MB Cache DDR5 6000MT/s (UCS-CPU-A9555)
- AMD 9355 3.4GHz 280W 32C/256MB Cache DDR5 6000MT/s (UCS-CPU-A9355)
- AMD 9135 3.5GHz 200W 16C/64MB Cache DDR5 6000MT/s (UCS-CPU-A9135)
- AMD 9655P 2.6GHz 400W 96C/384MB Cache DDR5 6000MT/s (UCS-CPU-A9655P)
- AMD 9555P 3.2GHz 360W 64C/256MB Cache DDR5 6000MT/s (UCS-CPU-A9555P)
- AMD 9455P 2.9GHz 300W 48C/256MB Cache DDR5 6000MT/s (UCS-CPU-A9455P)
- AMD 9355P 3.55GHz 280W 32C/256MB Cache DDR5 6000MT/s (UCS-CPU-A9355P)
- AMD 9645 2.0GHz 320W 96C/256MB Cache DDR5 6000MT/s (UCS-CPU-A9645)
- AMD 9455 2.9GHz 300W 48C/256MB Cache DDR5 6000MT/s (UCS-CPU-A9455)
- AMD 9365 3.2GHz 300W 36C/192MB Cache DDR5 6000MT/s (UCS-CPU-A9365)
- AMD 9255 3.2GHz 200W 24C/128MB Cache DDR5 6000MT/s (UCS-CPU-A9255)
- AMD 9015 3.5GHz 155W 8C/64MB Cache DDR5 6000MT/s (UCS-CPU-A9015)
- AMD 9475F 3.6GHz 360W 48C/256MB Cache DDR5 6000MT/s (UCS-CPU-A9475F)
- AMD 9375F 3.7GHz 320W 32C/256MB Cache DDR5 6000MT/s (UCS-CPU-A9375F)
- AMD 9845 2.0GHz 400W 160C/320MB Cache DDR5 6000MT/s (UCS-CPU-A9845)
- AMD 9825 2.0GHz 400W 144C/384MB Cache DDR5 6000MT/s (UCS-CPU-A9825)
- AMD 9745 2.2GHz 400W 128C/256MB Cache DDR5 6000MT/s (UCS-CPU-A9745)
- AMD 9565 3.0GHz 400W 72C/384MB Cache DDR5 6000MT/s (UCS-CPU-A9565)
- AMD 9535 2.1GHz 300W 64C/256MB Cache DDR5 6000MT/s (UCS-CPU-A9535)
- AMD 9335 3.2GHz 210W 32C/128MB Cache DDR5 6000MT/s (UCS-CPU-A9335)
- AMD 9275F 3.9GHz 320W 24C/256MB Cache DDR5 6000MT/s (UCS-CPU-A9275F)
- AMD 9175F 4.2GHz 320W 16C/512MB Cache DDR5 6000MT/s (UCS-CPU-A9175F)
- AMD 9115 3.2GHz 165W 16C/64MB Cache DDR5 6000MT/s (UCS-CPU-A9115)

Support for the following 5th Gen AMD® EPYC® Processors with Cisco UCS C225 M8 servers:

- AMD 9355 3.4GHz 280W 32C/256MB Cache DDR5 6000MT/s (UCS-CPU-A9355)
- AMD 9135 3.5GHz 200W 16C/64MB Cache DDR5 6000MT/s (UCS-CPU-A9135)

- AMD 9655P 2.6GHz 400W 96C/384MB Cache DDR5 6000MT/s (UCS-CPU-A9655P)
- AMD 9555P 3.2GHz 360W 64C/256MB Cache DDR5 6000MT/s (UCS-CPU-A9555P)
- AMD 9355P 3.4GHz 280W 32C/256MB Cache DDR5 6000MT/s (UCS-CPU-A9355P)
- AMD 9825 2.0GHz 390W 144C/384MB Cache DDR5 6000MT/s (UCS-CPU-A9825)
- AMD 9745 2.4GHz 400W 128C/256MB Cache DDR5 6000MT/s (UCS-CPU-A9745)
- AMD 9655 2.6GHz 400W 96C/384MB Cache DDR5 6000MT/s (UCS-CPU-A9655)
- AMD 9565 3.0GHz 400W 72C/384MB Cache DDR5 6000MT/s (UCS-CPU-A9565)
- AMD 9575F 3.3GHz 400W 64C/256MB Cache DDR5 6000MT/s (UCS-CPU-A9575F)
- AMD 9555 3.2GHz 360W 64C/256MB Cache DDR5 6000MT/s (UCS-CPU-A9555)
- AMD 9645 2.0GHz 320W 96C/256MB Cache DDR5 6000MT/s (UCS-CPU-A9645)
- AMD 9455 2.9GHz 300W 48C/256MB Cache DDR5 6000MT/s (UCS-CPU-A9455)
- AMD 9365 3.2GHz 300W 36C/192MB Cache DDR5 6000MT/s (UCS-CPU-A9365)
- AMD 9255 3.2GHz 200W 24C/128MB Cache DDR5 6000MT/s (UCS-CPU-A9255)
- AMD 9015 3.5GHz 155W 8C/64MB Cache DDR5 6000MT/s (UCS-CPU-A9015)
- AMD 9475F 3.6GHz 360W 48C/256MB Cache DDR5 6000MT/s (UCS-CPU-A9475F)
- AMD 9375F 3.7GHz 320W 32C/256MB Cache DDR5 6000MT/s (UCS-CPU-A9375F)
- AMD 9845 2.1GHz 390W 160C/320MB Cache DDR5 6000MT/s (UCS-CPU-A9845)
- AMD 9535 2.1GHz 300W 64C/256MB Cache DDR5 6000MT/s (UCS-CPU-A9535)
- AMD 9335 3.2GHz 210W 32C/128MB Cache DDR5 6000MT/s (UCS-CPU-A9335)
- AMD 9275F 3.9GHz 320W 24C/256MB Cache DDR5 6000MT/s (UCS-CPU-A9275F)
- AMD 9175F 4.2GHz 320W 16C/512MB Cache DDR5 6000MT/s (UCS-CPU-A9175F)
- AMD 9455P 2.9GHz 300W 48C/256MB Cache DDR5 6000MT/s (UCS-CPU-A9455P)
- AMD 9115 3.2GHz 165W 16C/64MB Cache DDR5 6000MT/s (UCS-CPU-A9115)

Support for the following 5th Gen AMD® EPYC® Processors with Cisco UCS X215c M8 Compute Node:

- AMD 9655 2.6GHz 400W 96C/384MB Cache DDR5 6000MT/s (UCS-CPU-A9655)
- AMD 9575F 3.3GHz 400W 64C/256MB Cache DDR5 6000MT/s (UCS-CPU-A9575F)
- AMD 9555 3.2GHz 360W 64C/256MB Cache DDR5 6000MT/s (UCS-CPU-A9555)
- AMD 9355 3.4GHz 280W 32C/256MB Cache DDR5 6000MT/s (UCS-CPU-A9355)
- AMD 9135 3.5GHz 200W 16C/64MB Cache DDR5 6000MT/s (UCS-CPU-A9135)

GPU Support

Support for the following new GPU:

- AMD MI210 GPU; 300W 64GB, 2 slot FHFL (UCSC-GPU-MI210) on Cisco UCS C245 M8 servers

RAID Controllers

Cisco UCS Manager adds support for the following Cisco Tri-Mode M1 24G RAID with Cisco UCS C245 M8 Server and Cisco UCS C225 M8 Server equipped with 5th Gen AMD® EPYC Processors:

- UCSC-RAID-M1L16
- UCSC-RAID-MP1L32

Cisco UCS Manager adds support for the following Cisco Tri-Mode M1 24G RAID and HBA controllers with Cisco UCS C245 M8 Server and Cisco UCS C225 M8 Server equipped with 4th Gen AMD® EPYC Processors:

- UCSC-HBA-M1L16
- UCSC-RAID-M1L16
- UCSC-RAID-MP1L32

New Hardware in Release 4.3(5a)

Cisco UCS X215c M8 Compute Node

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. Powered by the Cisco Intersight™ cloud operations platform, it shifts your thinking from administrative details to business outcomes with hybrid cloud infrastructure that is assembled from the cloud, shaped to your workloads, and continuously optimized.

The Cisco UCS X215c M8 Compute Node is 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, IO, and storage per rack unit in the industry.

The Cisco UCS X215c M8 Compute Node offers the following:

- CPU: Up to 2x 4th Generation AMD EPYC Processors with up to 128 cores per processors
- Memory:
  - 24 DIMM slots (12 DIMMs per CPU socket), up to 4800 MT/s DDR5.
  - Up to 6 TB of capacity.
- 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 (RAID) or pass-through controllers with four lanes each of PCIe Gen 4 connectivity and up to 2 M.2 SATA or NVMe 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 or U.3 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 50Gbps (2 x25Gbps) of unified fabric connectivity to each of the chassis Intelligent Fabric Modules (IFMs) for 100Gbps connectivity per server.
- Cisco UCS Virtual Interface Card (VIC) 15230 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 with secure boot capability.

- Optional Mezzanine card:
  - Cisco UCS Virtual Interface Card (VIC) 15422 can occupy the server's mezzanine slot at the bottom rear of the chassis. An included bridge card extends this VIC's 100Gbps (4 x 25Gbps) of network connections through IFM connectors, bringing the total bandwidth to 100Gbps per VIC 15420 and 15422 (for a total of 200Gbps per server). In addition to IFM connectivity, the VIC 15422 I/O connectors link to Cisco UCS X-Fabric technology.
  - 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: Includes secure boot silicon root of trust FPGA, ACT2 anti-counterfeit provisions, and optional Trusted Platform Model (TPM).

For complete list of supported peripherals for Cisco UCS X215c M8 Compute Node, see Cisco UCS X215c M8 Compute Node Spec Sheet.

Note Cisco UCS X215c M8 Compute Node supports only 15000 Series secure boot VIC adapters.

Cisco UCS C225 M8 Server

The Cisco UCS C225 M8 Server is a versatile general-purpose infrastructure and application server. This high-density, 1RU, single-socket rack server delivers industry-leading performance and efficiency for a wide range of workloads, including virtualization, collaboration, and bare-metal applications.

The Cisco UCS C225 M8 Server extends the capabilities of the Cisco UCS rack server portfolio. It powers 4th Gen AMD EPYC™ Processors with 100 percent more cores per socket designed using AMD's chiplet architecture. With advanced features such as AMD Infinity Guard, compute-intensive applications will see significant performance improvements and reap other benefits such as power and cost efficiencies.

You can deploy the Cisco UCS C225 M8 Server as standalone servers or as part of the Cisco Unified Computing System™ managed by Cisco Intersight® or Cisco UCS Manager to take advantage of Cisco® standards-based unified computing innovations that can help reduce your Total Cost of Ownership (TCO) and increase your business agility.

The C225 M8 rack server brings many new innovations to the Cisco UCS AMD rack server portfolio. With the introduction of PCIe Gen 5.0 for high-speed I/O, a DDR5 memory bus, and expanded storage capabilities, the server delivers significant performance and efficiency gains that will improve your application performance.

The key features of Cisco UCS C225 M8 Server include:

- Supports one 4th Gen AMD EPYC CPU, with up to 128 cores per socket
- Up to 12 DDR5 DIMMs for up to 1.5 TB of capacity using 128 GB DIMMs

- Up to 4800 MT/s DDR5 memory
- Up to 3 PCIe 4.0 slots or up to 2 PCIe 5.0 slots, plus a modular LAN on motherboard (mLOM) / OCP slot 3.0 (details below)
- Support for Cisco UCS VIC 15000 Series adapters as well as a host of third-party NIC options
- UCS C225 M8S chassis: up to 10 SAS/SATA or NVMe disk drives
  - New tri-mode RAID controller supports SAS4 or NVMe hardware RAID
  - Up to 4 direct-attach NVMe SSDs
- UCS C225 M8N chassis: up to 10 direct attach NVMe SSDs
  - All 10 NVMe drives connected at PCIe Gen4 x4
- M.2 boot options
  - Up to two 960GB SATA M.2 drives with hardware RAID, or
  - Up to two 960GB NVMe M.2 drives with NVMe hardware RAID
- Up to three GPUs supported
- Hybrid modular LOM/OCP 3.0
  - One dedicated Gen 4.0 x16 slot that can be used to add an mLOM or OCP 3.0 card for additional rear-panel connectivity
  - mLOM allows for Cisco UCS Virtual Interface Cards (VICs) without consuming a PCIe slot, supporting quad-port 10/25/50 Gbps or dual-port 40/100/200 Gbps network connectivity
  - OCP 3.0 slot features full out-of-band management for select adapters

Cisco UCS Manager supports all the peripherals supported by Cisco UCS C225 M8 Server. For complete list of supported peripherals for Cisco UCS C225 M8 Server, see Cisco UCS C225 M8 SFF Rack Server Spec Sheet.

Note Cisco UCS C225 M8 Server supports only 15000 Series secure boot VIC adapters.

RAID Controllers

Cisco UCS Manager adds support for the following Cisco Tri-Mode M1 24G RAID and HBA controllers on Cisco UCS C-Series M7 servers:

- UCSC-HBA-M1L16 and UCSC-RAID-M1L16 on Cisco UCSC-C220-M7 servers
- UCSC-HBA-M1L16 and UCSC-RAID-MP1L32 on Cisco UCSC-C240-M7 servers

GPU Support

Support for the following new GPUs:

- NVIDIA A16 GPU on X440p: PCIE 250W 4X16GB, FHFL (UCSC-GPU-A16)—Cisco UCS X215c M8 (with PCIe Node).
- NVIDIAH100-NVL GPU 400W, 94GB, 2-slot FHFL (UCSC-GPU-H100-NVL)—Cisco UCS X215c M8 (with PCIe Node), UCS X210c M7, UCS C245 M8, UCS C240 M7.
- NVIDIA L4-Mezz GPU 70W, 24GB, 1-slot HHHL (UCSX-GPU-L4-Mezz)—Cisco UCS X215c M8 and UCS X210c M7.

Extended support for the following existing GPUs:

- NVIDIAL40 300W, 48GB wPWR CBL (UCSC-GPU-L40)—Cisco UCS X215c M8 (with PCIe Node).
- NVIDIA L40S: 350W, 48GB, 2-slot FHFL GPU (UCSC-GPU-L40S)—Cisco UCS X215c M8 (with PCIe Node).
- NVIDIA L4:70W, 24GB, 1-slot HHHL GPU (UCSC-GPU-L4)—Cisco UCS X215c M8 (with PCIe Node).

New Hardware in Release 4.3(4b)

Cisco UCS X-Series Direct®

The Cisco UCS X-Series Direct® simplifies your data center, adapting to the unpredictable needs of modern applications while also providing an edge scaled for remote branch office workloads. It minimizes the IT infrastructure deployed at edge locations to achieve desired business outcomes. As you are looking to increase the number of applications at the edge while deploying as little IT infrastructure as possible, the Cisco UCS X-Series Direct®, powered by Cisco Intersight® and Cisco UCS Manager, enables the benefits of scale together with a secure and unified connectivity.

The Cisco UCS X-Series Direct begins with the Cisco UCS X9508 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. The I/O connectivity modules of the solution are the Cisco UCS X-Series Direct Fabric Interconnect Modules, a unified fabric for Ethernet and Fibre Channel. Additionally, the UCS X9508 chassis can have expanded GPU capabilities using the Cisco UCS X-Fabric technology which interconnects X-series compute and PCIe nodes using high-speed PCIe technology.

For more information see Cisco UCS X-Series Direct Data Sheet.

Cisco UCS C245 M8 Rack Server

The Cisco UCS C245 M8 Server is perfectly suited for a wide range of storage and I/O-intensive applications such as big data analytics, databases, collaboration, virtualization, consolidation, AI/ML and high-performance computing supporting up to two AMD® CPUs in a 2RU form factor.

The Cisco UCS C245 M8 Server extends the capabilities of the Cisco UCS rack server portfolio. With advanced features like AMD Infinity Guard, compute-intensive applications will see significant performance improvements and will reap other benefits such as power and cost efficiencies.

You can deploy the Cisco UCS C-Series rack servers as part of the Cisco Unified Computing System™ managed by Cisco Intersight® or Cisco UCS Manager® to take advantage of Cisco® standards-based unified computing

innovations that can help reduce your Total Cost of Ownership (TCO) and increase your business agility or as standalone servers.

The Cisco UCS C245 M8 Server brings many innovations to the UCS AMD® rack server line. With the introduction of PCIe Gen 5.0 expansion slots for high-speed I/O, a DDR5 memory bus, and expanded storage capabilities, the server delivers significant performance and efficiency gains that will greatly enhance application performance. Features include:

- Support for up to two 4th Gen AMD EPYC™ CPUs in a server designed to drive as much as 256 CPU cores (128 cores per socket)
- Up to 24 DDR5 DIMM slots
- Up to 4800 MT/s DDR5 memory
- Up to 8 x PCIe Gen 4.0 slots or up to 4 x PCIe Gen 5.0 slots, plus a hybrid modular LAN on motherboard (mLOM) /OCP 3.0 slot (details below)
- Support for Cisco UCS VIC 15000 Series adapters as well as a host of third-party NIC options
- Up to 28 hot-swappable small-form-factor (SFF) SAS/SATA or NVMe drives (with up to 8 direct-attach NVMe drives) and New tri-mode RAID controller supports SAS4 plus NVMe hardware RAID.
- M.2 boot options
  - Up to two 960GB SATA M.2 drives with hardware RAID support
  - Up to two 960GB NVMe M.2 drives with NVMe hardware RAID
- Support for up to Eight GPUs
- Modular LOM / OCP 3.0
  - One dedicated PCIe Gen4x16 slot that can be used to add an mLOM or OCP 3.0 card for additional rear-panel connectivity
  - mLOM slot that can be used to install a Cisco UCS Virtual Interface Card (VIC) without consuming a PCIe slot, supporting quad-port 10/25/50 Gbps or dual-port 40/100/200 Gbps network connectivity
  - OCP 3.0 slot that features full out-of-band management for select adapters

Cisco UCS Manager supports all the peripherals supported by Cisco UCS C245 M8 Server. For complete list of supported peripherals for Cisco UCS C245 M8 Server, see Cisco UCS C245 M8 SFF Rack Server Spec Sheet.

Note Cisco UCS C245 M8 Server supports only 15000 Series secure boot VIC adapters.

New Hardware in Release 4.3(4a)

- Support for the following RAID controllers:
  - Cisco Tri-Mode 24G SAS RAID Controller w/4GB Cache (UCSC-RAID-HP) with Cisco UCS C220 M7 and C240 M7 servers.

- Cisco boot optimized M.2 NVMe RAID controller (UCS-M2-NVRAID) with Cisco UCS C220 M7 and C240 M7 servers.

  This controller supports only RAID0, RAID1, or JBOD (default - JBOD) mode and only UEFI boot mode.

- Support for the UCS-TPM-002D TPM module with Cisco UCS X410c M7, X210c M7, X210c M6, B200 M6, C220 M7, C240 M7, C220 M6, and C240 M6 servers.
- Support for the UCS-TPM2-002D TPM module on Cisco UCS C225 M6 and C245 M6 servers.
- Support for Cisco UCSX-440P PCIe Node. For more information, see Cisco UCS X440p PCIe Node Spec Sheet.
- Support for the following GPUs:
  - Intel® Data Center GPU Flex 140, HHHL, 75W PCIe (UCSC-GPU-FLEX140) with Cisco UCS C220 M7 and C240 M7 servers
  - Intel® Data Center GPU Flex 170, FH-3/4L, 150W PCIe (UCSC-GPU-FLEX170) with Cisco UCS C240 M7 servers
  - NVIDIA® 350W, 40GB, 2-Slot FHFL L40S GPU (UCSX-GPU-L40S) on Cisco UCS X440p PCIe Node and Cisco UCS C240 M7 servers
  - NVIDIA® Hopper L4 70W, 24GB, 1-slot HHHL (UCSC-GPU-L4M6) with Cisco UCS C220 and C240 M6 servers
  - NVIDIA® H100 on Cisco UCS X440p PCIe Node, and Cisco UCS C240 M7 servers
- Support for Hynix® 96GB 2Rx4 PC5-5600B-RA0-1010-XT (HMCGM4MGBRB) DIMM with Cisco UCS X410c M7 servers equipped with the following processors:
  - Intel® Xeon® Gold 6416H Processor
  - Intel® Xeon® Gold 6418H Processor
  - Intel® Xeon® Gold 6434H Processor
  - Intel® Xeon® Gold 6448H Processor

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® Platinum 8558 Processor
- Intel® Xeon® Platinum 8558U Processor
- Intel® Xeon® Platinum 8570 Processor
- Intel® Xeon® Platinum 8571N Processor
- Intel® Xeon® Platinum 8581V 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
- Intel® Xeon® Gold 5512U Processor
- Intel® Xeon® Gold 5515+ Processor
- Intel® Xeon® Gold 5520+ Processor
- Intel® Xeon® Gold 6538N Processor
- Intel® Xeon® Silver 4514Y Processor
- Intel® Xeon® Silver 4516Y+ 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 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)

Support for Hynix® 96GB 2Rx4 PC5-5600B-RA0-1010-XT (HMCGM4MGBRB) DIMM with Cisco UCS X410c M7 servers equipped with the following processors:

- Intel® Xeon® Platinum 8444H Processor
- Intel® Xeon® Platinum 8450H Processor
- Intel® Xeon® Platinum 8454H Processor
- Intel® Xeon® Platinum 8460H Processor
- Intel® Xeon® Platinum 8468H Processor
- Intel® Xeon® Platinum 8490H Processor

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(6a)

Cisco UCS Manager adds the following new features:

- Package Power Limit (PPL) feature, aimed at measuring and controlling the power delivered to the CPU socket on the motherboard. This feature is supported only with Cisco UCS C225, C245 M8, and X210c servers. It enhances power management efficiency and ensures optimal power usage by allowing users to configure PPL to Default, Maximum, or Minimum, thereby optimizing server performance and energy efficiency.
- Expanded Forward Error Correction (FEC) capabilities, adding RS Cons 16 and RS 1eee to its existing suite of options which includes Auto, CL74, and CL91. Both RS Cons 16 and RS 1eee FEC options are supported on Cisco Nexus switches and are configurable for 25 Gbps port speed, providing flexibility and enhanced error correction for high-speed networking environments. This enhancement boosts data integrity and transmission reliability for Ethernet and Appliance ports to optimize network performance and efficiency.
- New option in the fan policy of Power Control Policy, **Maximum Cooling**, designed for C-Series servers to optimize cooling efficiency. This option enforces a 100% Pulse Width Modulation (PWM) fan speed, ensuring that CPU temperatures remain as low as possible. You can select this new option in addition to Acoustic, Low Power, Balanced, High Power, and Max Power, offering enhanced control over server cooling strategies.
- Support for PXE Boot in IPv6-only environments using UEFI mode for LAN Boot. This enhancement allows administrators to operate in modern network settings while minimizing the dependency on IPv4 addresses, ensuring efficient server provisioning and management.
- The session timeout setting in Cisco UCS Manager has been updated from **Never** to a default of **30 minutes** for GUI inactivity. This change enhances security by automatically ending inactive sessions. You can still adjust the timeout setting to meet specific security needs.
- Support for the NVMe Management Interface (NVMe-MI) for all Cisco UCS M8 servers. This advancement facilitates seamless integration of next-generation NVMe drives, ensuring robust compatibility and enhanced performance for advanced NVMe drive management and integration:

New Software Feature in Release 4.3(5d)

Cisco UCS Manager adds a security option that enables administrators to configure user blocking levels following failed login attempts, allowing them to choose between blocking all users at once or imposing restrictions on a per-user basis.

Additionally, syslog messages are generated for authentication failures, providing details such as user ID, domain ID, IP address, and account status.

New Software Feature in Release 4.3(5c)

Cisco UCS Manager 4.3(5c) now supports **Local Disk Configuration Policy** for the following Cisco Tri-Mode M1 24G RAID and HBA controllers on the Cisco UCS C225 M8 and C245 M8 servers:

- UCSC-HBA-M1L16

- UCSC-RAID-M1L16
- UCSC-RAID-MP1L32

New Software Feature in Release 4.3(5a)

- The Cisco UCS Manager release 4.3(5a) introduces advanced security management to protect sensitive data and ensure network integrity. This release includes encryption management with an AES encryption master key option. Additionally, Media Access Control Security (MACsec) now supports Type-6 (AES encryption) in addition to Type-0 and Type-7 encryption for Ethernet uplink ports on Cisco UCS 6536, 6454, and 64108 Fabric Interconnects through GUI and CLI interfaces. This feature offers robust encryption capabilities, allowing administrators to manage encryption settings effectively and ensure data security and compliance with encryption standards.



Note This functionality is not supported on Cisco UCS X-Series Direct (Cisco UCS Fabric Interconnects 9108 100G).

- Cisco UCS Manager now includes dynamic polling support to monitor the port status (up/down) and port speed of third-party Network Interface Cards (NICs) on Cisco UCS C-Series M6, M7, and M8 servers, offering real-time insights into network interface performance and ensuring optimal server connectivity and efficiency.
- Cisco UCS Manager enhances support for the server personality configuration of Hyperconverged Infrastructure (HCI). This feature is supported on Cisco UCS M6, M7, and M8 servers, allowing the servers to function either as standard UCS servers or HCI servers. The server personality field is an informational attribute that indicates the specific configuration or role assigned to the server. This simplifies the management of HCI and offers great visibility into server roles, enabling more efficient operations.
- Cisco UCS Manager supports enabling the EtherChannel pinning option for Cisco UCS VIC adapters to enhance performance. This option allows vNIC adapters with EtherChannel capabilities to utilize multiple uplink ports for optimized traffic distribution. This setting applies only to eNIC interfaces on Cisco UCS 1400, 14000, and 15000 series adapters and does not apply to fNIC interfaces.
- Cisco UCS Manager enables IPv6 overlay offload functionality. This feature, supported by updated async drivers, optimizes IPv6 network performance and enhances efficiency.
- Support for U.2 Solidigm P5520 NVMe High Perf. Medium Endurance and U.2 Solidigm P5620 NVMe High Perf. High Endurance with Cisco UCS UCS C225 M8, C245 M8, and all M7 and M6 servers.

New Software Feature in Release 4.3(4a)

- Cisco UCS Manager introduces support for Media Access Control Security (MACsec) type-0 and type-7 encryption for Ethernet uplink ports on Cisco UCS FI 6536, 6454 and 64108 through GUI and CLI interfaces.



Note This functionality is not supported on Cisco UCS X-Series Direct.

- Cisco UCS Manager support for ERSPAN traffic monitoring on Cisco UCS 6536, 6454, and 64108 Fabric Interconnects.



Note This functionality is not supported on Cisco UCS X-Series Direct.

- Cisco UCS Manager now provides support to configure Hybrid Slots Configuration policy for Cisco Tri-Mode 24G SAS RAID Controller w/4GB Cache (UCSC-RAID-HP) that indicates whether the RAID controller can handle U.3 drives in RAID or Direct attached modes.
- Cisco UCS Manager uses Data Sanitization feature to erase all sensitive data, thus making extraction or recovery of data impossible on the following UCS servers:
  - Cisco UCS C220 M7, C240 M7, X210c M7, X410c M7
  - Cisco UCS C220 M6, C240 M6, C225 M6, C245 M6, B200 M6, X210c M6 servers
  - Cisco UCS C220 M5, C240 M5, C480 M5, C125 M5, B200 M5, B480 M5 servers
- Cisco UCS Manager supports inventory listing for PCIe Node adapters.
- Cisco UCS Manager supports TLS 1.3 protocol for HTTPS communication for improved Transport Layer Security.
- New Ethernet port error, MACsec and DCE counters are added for the adapters under statistics.
- Starting with Cisco UCS Manager release 4.3(4a), new optimized adapter policies are available for Windows, Linux, and VMware operating systems, for the Cisco UCS VIC 1400, 14000 and 15000 series adapter.
- Starting with Cisco UCS Manager release 4.3(4a), adapter stats collection includes the following:
  - **rx_no_buffer** counters of vNIC which is represented as **no buffer drop packets**.
  - support for PFC pause time through **TxWait** and **RxWait** counters.
- NXOS now includes Fabric Interconnect port data-rate and PFC monitoring and is accessible through **show logging onboard** commands, capturing threshold crossings without duplications allowing user to monitor congestion in the Cisco UCS fabric interconnects.
- Release 4.3(4a) qualifies the new CipherTrust KMIP server from Thales®, which is set to take over from the old SafeNet and Vormetric servers that are being phased out. The new CipherTrust KMIP server offers enhanced usability and an expanded feature set, but keeps the user experience the same. Support for new CipherTrust in Cisco UCS Manager starts with version 4.3(4a). For detailed instructions on the configuration process of the CipherTrust KMIP manager, please refer to the CipherTrust Manager user guide provided by Thales®.

New Software Feature in Release 4.3(3c)

Cisco UCS Manager is enhanced to better handle high power demand during discovery and deep discovery of a server in Cisco UCSX-9508 chassis when the chassis is under load.

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.
```

Security Fixes

Security fixes in Release 4.3(6i)

There are no security fixes in release 4.3(6i).

Security fixes in Release 4.3(6h)

There are no security fixes in release 4.3(6h).

Security Fixes in Release 4.3(6g)

There are no security fixes in release 4.3(6g).

Security Fixes in Release 4.3(6f)

Defect ID - CSCwn23026

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

CVE-2023-20077—A vulnerability in the CLI and web-based management interface of the Cisco UCS Manager Software could allow an authenticated, remote attacker with valid administrative privileges to execute arbitrary commands on the underlying operating system of an affected device with root-level privileges. This vulnerability is due to insufficient input validation of command arguments supplied by the user.

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

For more information, see: Cisco UCS Manager Software Command Injection Vulnerability

Defect ID - CSCwm68934

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

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

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

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

Security Fixes in Release 4.3(6e)

There are no security fixes in release 4.3(6e).

Security Fixes in Release 4.3(6d)

Defect ID - CSCwq36167

The Cisco UCS B-Series M6 Blade Servers, UCS C-Series M6 Rack Servers, and 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-2025-20067—Observable timing discrepancy in firmware for some Intel® CSME and Intel® SPS may allow a privileged user to potentially enable information disclosure via local access.

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

Defect ID - CSCwq36167

The Cisco products UCS C-Series M7 Rack Servers and UCS X-Series M7 Compute Nodes include an Intel® CPU that is affected by the vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) IDs:

- CVE-2025-21096—Improper buffer restrictions in the firmware for some Intel® TDX may allow a privileged user to potentially enable escalation of privilege via local access.
- CVE-2025-20053—Improper buffer restrictions for some Intel® Xeon® processor firmware with SGX enabled may allow a privileged user to potentially enable escalation of privilege via local access.
- CVE-2025-24305—Insufficient control flow management in the Alias Checking Trusted Module (ACTM) firmware for some Intel® Xeon® processors may allow a privileged user to potentially enable escalation of privilege via local access.

- CVE-2025-20613—Predictable Seed in Pseudo-Random Number Generator (PRNG) in the firmware for some Intel® TDX may allow an authenticated user to potentially enable information disclosure via local access.
- CVE-2025-21090—Missing reference to active allocated resource for some Intel® Xeon® processors may allow an authenticated user to potentially enable denial of service via local access.
- CVE-2025-22853—Improper synchronization in the firmware for some Intel® TDX may allow a privileged user to potentially enable escalation of privilege via local access.

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

Security Fixes in Release 4.3(6c)

Defect ID - CSCwo49706 and CSCwo49702

The Cisco UCS B-Series M5/M6 Blade Servers, UCS C-Series M5/M6 Rack Servers, and 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-2024-45332—Exposure of sensitive information caused by shared microarchitectural predictor state that influences transient execution in the indirect branch predictors for some Intel® Processors may allow an authenticated user to potentially enable information disclosure via local access.

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

Defect ID - CSCwo49711

The Cisco products UCS C-Series M7 Rack Servers and UCS X-Series M7 Compute Nodes include an Intel CPU that is affected by the vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) IDs:

- CVE-2025-20103—Insufficient resource pool in the core management mechanism for some Intel® Processors may allow an authenticated user to potentially enable denial of service via local access.
- CVE-2025-20054—Uncaught exception in the core management mechanism for some Intel® Processors may allow an authenticated user to potentially enable denial of service through local access.
- CVE-2024-45332—Exposure of sensitive information caused by shared microarchitectural predictor state that influences transient execution in the indirect branch predictors for some Intel® Processors may allow an authenticated user to potentially enable information disclosure via local access.

Security Fixes in Release 4.3(6b)

There are no security fixes in release 4.3(6b).

Security Fixes in Release 4.3(6a)

Defect ID - CSCwm82813

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

- CVE-2010-5298—Race condition in the ssl3_read_bytes function in s3_pkt.c in OpenSSL through 1.0.1g, when SSL_MODE_RELEASE_BUFFERS is enabled, allows remote attackers to inject data across sessions or cause a denial of service (use-after-free and parsing error) through an SSL connection in a multithreaded environment.
- CVE-2011-0014—ssl/t1_lib.c in OpenSSL 0.9.8h through 0.9.8q and 1.0.0 through 1.0.0c allows remote attackers to cause a denial of service (crash), and possibly obtain sensitive information in applications that use OpenSSL, through a malformed ClientHello handshake message that triggers an out-of-bounds memory access, also called **OCSP stapling vulnerability**.
- CVE-2011-1945—The elliptic curve cryptography (ECC) subsystem in OpenSSL 1.0.0d and earlier, when the Elliptic Curve Digital Signature Algorithm (ECDSA) is used for the ECDHE_ECDSA cipher suite, does not properly implement curves over binary fields, which makes it easier for context-dependent attackers to determine private keys through a timing attack and a lattice calculation.
- CVE-2011-3207—crypto/x509/x509_vfy.c in OpenSSL 1.0.x before 1.0.0e does not initialize certain structure members, which makes it easier for remote attackers to bypass CRL validation by using a nextUpdate value corresponding to a time in the past.
- CVE-2011-3210—The ephemeral ECDH ciphersuite functionality in OpenSSL 0.9.8 through 0.9.8r and 1.0.x before 1.0.0e does not ensure thread safety during processing of handshake messages from clients, which allows remote attackers to cause a denial of service (daemon crash) through out-of-order messages that violate the TLS protocol.
- CVE-2011-4108—The DTLS implementation in OpenSSL before 0.9.8s and 1.x before 1.0.0f performs a MAC check only if certain padding is valid, which makes it easier for remote attackers to recover plaintext through a padding oracle attack.
- CVE-2011-4576—The SSL 3.0 implementation in OpenSSL before 0.9.8s and 1.x before 1.0.0f does not properly initialize data structures for block cipher padding, which might allow remote attackers to obtain sensitive information by decrypting the padding data sent by an SSL peer.
- CVE-2011-4577—OpenSSL before 0.9.8s and 1.x before 1.0.0f, when RFC 3779 support is enabled, allows remote attackers to cause a denial of service (assertion failure) through an X.509 certificate containing certificate-extension data associated with IP address blocks or Autonomous System (AS) identifiers.
- CVE-2011-4619—The Server Gated Cryptography (SGC) implementation in OpenSSL before 0.9.8s and 1.x before 1.0.0f does not properly handle handshake restarts, which allows remote attackers to cause a denial of service (CPU consumption) through unspecified vectors.
- CVE-2012-0027—The GOST ENGINE in OpenSSL before 1.0.0f does not properly handle invalid parameters for the GOST block cipher, which allows remote attackers to cause a denial of service (daemon crash) through crafted data from a TLS client.
- CVE-2012-0884—The implementation of Cryptographic Message Syntax (CMS) and PKCS #7 in OpenSSL before 0.9.8u and 1.x before 1.0.0h does not properly restrict certain oracle behavior, which makes it easier for context-dependent attackers to decrypt data through a Million Message Attack (MMA) adaptive chosen ciphertext attack.
- CVE-2012-1165—The mime_param_cmp function in crypto/asn1/asn_mime.c in OpenSSL before 0.9.8u and 1.x before 1.0.0h allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) through a crafted S/MIME message, a different vulnerability than CVE-2006-7250.
- CVE-2012-2110—The asn1_d2i_read_bio function in crypto/asn1/a_d2i_fp.c in OpenSSL before 0.9.8v, 1.0.0 before 1.0.0i, and 1.0.1 before 1.0.1a does not properly interpret integer data, which allows remote

attackers to conduct buffer overflow attacks, and cause a denial of service (memory corruption) or possibly have unspecified other impact, through crafted DER data, as demonstrated by an X.509 certificate or an RSA public key.

- CVE-2012-2333—Integer underflow in OpenSSL before 0.9.8x, 1.0.0 before 1.0.0j, and 1.0.1 before 1.0.1c, when TLS 1.1, TLS 1.2, or DTLS is used with CBC encryption, allows remote attackers to cause a denial of service (buffer over-read) or possibly have unspecified other impact through a crafted TLS packet that is not properly handled during a certain explicit IV calculation.
- CVE-2013-0166—OpenSSL before 0.9.8y, 1.0.0 before 1.0.0k, and 1.0.1 before 1.0.1d does not properly perform signature verification for OCSP responses, which allows remote OCSP servers to cause a denial of service (NULL pointer dereference and application crash) through an invalid key.
- CVE-2013-0169—The TLS protocol 1.1 and 1.2 and the DTLS protocol 1.0 and 1.2, as used in OpenSSL, OpenJDK, PolarSSL, and other products, do not properly consider timing side-channel attacks on a MAC check requirement during the processing of malformed CBC padding, which allows remote attackers to conduct distinguishing attacks and plaintext-recovery attacks through statistical analysis of timing data for crafted packets, also called the **Lucky Thirteen** issue.
- CVE-2013-6449—The ssl_get_algorithm2 function in ssl/s3_lib.c in OpenSSL before 1.0.2 obtains a certain version number from an incorrect data structure, which allows remote attackers to cause a denial of service (daemon crash) through crafted traffic from a TLS 1.2 client.
- CVE-2013-6450—The DTLS retransmission implementation in OpenSSL 1.0.0 before 1.0.0l and 1.0.1 before 1.0.1f does not properly maintain data structures for digest and encryption contexts, which might allow man-in-the-middle attackers to trigger the use of a different context and cause a denial of service (application crash) by interfering with packet delivery, related to ssl/d1_both.c and ssl/t1_enc.c.
- CVE-2014-0076—The Montgomery ladder implementation in OpenSSL through 1.0.0l does not ensure that certain swap operations have a constant-time behavior, which makes it easier for local users to obtain ECDSA nonces through a FLUSH+RELOAD cache side-channel attack.
- CVE-2014-0195—The dtls1_reassemble_fragment function in d1_both.c in OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h does not properly validate fragment lengths in DTLS ClientHello messages, which allows remote attackers to execute arbitrary code or cause a denial of service (buffer overflow and application crash) through a long non-initial fragment.
- CVE-2014-0198—The do_ssl3_write function in s3_pkt.c in OpenSSL 1.x through 1.0.1g, when SSL_MODE_RELEASE_BUFFERS is enabled, does not properly manage a buffer pointer during certain recursive calls, which allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) through vectors that trigger an alert condition.
- CVE-2014-0221—The dtls1_get_message_fragment function in d1_both.c in OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h allows remote attackers to cause a denial of service (recursion and client crash) through a DTLS hello message in an invalid DTLS handshake.
- CVE-2014-0224—OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h does not properly restrict processing of ChangeCipherSpec messages, which allows man-in-the-middle attackers to trigger use of a zero-length master key in certain OpenSSL-to-OpenSSL communications, and consequently hijack sessions or obtain sensitive information, through a crafted TLS handshake, also called the **CCS Injection** vulnerability.
- CVE-2014-3470—The ssl3_send_client_key_exchange function in s3_clnt.c in OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h, when an anonymous ECDH cipher suite is used, allows

remote attackers to cause a denial of service (NULL pointer dereference and client crash) by triggering a NULL certificate value.

- CVE-2014-3505—Double free vulnerability in d1_both.c in the DTLS implementation in OpenSSL 0.9.8 before 0.9.8zb, 1.0.0 before 1.0.0n, and 1.0.1 before 1.0.1i allows remote attackers to cause a denial of service (application crash) through crafted DTLS packets that trigger an error condition.
- CVE-2014-3506—d1_both.c in the DTLS implementation in OpenSSL 0.9.8 before 0.9.8zb, 1.0.0 before 1.0.0n, and 1.0.1 before 1.0.1i allows remote attackers to cause a denial of service (memory consumption) through crafted DTLS handshake messages that trigger memory allocations corresponding to large length values.
- CVE-2014-3507—Memory leak in d1_both.c in the DTLS implementation in OpenSSL 0.9.8 before 0.9.8zb, 1.0.0 before 1.0.0n, and 1.0.1 before 1.0.1i allows remote attackers to cause a denial of service (memory consumption) through zero-length DTLS fragments that trigger improper handling of the return value of a certain insert function.
- CVE-2014-3508—The OBJ_obj2txt function in crypto/objects/obj_dat.c in OpenSSL 0.9.8 before 0.9.8zb, 1.0.0 before 1.0.0n, and 1.0.1 before 1.0.1i, when pretty printing is used, does not ensure the presence of '\0' characters, which allows context-dependent attackers to obtain sensitive information from process stack memory by reading output from X509_name_oneline, X509_name_print_ex, and unspecified other functions.
- CVE-2014-3509—Race condition in the ssl_parse_serverhello_tlsext function in t1_lib.c in OpenSSL 1.0.0 before 1.0.0n and 1.0.1 before 1.0.1i, when multithreading and session resumption are used, allows remote SSL servers to cause a denial of service (memory overwrite and client application crash) or possibly have unspecified other impact by sending Elliptic Curve (EC) Supported Point Formats Extension data.
- CVE-2014-3510—The ssl3_send_client_key_exchange function in s3_clnt.c in OpenSSL 0.9.8 before 0.9.8zb, 1.0.0 before 1.0.0n, and 1.0.1 before 1.0.1i allows remote DTLS servers to cause a denial of service (NULL pointer dereference and client application crash) through a crafted handshake message in conjunction with a (1) anonymous DH or (2) anonymous ECDH ciphersuite.
- CVE-2014-3511—The ssl23_get_client_hello function in s23_srvr.c in OpenSSL 1.0.1 before 1.0.1i allows man-in-the-middle attackers to force the use of TLS 1.0 by triggering ClientHello message fragmentation in communication between a client and server that both support later TLS versions, related to a **protocol downgrade** issue.
- CVE-2014-3512—Multiple buffer overflows in crypto/srp/srp_lib.c in the SRP implementation in OpenSSL 1.0.1 before 1.0.1i allow remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact through an invalid SRP (1) g, (2) A, or (3) B parameter.
- CVE-2014-3566—The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data through a padding-oracle attack, aka the **POODLE** issue.
- CVE-2014-3567—Memory leak in the tls_decrypt_ticket function in t1_lib.c in OpenSSL before 0.9.8zc, 1.0.0 before 1.0.0o, and 1.0.1 before 1.0.1j allows remote attackers to cause a denial of service (memory consumption) through a crafted session ticket that triggers an integrity-check failure.
- CVE-2014-3568—OpenSSL before 0.9.8zc, 1.0.0 before 1.0.0o, and 1.0.1 before 1.0.1j does not properly enforce the no-ssl3 build option, which allows remote attackers to bypass intended access restrictions through an SSL 3.0 handshake, related to s23_clnt.c and s23_srvr.c.

- CVE-2014-3570—The BN_sqr implementation in OpenSSL before 0.9.8zd, 1.0.0 before 1.0.0p, and 1.0.1 before 1.0.1k does not properly calculate the square of a BIGNUM value, which might make it easier for remote attackers to defeat cryptographic protection mechanisms through unspecified vectors, related to crypto/bn/asm/mips.pl, crypto/bn/asm/x86_64-gcc.c, and crypto/bn/bn_asm.c.
- CVE-2014-3571—OpenSSL before 0.9.8zd, 1.0.0 before 1.0.0p, and 1.0.1 before 1.0.1k allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) through a crafted DTLS message that is processed with a different read operation for the handshake header than for the handshake body, related to the dtls1_get_record function in d1_pkt.c and the ssl3_read_n function in s3_pkt.c.
- CVE-2014-3572—The ssl3_get_key_exchange function in s3_clnt.c in OpenSSL before 0.9.8zd, 1.0.0 before 1.0.0p, and 1.0.1 before 1.0.1k allows remote SSL servers to conduct ECDHE-to-ECDH downgrade attacks and trigger a loss of forward secrecy by omitting the ServerKeyExchange message.
- CVE-2014-8176—The dtls1_clear_queues function in ssl/d1_lib.c in OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h frees data structures without considering that application data can arrive between a ChangeCipherSpec message and a Finished message, which allows remote DTLS peers to cause a denial of service (memory corruption and application crash) or possibly have unspecified other impact through unexpected application data.
- CVE-2014-8275—OpenSSL before 0.9.8zd, 1.0.0 before 1.0.0p, and 1.0.1 before 1.0.1k does not enforce certain constraints on certificate data, which allows remote attackers to defeat a fingerprint-based certificate-blacklist protection mechanism by including crafted data within a certificate's unsigned portion, related to crypto/asn1/a_verify.c, crypto/dsa/dsa_asn1.c, crypto/ecdsa/ecs_vrf.c, and crypto/x509/x_all.c.
- CVE-2015-0204—The ssl3_get_key_exchange function in s3_clnt.c in OpenSSL before 0.9.8zd, 1.0.0 before 1.0.0p, and 1.0.1 before 1.0.1k allows remote SSL servers to conduct RSA-to-EXPORT_RSA downgrade attacks and facilitate brute-force decryption by offering a weak ephemeral RSA key in a noncompliant role, related to the **FREAK** issue. NOTE: the scope of this CVE is only client code based on OpenSSL, not EXPORT_RSA issues associated with servers or other TLS implementations.
- CVE-2015-0205—The ssl3_get_cert_verify function in s3_srvr.c in OpenSSL 1.0.0 before 1.0.0p and 1.0.1 before 1.0.1k accepts client authentication with a Diffie-Hellman (DH) certificate without requiring a CertificateVerify message, which allows remote attackers to obtain access without knowledge of a private key through crafted TLS Handshake Protocol traffic to a server that recognizes a Certification Authority with DH support.
- CVE-2015-0206—Memory leak in the dtls1_buffer_record function in d1_pkt.c in OpenSSL 1.0.0 before 1.0.0p and 1.0.1 before 1.0.1k allows remote attackers to cause a denial of service (memory consumption) by sending many duplicate records for the next epoch, leading to failure of replay detection.
- CVE-2015-0209—Use-after-free vulnerability in the d2i_ECPrivateKey function in crypto/ec/ec_asn1.c in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a might allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly have unspecified other impact through a malformed Elliptic Curve (EC) private-key file that is improperly handled during import.
- CVE-2015-0286—The ASN1_TYPE_cmp function in crypto/asn1/a_type.c in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a does not properly perform boolean-type comparisons, which allows remote attackers to cause a denial of service (invalid read operation and application crash) through a crafted X.509 certificate to an endpoint that uses the certificate-verification feature.

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.

Defect ID - CSCwm73565

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

- CVE-2024-28047—Improper input validation in UEFI firmware for some Intel(R) Processors may allow a privileged user to potentially enable information disclosure via local access.

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

Security Fixes in Release 4.3(5d)

There are no security fixes in release 4.3(5d).

Security Fixes in Release 4.3(5c)

Defect ID - CSCwm73573

Cisco UCS C-Series M7 Rack Servers and Cisco UCS X-Series M7 Compute Nodes include an Intel® CPU that is affected by the vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) IDs:

- CVE-2024-27457—Improper check for unusual or exceptional conditions in Intel(R) TDX Module firmware before version 1.5.06 may allow a privileged user to potentially enable information disclosure via local access.
- CVE-2024-23918—Improper conditions check in some Intel(R) Xeon(R) processor memory controller configurations when using Intel(R) SGX may allow a privileged user to potentially enable escalation of privilege via local access.
- CVE-2024-21820—Incorrect default permissions in some Intel(R) Xeon(R) processor memory controller configurations when using Intel(R) SGX may allow a privileged user to potentially enable escalation of privilege via local access.
- CVE-2024-21853—Improper finite state machines (FSMs) in the hardware logic in some 4th and 5th Generation Intel(R) Xeon(R) Processors may allow an authorized user to potentially enable denial of service via local access.
- CVE-2024-25565—Insufficient control flow management in UEFI firmware for some Intel(R) Xeon(R) Processors may allow an authenticated user to enable denial of service via local access.
- CVE-2024-23984—Observable discrepancy in RAPL interface for some Intel(R) Processors may allow a privileged user to potentially enable information disclosure via local access.
- CVE-2024-24968—Improper finite state machines (FSMs) in hardware logic in some Intel(R) Processors may allow a privileged user to potentially enable a denial of service via local access.
- CVE-2024-22185—Time-of-check Time-of-use Race Condition in some Intel(R) processors with Intel(R) ACTM may allow a privileged user to potentially enable escalation of privilege via local access.
- CVE-2024-24985—Exposure of resource to wrong sphere in some Intel(R) processors with Intel(R) ACTM may allow a privileged user to potentially enable escalation of privilege via local access.

- CVE-2024-21829—Improper input validation in UEFI firmware error handler for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access.
- CVE-2024-23599—Race condition in Seamless Firmware Updates for some Intel(R) reference platforms may allow a privileged user to potentially enable denial of service via local access.
- CVE-2024-21781—Improper input validation in UEFI firmware for some Intel(R) Processors may allow a privileged user to enable information disclosure or denial of service via local access.
- CVE-2024-39279—Insufficient granularity of access control in UEFI firmware in some Intel(R) processors may allow an authenticated user to potentially enable denial of service via local access.
- CVE-2024-28047—Improper input validation in UEFI firmware for some Intel(R) Processors may allow a privileged user to potentially enable information disclosure via local access.
- CVE-2024-31157—Improper initialization in UEFI firmware OutOfBandXML module in some Intel(R) Processors may allow a privileged user to potentially enable information disclosure via local access.
- CVE-2024-36293—Improper access control in the EDECCSSA user leaf function for some Intel(R) Processors with Intel(R) SGX may allow an authenticated user to potentially enable denial of service via local access.
- CVE-2024-31068—Improper Finite State Machines (FSMs) in Hardware Logic for some Intel(R) Processors may allow privileged user to potentially enable denial of service via local access.
- CVE-2024-25571—Improper input validation in some Intel(R) SPS firmware before SPS_E5_06.01.04.059.0 may allow a privileged user to potentially enable denial of service via local access.
- CVE-2024-21859—Improper buffer restrictions in the UEFI firmware for some Intel(R) Processors may allow a privileged user to potentially enable information disclosure via local access.
- CVE-2024-31155—Improper buffer restrictions in the UEFI firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access.
- CVE-2024-37020—Sequence of processor instructions leads to unexpected behavior in the Intel(R) DSA V1.0 for some Intel(R) Xeon(R) Processors may allow an authenticated user to potentially enable denial of service via local access.

Security Fixes in Release 4.3(5a)

Defect ID - CSCwk62264

Cisco UCS 6400 Series Fabric Interconnects and UCS 6500 Series Fabric Interconnects in UCS Manager Mode includes Third-party Software that is affected by the vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) IDs:

- CVE-2024-6387—A security regression (CVE-2006-5051) has been discovered in the OpenSSH server (sshd). A race condition exists that may cause sshd to handle certain signals unsafely. This vulnerability can potentially be exploited by an unauthenticated, remote attacker by failing to authenticate within a specified time period.

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.

Defect ID - CSCwk62723

Cisco UCS B-Series Blade Servers - Serial over LAN (SOL) and Cisco UCS X-Series Compute Nodes - Serial over LAN (SOL) includes Third-party Software that is affected by the vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) IDs:

- CVE-2024-6387—A security regression (CVE-2006-5051) has been discovered in the OpenSSH server (sshd). A race condition exists that may cause sshd to handle certain signals unsafely. This vulnerability can potentially be exploited by an unauthenticated, remote attacker by failing to authenticate within a specified time period.

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.

Defect ID - CSCwk75392

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

- CVE-2023-52425—libexpat through 2.5.0 allows a denial of service (resource consumption) because many full reparsings are required in the case of a large token for which multiple buffer fills are needed.

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(4f)

There are no security fixes in release 4.3(4f).

Security Fixes in Release 4.3(4e)

There are no security fixes in release 4.3(4e).

Security Fixes in Release 4.3(4d)

There are no security fixes in release 4.3(4d).

Security Fixes in Release 4.3(4c)

Defect ID - CSCwk62264

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

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

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

Security Fixes in Release 4.3(4b)

There are no security fixes in release 4.3(4b).

Security Fixes in Release 4.3(4a)

Defect ID - CSCwi59915

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

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

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

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

Security Fixes in Release 4.3(3c)

There are no security fixes in Release 4.3(3c).

Security Fixes in Release 4.3(3a)

Defect ID - CSCwh58728

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

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

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

Defect ID - 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(2f)

There are no security fixes in release 4.3(2f).

Security Fixes in Release 4.3(2e)

Defect ID - 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.

Defect ID - 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.

Defect ID - 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)

Defect ID - 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)

Defect ID - 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.

Resolved caveats in Release 4.3(6i)

There are no resolved caveats in release 4.3(6i).

Resolved caveats in Release 4.3(6h)

Defect ID	Symptoms	First Bundle Affected	Resolved in Release
CSCwt12837	During Cisco UCS Manager activation, a loss of SSH connectivity between the fabric interconnects can leave the two fabrics on different versions and block GUI access. This issue is specific to upgrade scenarios in which the activation depends on uninterrupted SSH communication between the fabrics. This issue is resolved.	3.2(3d)A	4.3(6h)
CSCws79672	The Cisco UCS 6454 FI running release 4.3(6b) experiences management service unresponsiveness on Fabric Interconnect B due to the DME database becoming full. This condition triggers Call Home alerts and causes the management services to become unresponsive temporarily. This issue is resolved.	4.3(6b)	4.3(6h)
CSCwn42410	A partial failure of one of the M.2 drives on a Cisco UCS-M2-HWRAID controller may cause the affected drive to be reported incorrectly and may degrade the RAID 1 virtual drive. In this condition, the drive can appear in `PhyDriveInfo` with no valid device data visible, while the reported link speed is reduced to 1.5 GB. Additional drive attributes such as power-on hours, power cycle count, percentage life, wear status days, and temperature may all appear as 0. Product ID and firmware fields may also be blank even though the drive is still shown as online. In some cases, the messages log may incorrectly report the affected drive as having 0% life remaining by generating an `SSD LIFE TIME LAPSE` fault. T This issue has been observed on systems using the Cisco UCS-M2-HWRAID M.2 storage controller with M.2 drives configured in a RAID 1 virtual drive. This issue is resolved.	4.2(3m)	4.3(6h)
CSCwu82212	The fabric interconnect root file system can reach 100 percent utilization, which may affect services such as DNS resolution. This issue can occur during normal fabric interconnect operation. This issue can cause DNS-related failures on the fabric interconnect. This issue is resolved.	4.3(6d)A	4.3(6h)

Defect ID	Symptoms	First Bundle Affected	Resolved in Release
CSCwt96184	After server decommission and recommission for the Cisco UCS M6 rack servers, the Cisco UCS 15428 VIC adapter remains stuck in the Inoperable state. The server fails to receive discovery from Cisco UCS Manager due to a DHCP packet parsing error at the Baseboard Management Controller (BMC). This error occurs because the DHCP packet contains extra fields or characters, causing Cisco UCS Manager initialization to fail with a `FATAL ERROR! Invalid UCSM DHCP mode token` message and aborting the mode change process. This issue prevents proper adapter operation and server discovery. This issue is resolved.	4.3(6f)	4.3(6h)
CSCwt79531	After an infrastructure upgrade, server discovery can fail at 25 percent because the svc_sam_dme process restarts unexpectedly. This issue is seen Cisco UCS 6454 fabric interconnect deployments, where NIC AG logs reported memory allocation failures during the upgrade flow. This issue is resolved.	4.3(4e)A	4.3(6h)
CSCwp23550	When a non-admin user exits a fabric interconnect CLI session, the session can prompt for a sudo password instead of closing normally. This issue is resolved.	4.3(6c)A	4.3(6h)
CSCwr55882	After an upgrade, some IOM backplane ports can remain down because fabric evacuation does not turn off as expected. This issue can occur after fabric evacuation is enabled before an auto-upgrade and the first fabric interconnect completes the upgrade while shallow discovery is still in progress. A shallow discovery can update the evacuation state too early and keep HIF ports down on affected chassis. This issue is resolved.	4.3(4e)A	4.3(6h)
CSCwn60596	After an infrastructure firmware upgrade, KVM consoles can become inoperable even though the assigned KVM IP address remains reachable. This issue has been observed in domains with multiple chassis and out-of-band management after firmware upgrades or PMON restarts. This issue is resolved.	4.3(4a)	4.3(6h)

Resolved Caveats in Release 4.3(6g)

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCwt18924	After an upstream Cisco ACI fabric upgrade or reload, Cisco UCS VIC adapters may fail to bring vNICs online, leaving them stuck in an initializing state. This issue specifically affects configurations using 10GBase-T (SFP-10G-T-X) transceivers connected to Cisco UCS VIC 1400 series adapters (1455, 1457, 1467) or 15000 series adapters (15427, 15428, 15425) on supported Nexus switches. The root cause is a memory leak within the adapter triggered when the 10GBase-T transceiver hogs the I2C bus during operations, including—but not limited to—server or switch resets and reboots. Although the adapter physical interfaces may come up, the memory leak prevents the vNICs from recovering automatically. This issue is resolved.	4.3(5a)	4.3(6g)
CSCwi16863	BMC watchdog resets can occur on Cisco UCS B200 M6 and UCS X210c M6 servers, causing CIMC to reboot unexpectedly. This issue is resolved.	4.2(3d)	4.3(6g)

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCws91466	IOMs in the Cisco UCS domain running Cisco UCS Manager version 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(6b)A	4.3(6g)

Resolved Caveats in Release 4.3(6f)

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCwo01109	On some FIs, SNMP requests may stop receiving responses under specific error conditions. When SNMP queries are issued for certain invalid interfaces, SNMP responsiveness may be impacted and technical support data collection can be delayed. This issue is resolved.	4.2(3k)	4.3(6f)

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCwq38681	In environments where Cisco UCS Manager is managed by Cisco UCS Central with settings configured to Global, locally configured Trust Points on Cisco UCS Manager may be deleted. This can occur when Trust Points are manually created on Cisco UCS Manager while User Management and related settings are controlled by Cisco UCS Central. Alarms may be raised if keyrings are associated with the deleted Trust Points. This issue is resolved.	4.3(6c)	4.3(6f)
CSCwr64103	On some FIs, SSH access to the Cisco UCS Manager CLI may fail with a `More than 32 UCSM CLI sessions are not allowed` error. In this condition, login using LDAP or local admin credentials via SSH may not be possible, while Cisco UCS Manager GUI access remains available. Technical support information collection may be incomplete, with certain log files appearing truncated or reporting errors when gathering Cisco UCS Manager information. This issue is resolved.	4.3(5a)	4.3(6f)

Resolved Caveats in Release 4.3(6e)

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCws30219	Cisco UCS M7 servers managed by Cisco UCS Manager with server bundle versions 4.3(6c), 4.3(6d), 6.0(1b), 6.0(1c), and 6.0(1d) are susceptible to host lockups triggered by ECC (Error Correcting Code) memory events. This issue is specifically related to how the server BIOS interacts with the Extensible Firmware Interface (EFI) during error conditions. During these events, the BIOS does not correctly retrieve a required variable, causing EFI to return an invalid parameter. As a result, the operating system is unable to continue normal operation and freezes without logging any errors. When this occurs, the host becomes unresponsive and KVM input is not accepted. Single-bit ECC errors—while not logged due to DDR5 specifications—can trigger this condition, resulting in complete loss of host responsiveness. This issue is resolved.	4.3(6c) server bundle B/C	4.3(6e) server bundle B/C

Resolved Caveats in Release 4.3(6d)

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCwr23094	The Cisco UCS 6536 Fabric Interconnect may experience unexpected reboots due to the **vntag_mgr hap reset** service crashing from a memory leak. The system reset reason shows a reset triggered by HA policy related to this service. Logs indicate the **vntag_mgr** service crashes with an unhandled signal 6, causing core dumps. This issue is resolved.	4.2(3b)A	4.3(6d)A
CSCwq34720	Re-association of the Cisco UCS X210c M7 compute node, running Windows 2022 Server with Secure Boot enabled, fails with the following error:SBAT self-check failed: Security Policy Violation This issue is resolved.	4.3(5c)B	4.3(6d)B
CSCwo57642	An issue arises when attempting to power on an Cisco US X210c M7 blade server with a PCIe X440p attached in a chassis within a capped Power Group. The blade fails to boot, displaying the error message **Insufficient power available to power on server**. This problem occurs even if other blades in the chassis are already discovered and operational. This issue is resolved.	4.3(4a)	4.3(6d)B

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCwq32344	After upgrading the infra firmware, the Cisco UCS 5108 Blade Server chassis reports a critical malformed FRU error for power supply units with blank modules. Cisco UCS Manager incorrectly flags these slots as having malformed FRUs instead of reporting FRU not installed. This issue is resolved.	4.3(5c)A	4.3(6d)A
CSCwo61643	Downgrading the infrastructure bundle from a newer release to an older one causes a permissions issue on one Fabric Interconnect. This issue blocks internal user login to the peer Fabric Interconnect, preventing successful upgrades afterward. This issue is resolved.	4.3(6a)	4.3(6d)
CSCwr24516	Cisco UCS blade server encounters a power-on failure and does not boot due to an under-current fault in the standby voltage regulator for CPU1. The fault is identified by the **IOUT UC FAULT** flag in the voltage regulator fault registers. This issue prevents normal system startup. This issue is resolved.	6.0(1b)	4.3(6d)

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCwr31522	Cisco UCS M8 servers may fail to complete POST and not boot if the BMC firmware is downgraded to release 4.3 from any higher release, and a warm reset is performed. This issue is resolved.	4.3(6a)	4.3(6d)
CSCwp64077	The snmpd process crashes repeatedly on Cisco UCS 64108 FI, triggered by an unhandled SIGABRT signal after kernel messages report **sap recovering failed and so Killed with SIGABRT - kernel.** This issue is resolved.	4.3(5a)	4.3(6d)
CSCwq58890	The firmware for the Cisco UCS VIC 15000 series adapters is updated to fix a rare, intermittently seen memory issue and to ensure more robust and consistent operation across diverse memory types and configurations. **Note** If you continue to experience any memory error, then contact Cisco TAC.	6.0(1b)	4.3(6d)

Resolved Caveats in Release 4.3(6c)

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCwo90621	Cisco UCS systems equipped with Cisco UCS 2408 IOMs running infrastructure bundle release 4.3(5c) report thermal alerts. These alerts cause system fans to increase speed temporarily. Despite the critical alerts, the reported temperatures remain within normal operating ranges. This issue is resolved.	4.3(5c)	4.3(6c)
CSCwp20088	Cisco UCS domains managed by Cisco UCS Central may become suspended after upgrading Cisco UCS Manager to certain versions. This occurs when a deprecated IO policy was configured from Cisco UCS Central. The domain shows as suspended in Cisco UCS Central, Cisco UCS Manager displays a warning F1057, and attempts to activate or acknowledge the domain fail with an error regarding the IO Policy. This issue is resolved.	4.3(5a)	4.3(6c)

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCwn86965	Cisco UCS chassis equipped with 2204XP IOMs may report a persistent `error accessing shared-storage` warning. This warning is triggered by read or write errors on the chassis. The warning does not clear automatically and requires a fix. This issue is resolved.	4.2(3k)	4.3(6c)
CSCwo62993	Cisco UCS Manager domains may experience secure LDAP authentication failures after a Trustpoint configuration change. This issue has occurred intermittently and is often accompanied by **TLS Start failed** or **Unknown CA** errors in debug output. Affected domains are unable to authenticate users through LDAP. This issue is resolved.	4.3(3a)	4.3(6c)
CSCwo85317	Cisco UCS Manager on servers equipped with DIMMs having vendor part number 36ASF4G72PZ-3G2J3 reports a Warning Fault F0502, indicating an invalid FRU. This occurs because the capability catalog does not recognize this specific DIMM part number. As a result, the DIMM identity is **unestablishable**. This issue is resolved.	4.2(3m)	4.3(6c)

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCwo37410	When Cisco UCS Manager is managed by Cisco UCS Central with the **Infrastructure & Catalog Firmware** setting changed from **Global** to **Local**, the bundle firmware version does not display on any Fabric Interconnect after a reboot. The **Package Version** field becomes empty following any reboot triggered by configuration changes. This issue is resolved.	4.0(4g)	4.3(6c)

Resolved Caveats in Release 4.3(6b)

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCwm45755	In Cisco UCS C220 M8 servers equipped with M.2 disks connected to a storage controller, the disks are not detected on the Windows Server 2025 installation page. However, the disks are detected during the installation of Windows Server 2022. This issue occurs specifically with Windows Server 2025. This issue is resolved.	4.3(6a)	4.3(6b)
CSCwn99720	On Cisco UCS C-Series M8 servers with Intel processors and an R1S CPU configured in a single CPU setup on the 2S platform, Intel SGX remains disabled even after being enabled in the BIOS. This issue does not occur with a dual CPU configuration. This issue is resolved.	4.3(6a)	4.3(6b)

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCwn51498	Raw OEM SEL records are logged in CIMC SEL during the booting and shutdown of Windows Server 2025 on Cisco UCS C220 M8 servers. This issue is resolved.	4.3(6a)	4.3(6b)

Resolved Caveats in Release 4.3(6a)

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCwj61708		4.3(4a)	4.3(6a)

Defect ID	Symptom	First Bundle Affected	Resolved in Release
	When performing a warm reboot of multiple servers in a scale-setup of 160 servers and high PV count of greater than 64K in Cisco UCS FI domain, secure boot adapters may not restart instantly under certain situations. This was observed in a scale setup where simultaneous warm reboot of 22 blades across three chassis was initiated. Some blades with Cisco UCS VIC 15000 series secure boot adapters failed to boot from the SAN after a soft reboot. These adapters execute a cleanup process with the Fabric Interconnects to maintain system integrity, which needs to be finished before the server BIOS can recognize the adapters. This issue arises specifically under conditions of very high PV count or exceptionally high CPU utilization on the FI. During these instances, if the server BIOS finalizes the boot sequence before the secure boot adapters finish the cleanup, the adapters may fail to be detected. Consequently, the server may not successfully boot from the SAN. This issue is observed in configurations using Cisco UCS blade servers equipped with Cisco UCS VIC 15000 series adapters.		

Defect ID	Symptom	First Bundle Affected	Resolved in Release
	This issue is resolved.		
CSCwn44955	During Cisco UCS Fabric Interconnect (FI) replacement, the DME service may crash upon connecting the new FI, resulting in the failure of management services. This issue affects FI models under firmware version 4.3(5a) and leads to HA readiness and replication sync failures between FI-A and FI-B. This issue is resolved.	4.3(5a)	4.3(6a)
CSCwo18968	During the transition of SNMP services to BMC Inventory, communication issues have been observed in two out of four Cisco UCS Manager instances. Traceroute confirms no network blockage, and the SNMP service (svc_sam_netSnmpAG) remains operational with no failures reported. However, reports indicate SNMP ports as closed. This issue is resolved.	4.3(2c)	4.3(6a)

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCwk47042	During migration from Cisco UCS 6200/6300 Series Fabric Interconnects to Cisco UCS 6500 FI, you may see errors when configuring Fibre Channel (FC) storage ports. The system returns an error indicating that FcEstcEp must be contained under the SubGroup hierarchy and does not support FC Breakout in this platform. Attempts to configure FC ports via CLI using the Unified Breakout Storage Ports guide result in an **Update failed** message. This issue is resolved.	4.2(3l)	4.3(6a)
CSCwn29896	An error occurs at the FSM level when creating an SNMP user with a user name exceeding 23 characters. This issue has been observed specifically on Cisco UCS 6454 FI running firmware version 4.2(3k). This issue is resolved.	4.2(3k)	4.3(6a)

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCwo62993	After upgrading Cisco UCS Manager from any 4.1(3) release to 4.3(3a), LDAP/AD authentication fails intermittently, affecting login with AD credentials across multiple domains. **TLS start failed** error is repored, and packet captures indicate an **Unknown CA** alert. OpenSSL commands show a certificate verification error. Despite successful connectivity to the LDAP server, authentication issues persist.	4.3(3a)	4.3(6a)

Resolved Caveats in Release 4.3(5d)

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCwn65779	The UCS-FI-64108 Fabric Interconnects may experience unexpected reboots due to kernel panics. This is not a very common case. Initially, the Primary Fabric Interconnect (B) encountered a kernel panic and rebooted, leading to a cluster failover to the Secondary FI (A). About 48 hours later, the new Primary FI (A) also suffered a kernel panic and rebooted. The stack trace reveals a null pointer dereference, resulting in a fatal exception. This issue is resolved.	4.2(3g)A	4.3(5d)A

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCwn41380	Cisco UCS Blade servers lose SAN connectivity when one of the FC up-link or FI is down because of the following reasons: • FC link is congested • Peer FC link is down due to peer system crash or errors on the receiving side This issue is resolved.	4.2(1f)A	4.3(5d)A
CSCwn32035	Some 5108 Chassis fans may pull the SDA line of the I2C bus low for an extended duration, causing the I2C bus to lock up and all system fans are flagged as faulty. Alarms are seen for the bad fans. While not common, if it happens, replace the faulty fans, if the problem persists, contact TAC for more assistance. This issue is resolved.	4.3(5a)	4.3(5d)
CSCwj60167	Cisco UCS B-Series Servers managed by Cisco UCS Manager may experience a temporary BMC reboot due to a kernel panic, affecting management connectivity without impacting server operation. You may notice a temporary loss of CIMC connectivity. This issue is resolved.	4.3(2c)B	4.3(5d)B

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCwn69805	The Cisco UCS 64108 Fabric Interconnectreboots unexpectedly, leading to a loss of network redundancy and high availability (HA), although the fabric interconnect eventually recovers itself. These reboots are often caused by a fatal upgrade error, as indicated by "IOFPGA POWER DEBUG" and "IOFPGA RESET CAUSE" messages in the logs. While rare, this issue can occur under specific conditions related to certain software and hardware configurations. This issue is resolved.	4.2(1n)A	4.3(5d)B
CSCwn83351	This defect causes system reloads due to a Watchdog Timeout without generating diagnostic traces or cores. The condition is identified by the absence of kernel trace, dmesg, and show cores outputs, with the reset reason indicating a watchdog timeout or CATERR. No workaround is available; upgrading to the latest software version is necessary to resolve the issue. Data plane outages will not occur as long as the failover is enabled. This issue is resolved.	4.3(5a)A	4.3(5d)A

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCwm13829	On Cisco UCS X210c M6/M7 servers with a UCSX-X10C-RAIDF RAID controller, a BBU fault may occur, indicated by Safety Status Register 0xf000 in logs. This indicates a corrupted voltage reading, marking the BBU as bad and potentially needing replacement. To resolve, access the RAID setup during boot, reset to factory defaults, confirm, and save changes. This issue is resolved.	4.2(3k)	4.3(5d)
CSCwo05892	Disabling a login profile does not delete the entry, resulting in stale configurations that continue to enforce policies even after disabling. This occurs when the blocking level is set to **all-user** or changed from **all-users** to **per-user**. This issue is resolved.	4.3(5a)	4.3(5d)
CSCwn92039	Cisco UCS Fabric Interconnect resets due to an HA policy triggered by a crash in the `snmpd` service. The issue, categorized as a software fault, results in a core dump and a supervisor reset in VDC 1. This occurs in environments using SNMP for management.	4.3(5a)	4.3(5d)

Resolved Caveats in Release 4.3(5c)

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCwm72893	Under rare conditions, Cisco UCS VIC adapter may experience a firmware hang due to a software anomaly in the embedded CPU (eCPU), leading to a watchdog timeout and Non-Maskable Interrupt (NMI). This can result in temporary storage connectivity loss. This issue is resolved. The latest firmware update addresses this issue by enhancing error-handling mechanisms to prevent such occurrences.	4.2(3i)A	4.3(5c)A
CSCwm36266	In certain conditions, after a watchdog reset or kernel panic, the blade IOM may incorrectly set the blade to Safe Mode, causing fans to spin at full speed. This issue occurs when the CIMC kernel experiences a panic, and before rebooting completes, the IOM misidentifies the CIMC capabilities, leading to an incorrect state. This state persists even after rebooting the CIMC or the blade, resulting in elevated fan speeds. The issue is observed with Cisco UCS B200 M6 blade servers and requires an update to ensure proper IOM communication and blade state management. This issue is resolved.	4.2(3b)B	4.3(5c)B

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCwm83085	In Cisco UCS Manager, changing the FCoE VLAN associated with a VSAN can result in the loss of storage paths from the operating system perspective, even though Fibre Channel interfaces remain active and stable. This issue occurs in Cisco UCS 6454 FI environments using FC Switching mode connected directly to storage. Although the switch accurately reflects the changes, the operating system reports a loss of storage paths. Flapping the FC interfaces temporarily restores connectivity. This issue is resolved.	4.3(5a)	4.3(5c)B
CSCwn42969	After power cycling or resetting a Cisco UCS server, NVME disk FRONT-NVME-2 may become inoperable when left idle for over 1.5 weeks or under minimal workload. If this issue occurs and the drive is inoperable, check your drive PID against Drive PIDs for NVME Disk FRONT-NVME Inoperable Issue - CSCwn42969, on page 72. If listed, contact Cisco TAC for a replacement. If not listed, upgrade to firmware release 9CV10490.	4.3(4e)	4.3(5c)

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCwm47183	Certain HDDs (model MG06SCA800A) unexpectedly show removal marks by the backup application, even though Cisco IMC logs do not indicate any failures. This issue occurs on the Cisco UCS C240 M6 servers with firmware version 4.3(2.240002) equipped with Cisco 12G SAS HBA controller. Disk I/O errors indicate timeouts and read issues, preventing successful mounting and leading to removal marks on the disks. This situation impacts clusters using the backup application, requiring further investigation to prevent disruptions. This issue is resolved.	4.3(2e)C	4.3(5c)C
CSCwm80801	After applying the July 2024 patch KB5040434, you may experience issues logging into UCS devices through Radius, although other Cisco devices remain unaffected. This problem impacts UCS devices. The issue occurs in a system equipped with Cisco UCS 6332 FI managed by Cisco UCS Manager version 4.2(3h), and it may potentially affect any UCS device following the NPS upgrade with the specified patch. This issue is resolved.	4.2(3h)A	4.3(5c)A

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCwn00366	Server discovery failures occur on Cisco UCS C-series FI-managed Intersight Rack Servers with only eNICs or only vHBAs configured, due to a memory leak in the vniccfgd process triggered by the palo_vnic_listtype() API call. Over months, the memory leak accumulates, leading to failures once a threshold is crossed. Cisco UCS VIC 14xx and 15xxx series adapters experience persistent failures, while Cisco UCS VIC 13xx series adapters may reboot due to out-of-memory errors. This issue is resolved.	4.2(3b)	4.3(5c)

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

UCSX-NVME4-1600-D, UCSX-NVME4-1600-D=, HX-NVME4-1600, HX-NVME4-1600=, UCS-NVME4-3200, UCS-NVME4-3200=, UCSB-NVME4-3200, UCSB-NVME4-3200=, UCSX-NVME4-3200, UCSX-NVME4-3200=, UCS-NVME4-3200-D, UCS-NVME4-3200-D=, UCSX-NVME4-3200-D, UCSX-NVME4-3200-D=, HX-NVME4-3200, HX-NVME4-3200=, UCS-NVME4-6400, UCS-NVME4-6400=, UCSB-NVME4-6400, UCSB-NVME4-6400=, UCSX-NVME4-6400, UCSX-NVME4-6400=, UCS-NVME4-6400-D, UCS-NVME4-6400-D=, UCSX-NVME4-6400-D, UCSX-NVME4-6400-D=, HX-NVME4-6400, HX-NVME4-6400=, UCS-NVME4-1920, UCS-NVME4-1920=, UCSB-NVME4-1920, UCSB-NVME4-1920=, UCSX-NVME4-1920, UCSX-NVME4-1920=, UCS-NVME4-1920-D, UCS-NVME4-1920-D=, UCSX-NVME4-1920-D, UCSX-NVME4-1920-D=, HX-NVME4-1920, HX-NVME4-1920=, UCS-NVME4-3840, UCS-NVME4-3840=, UCSB-NVME4-3840, UCSB-NVME4-3840=, UCSX-NVME4-3840, UCSX-NVME4-3840=, UCS-NVME4-3840-D, UCS-NVME4-3840-D=, UCSX-NVME4-3840-D, UCSX-NVME4-3840-D=, HX-NVME4-3840, HX-NVME4-3840=, UCS-NVME4-7680, UCS-NVME4-7680=, UCSB-NVME4-7680, UCSB-NVME4-7680=, UCSX-NVME4-7680, UCSX-NVME4-7680=, UCS-NVME4-7680-D, UCS-NVME4-7680-D=, UCSX-NVME4-7680-D, UCSX-NVME4-7680-D=, HX-NVME4-7680, HX-NVME4-7680=, UCS-NVME4-15360, UCS-NVME4-15360, UCSB-NVME4-15360, UCSB-NVME4-15360, UCSX-NVME4-15360, UCS-NVME4-15360-D, UCSX-NVME4-15360D, HX-NVME4-15360, HX-NVME4-15360, UCSX-NVB1T6O1P, UCSX-NVB1T6O1P=, HX-NVB1T6O1PM6, HX-NVB1T6O1PM6=, UCS-NVB3T2O1PM6, UCS-NVB3T2O1PM6=, UCSB-NVA3T2O1P, UCSB-NVA3T2O1P=, UCSX-NVB3T2O1PM6, UCSX-NVB3T2O1PM6=, UCS-NVB3T2O1P, UCS-NVB3T2O1P=, UCSX-NVB3T2O1P, UCSX-NVB3T2O1P=, HX-NVB3T2O1PM6, HX-NVB3T2O1PM6=, UCS-NVB6T4O1PM6, UCS-NVB6T4O1PM6=, UCSB-NVA6T4O1P,

UCSB-NVA6T4O1P=, UCSX-NVB6T4O1PM6, UCSX-NVB6T4O1PM6=, UCS-NVB6T4O1P, UCS-NVB6T4O1P=, UCSX-NVB6T4O1P, UCSX-NVB6T4O1P=, HX-NVB6T4O1PM6, HX-NVB6T4O1PM6=, UCS-NVB1T9O1VM6, UCS-NVB1T9O1VM6=, UCSB-NVA1T9O1V, UCSB-NVA1T9O1V=, UCSX-NVB1T9O1VM6, UCSX-NVB1T9O1VM6=, UCS-NVB1T9O1V, UCS-NVB1T9O1V=, UCSX-NVB1T9O1V, UCSX-NVB1T9O1V=, HX-NVB1T9O1VM6, HX-NVB1T9O1VM6=, UCS-NVB3T8O1VM6, UCS-NVB3T8O1VM6=, UCSB-NVA3T8O1V, UCSB-NVA3T8O1V=, UCSX-NVB3T8O1VM6, UCSX-NVB3T8O1VM6=, UCS-NVB3T8O1V, UCS-NVB3T8O1V=, UCSX-NVB3T8O1V, UCSX-NVB3T8O1V=, HX-NVB3T8O1VM6, HX-NVB3T8O1VM6=, UCS-NVB7T6O1VM6, UCS-NVB7T6O1VM6=, UCSB-NVA7T6O1V, UCSB-NVA7T6O1V=, UCSX-NVB7T6O1VM6, UCSX-NVB7T6O1VM6=, UCS-NVB7T6O1V, UCS-NVB7T6O1V=, UCSX-NVB7T6O1V, UCSX-NVB7T6O1V=, HX-NVB7T6O1VM6, HX-NVB7T6O1VM6=, UCS-NVB15TO1VM6, UCS-NVB15TO1VM6, UCSB-NVA15TO1V, UCSB-NVA15TO1V, UCSX-NVB15TO1VM6, UCS-NVB15TO1V, UCSX-NVB15TO1V, HX-NVB15TO1VM6, HX-NVB15TO1VM6

Resolved Caveats in Release 4.3(5a)

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCwm67631	After updating the BMC and BIOS, clicking **Power Off** followed by **Reset CMOS** may result in a failure. The server remains powered off even after a Redfish power-on command. This issue occurs with UCS Blade servers equipped with AMD® processors are fully populated with 64GB or higher DIMMs and all drives loaded, not previously powered on. This issue is resolved.	4.3(5a)A	4.3(5a)A

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCwk91747	FC traffic may experience a brief disruption due to the flap of vEth associated with the vFC interfaces in the following scenarios: • Rebooting one of the Fabric Interconnects (affects all servers with vHBAs). • PMON restart (affects all servers with vHBAs). • Making changes to the vNIC or vHBA in the service profile associated with a server (affects the specific server whose service profile is modified). • Loss of CIMC connectivity due to a CIMC reset or other issues (affects the specific server with CIMC connectivity issues). This disruption can cause an FC traffic outage and may result in the operating system hanging, requiring a reset to restore normal functionality. This issue impacts vFC interfaces corresponding to the vHBAs and FC traffic of the servers only. It does not impact the vNIC interfaces and Ethernet traffic of the servers.	4.3(4a)A	4.3(5a)A

Resolved Caveats in Release 4.3(4f)

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCwn42969	After power cycling or resetting a Cisco UCS server, NVME disk FRONT-NVME-2 may become inoperable when left idle for over 1.5 weeks or under minimal workload. If this issue occurs and the drive is inoperable, check your drive PID against Drive PIDs for NVME Disk FRONT-NVME Inoperable Issue - CSCwn42969, on page 75. If listed, contact Cisco TAC for a replacement. If not listed, upgrade to firmware release 9CV10490.	4.3(4e)	4.3(4f)

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

UCSX-NVME4-1600-D, UCSX-NVME4-1600-D=, HX-NVME4-1600, HX-NVME4-1600=, UCS-NVME4-3200, UCS-NVME4-3200=, UCSB-NVME4-3200, UCSB-NVME4-3200=, UCSX-NVME4-3200, UCSX-NVME4-3200=, UCS-NVME4-3200-D, UCS-NVME4-3200-D=, UCSX-NVME4-3200-D, UCSX-NVME4-3200-D=, HX-NVME4-3200, HX-NVME4-3200=, UCS-NVME4-6400, UCS-NVME4-6400=, UCSB-NVME4-6400, UCSB-NVME4-6400=, UCSX-NVME4-6400, UCSX-NVME4-6400=, UCS-NVME4-6400-D, UCS-NVME4-6400-D=, UCSX-NVME4-6400-D, UCSX-NVME4-6400-D=, HX-NVME4-6400, HX-NVME4-6400=, UCS-NVME4-1920, UCS-NVME4-1920=, UCSB-NVME4-1920, UCSB-NVME4-1920=, UCSX-NVME4-1920, UCSX-NVME4-1920=, UCS-NVME4-1920-D, UCS-NVME4-1920-D=, UCSX-NVME4-1920-D, UCSX-NVME4-1920-D=, HX-NVME4-1920, HX-NVME4-1920=, UCS-NVME4-3840, UCS-NVME4-3840=, UCSB-NVME4-3840, UCSB-NVME4-3840=, UCSX-NVME4-3840, UCSX-NVME4-3840=, UCS-NVME4-3840-D, UCS-NVME4-3840-D=, UCSX-NVME4-3840-D, UCSX-NVME4-3840-D=, HX-NVME4-3840, HX-NVME4-3840=, UCS-NVME4-7680, UCS-NVME4-7680=, UCSB-NVME4-7680, UCSB-NVME4-7680=, UCSX-NVME4-7680, UCSX-NVME4-7680=, UCS-NVME4-7680-D, UCS-NVME4-7680-D=, UCSX-NVME4-7680-D, UCSX-NVME4-7680-D=, HX-NVME4-7680, HX-NVME4-7680=, UCS-NVME4-15360, UCS-NVME4-15360, UCSB-NVME4-15360, UCSB-NVME4-15360, UCSX-NVME4-15360, UCS-NVME4-15360-D, UCSX-NVME4-15360D, HX-NVME4-15360, HX-NVME4-15360, UCSX-NVB1T6O1P, UCSX-NVB1T6O1P=, HX-NVB1T6O1PM6, HX-NVB1T6O1PM6=, UCS-NVB3T2O1PM6, UCS-NVB3T2O1PM6=, UCSB-NVA3T2O1P, UCSB-NVA3T2O1P=, UCSX-NVB3T2O1PM6, UCSX-NVB3T2O1PM6=, UCS-NVB3T2O1P, UCS-NVB3T2O1P=, UCSX-NVB3T2O1P, UCSX-NVB3T2O1P=, HX-NVB3T2O1PM6, HX-NVB3T2O1PM6=, UCS-NVB6T4O1PM6, UCS-NVB6T4O1PM6=, UCSB-NVA6T4O1P,

UCSB-NVA6T4O1P=, UCSX-NVB6T4O1PM6, UCSX-NVB6T4O1PM6=, UCS-NVB6T4O1P, UCS-NVB6T4O1P=, UCSX-NVB6T4O1P, UCSX-NVB6T4O1P=, HX-NVB6T4O1PM6, HX-NVB6T4O1PM6=, UCS-NVB1T9O1VM6, UCS-NVB1T9O1VM6=, UCSB-NVA1T9O1V, UCSB-NVA1T9O1V=, UCSX-NVB1T9O1VM6, UCSX-NVB1T9O1VM6=, UCS-NVB1T9O1V, UCS-NVB1T9O1V=, UCSX-NVB1T9O1V, UCSX-NVB1T9O1V=, HX-NVB1T9O1VM6, HX-NVB1T9O1VM6=, UCS-NVB3T8O1VM6, UCS-NVB3T8O1VM6=, UCSB-NVA3T8O1V, UCSB-NVA3T8O1V=, UCSX-NVB3T8O1VM6, UCSX-NVB3T8O1VM6=, UCS-NVB3T8O1V, UCS-NVB3T8O1V=, UCSX-NVB3T8O1V, UCSX-NVB3T8O1V=, HX-NVB3T8O1VM6, HX-NVB3T8O1VM6=, UCS-NVB7T6O1VM6, UCS-NVB7T6O1VM6=, UCSB-NVA7T6O1V, UCSB-NVA7T6O1V=, UCSX-NVB7T6O1VM6, UCSX-NVB7T6O1VM6=, UCS-NVB7T6O1V, UCS-NVB7T6O1V=, UCSX-NVB7T6O1V, UCSX-NVB7T6O1V=, HX-NVB7T6O1VM6, HX-NVB7T6O1VM6=, UCS-NVB15TO1VM6, UCS-NVB15TO1VM6, UCSB-NVA15TO1V, UCSB-NVA15TO1V, UCSX-NVB15TO1VM6, UCS-NVB15TO1V, UCSX-NVB15TO1V, HX-NVB15TO1VM6, HX-NVB15TO1VM6

Resolved Caveats in Release 4.3(4e)

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCwk91747	FC traffic may experience a brief disruption due to the flap of vEth associated with the vFC interfaces in the following scenarios: • Rebooting one of the Fabric Interconnects (affects all servers with vHBAs). • PMON restart (affects all servers with vHBAs). • Making changes to the vNIC or vHBA in the service profile associated with a server (affects the specific server whose service profile is modified). • Loss of CIMC connectivity due to a CIMC reset or other issues (affects the specific server with CIMC connectivity issues). This disruption can cause an FC traffic outage and may result in the operating system hanging, requiring a reset to restore normal functionality. This issue impacts vFC interfaces corresponding to the vHBAs and FC traffic of the servers only. It does not impact the vNIC interfaces and Ethernet traffic of the servers.	4.3(4a)A	4.3(4e)A

Resolved Caveats in Release 4.3(4d)

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCwm49499	Upgrading Cisco UCS 6454 Fabric Interconnect from version 4.2(3h) to 4.3(4a) fails due to DME core file generation when Cisco UCS Manager setup includes Cisco UCS S3260 servers with Local LUN configured through a Storage Profile. This issue causes Cisco UCS Manager to become inaccessible post-upgrade. This issue is resolved.	4.3(4a)A	4.3(4d)A
CSCwm55862	In a Cisco UCS Central managed UCS domain, after upgrading Cisco UCS Manager to version 4.3(4a) or later, you are unable to use the **Use Global** option to convert local policies to global policies. The error message indicates that policy ownership cannot be modified to global due to a reference to a local policy. This issue is resolved.	4.3(4a)A	4.3(4d)A

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCwk92950	When attempting to update the firmware for servers equipped with two H100-NVL GPUs, the firmware update process fails during activation in Cisco UCS Manager. This issue occurs when there are two GPU cards of the same version, such as A10, A40, A100-80, A16, A30, H100-80, and L40S. The failure is indicated by error code 4131 and results in the GPU firmware update not being completed. This issue is resolved.	4.3(4d)A	4.3(4d)A
CSCwm44591	After upgrading the Cisco UCS Manager infrastructure firmware to version 4.3(4a), the Cisco UCS 6454 Fabric Interconnects stopped using the **10G_ETH_PORT_ACTIVATION_PKG** license and switched to the standard **ETH_PORT_ACTIVATION_PKG** license. This change results in a mismatch in license usage, triggering a grace period warning due to the overuse of the standard license. The system displays the error: `One or more ports with license type ETH_PORT_ACTIVATION_PKG on fabric-interconnect A have started using license grace period.` This issue is resolved.	4.3(4a)A	4.3(4d)A

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCwm02539	Booting from SAN sometimes fails to UEFI shell because an array is sending an ADISC to the initiator, or the initiator is sending an IO command before the connection is fully negotiated. This happens when multiple servers are booting from SAN to a target that uses ADISC to build the connection. This issue is resolved.	4.3(4a)B	4.3(4d)B

Resolved Caveats in Release 4.3(4c)

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCwk28221	When changing the FCoE VLAN from 3121 to 3120 in Cisco UCS Manager while FI is in FC Switch mode, initiators can FLOGI and obtain FCID but fail to PLOGI to target ports, resulting in indefinite timeouts. Admin down/up of the FC link or port-channel resolves the issue. This change causes path loss in ESXi, with host logs showing successful FLOGI and FCID assignment but PLOGI timeouts. This issue is resolved.	4.3(2b)	4.3(4c)

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCwk29071	On Cisco UCS-FI-6332-16UP FI running release 4.1(3j), the **Transmit Fault Count** increases by 3 when executing the show interface transceiver details command or generating tech support logs. This issue is observed on Fabric Interconnects (FI-A and FI-B) equipped with Cisco FINISAR SFP modules (DS-SFP-FC16G-SW) but does not occur with Cisco AVAGO SFP modules. The increment is specific to Cisco FINISAR SFP modules and does not indicate any hardware errors. This issue is resolved.	4.1(3j)A	4.3(4c)A
CSCwk49974	Cisco UCS-FI-6454 Fabric Interconnects Cisco UCS Manager release 4.3(4a) experience unexpected reboots when performing SNMP bulkwalkget requests with packet sizes greater than the MTU (1500). This issue is due to SNMP jumbo packet fragmentation, leading to kernel panics and high impact on data traffic if failover is not configured. This issue is resolved.	4.3(3a)A	4.3(4c)A

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCwk09092	During an upgrade of Cisco UCS Manager from 4.2(3g) to 4.3(3a) on Cisco UCS-FI-6454 Fabric Interconnects in UCS Manager Cluster mode, the Data Management Engine (DME) consumes 100% of FI CPU resources, leading to significant slowness. This results in the DME being inaccessible and unable to use scope commands. The Cisco UCS Manager GUI becomes inaccessible, CLI logins take excessive time and often fall to the default role regardless of the account, and changes in Cisco UCS Manager cannot be made. The issue persists through failover, pmon stop/start, and container restarts. This issue is resolved.	4.3(3a)A	4.3(4c)A

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCwf96053	When deploying a new Cisco UCS Domain within a Cisco UCS Central environment, global identifiers such as MAC pools, UUID pools, and iSCSI IP pools are not visible on Cisco UCS 6454 FI domains. This issue does not affect Cisco UCS 6300 FI. The issue occurs with Cisco UCS Central 2.0(1r) and Cisco UCS Manager 4.2(3d) on Cisco UCS 6454 FI, while Cisco UCS Manager 4.2(2c) or 4.2(1d) on Cisco 6300 FI works fine. The issue persists despite pushing global policies and identifiers from Cisco UCS Central. This issue is resolved.	4.2(3k)A	4.3(4c)A

Defect ID	Symptom	First Bundle Affected	Resolved in Release

CSCwk66102	After upgrading Cisco UCS Manager from 4.3(2e)A to 4.3(3c)A on Cisco UCSX-FI-6536 Fabric Interconnects, the Communication Service FSM fails with the following error:
	`[FSM:FAILED]: communication service configuration (FSM:sam:dme:CommSvcEpUpdateSvcEp).`
	`Remote-Invocation-Error:`
	`name to naming property('snmpCommSecP.name')`
	`mismatch: Rn: '[SNMP String]', Prop:'SNMP String'`
	This issue occurs despite the SNMP string being correctly set. The failure may impact LDAP authentication if FQDN is used for the LDAP server(s) due to DNS not being programmed when the FSM fails.
	This issue is resolved.
		4.3(3c)A	4.3(4c)A

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCwm02504	When updating the UBM firmware on Cisco UCS X210c M6 servers with UCSX-X10C-RAIDF, the update may fail with the following error: `Error: Failed to get product serial number` This results in the UBM getting stuck in an activating state, which can be observed under the installed firmware tab by expanding the RAID controller. This issue is typically found in IMM-based firmwares, as no UCS Manager firmwares have featured a 0x42e UBM firmware. This issue is resolved.	4.3(3a)A	4.3(4c)A

Resolved Caveats in Release 4.3(4b)

There are no resolved caveats in release 4.3(4b).

Resolved Caveats in Release 4.3(4a)

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCwf49262	UCS Manager prevents VLAN ID 1 from being employed as a Q-in-Q VLAN unless the default name of the VLAN, which is **default**, is modified by a user. This issue is resolved.	4.3(2b)	4.3(4a)

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCwd35712	A critical defect has been identified in the Cisco UCS Manager where the Data Management Engine (DME) crashes due to an **instance id not found** error. Additional symptoms include the inability to access the Cisco UCS Manager GUI, non-functionality of cluster management services, and a core dump indicated by the **show pmon state** command via SSH. The problem is not firmware-specific and can impact any Cisco UCS Manager domain. Although the data plane and server operations of the domain remain unaffected, there is no workaround for this issue, and affected environments may require restoration from a backup. This issue is resolved.	4.2(1d)	4.3(4a)

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCwj01478	During the deployment of Cisco UCSX-9508 chassis equipped with Cisco UCS 6454 FI and Cisco UCS 9108 25G Intelligent Fabric Module (IFM) with Cisco UCS Manager integration, the PSU view displays **Power: Error** and **Input Source: Unknown**, despite the physical server PSU LEDs showing green. Major faults in Cisco UCS Manager persist even after decommissioning and re-acknowledging the chassis.	4.3(2b)A	4.3(4a)

Resolved Caveats in Release 4.3(3c)

The following caveat is resolved in Release 4.3(3c):

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCwj08579	In a setup equipped with Cisco UCSX-9508 Chassis, there is an issue where the values for the PowerExtended Policy VextendedMode attribute do not get communicated to the IFM, despite the Cisco UCS Manager GUI accurately reflecting the updated values. This discrepancy occurs following modifications made through Cisco UCS Central. This issue is resolved.	4.3(3a)A	4.3(3c)A

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCwj00344	Cisco UCS Manager may report insufficient power during discovery and deep discovery phases. This issue is resolved. Cisco UCS Manager is updated to report real-time power available in Cisco UCSX-9508 Chassis equipped with Cisco UCS X-Series servers. This enhancement helps you to monitor power during discovery and deep discovery phases when the chassis available power is limited.	4.3(3a)A	4.3(3c)A

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCwj54974	After upgrading Cisco UCS Manager to release 4.3(3c) version, a Cisco UCS X-Series server may revert to using the maximum power budget listed in the catalog if Cisco UCS Manager is unable to perform real-time power profiling accurately. This could lead to a situation where Cisco UCS Manager predicts insufficient power budget allocation, which might prevent the server from being discovered or associated successfully. This issue occurs under following conditions: • UEFI BIOS Boot Security is enabled and applied to a server from Boot Order Service Profile Policy. • Global Power Profiling Policy is enabled. • A server is discovered or re-acknowledged before the activation of the host firmware pack version 4.3(3c). • Either the Grid Power mode is activated, or there is a reduced number of power supply units in a chassis. This issue is resolved.	4.3(3a)B	4.3(3c)B

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCwj28488	Cisco UCS server is unable to start the PNUOS because BIOS/bt/biosSecureVars/dbx_os file with an invalid certificate prevents PNUOS from operating. The `dbx_os` file holds certificates added by the operating system and specifies which certificates are prohibited from loading. The cause of the failure is a secure boot violation and following error message is displayed: `Invalid signature detected. Check secure boot policy in setup` This issue is resolved.	4.3(3a)A	4.3(3c)A

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(2f)

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

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCwm72893	Under rare conditions, Cisco UCS VIC adapter may experience a firmware hang due to a software anomaly in the embedded CPU (eCPU), leading to a watchdog timeout and Non-Maskable Interrupt (NMI). This can result in temporary storage connectivity loss. This issue is resolved. The latest firmware update addresses this issue by enhancing error-handling mechanisms to prevent such occurrences.	4.2(3i)A	4.3(2f)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
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
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

Defect ID	Symptom	First Bundle Affected	Resolved in Release
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
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
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.

Open caveats in Release 4.3(6i)

The following caveat is open in release 4.3(6i):

Defect ID	Symptom	Workaround	First Bundle Affected
CSCwv95321	The SAM Controller restarts the DME process prematurely during a prolonged FI cluster switchover when the switchover exceeds the configured timeout. This restart occurs even though the switchover is still in progress, causing the failover to not complete and the system to remain in its previous high-availability state. The issue typically happens after a cluster lead change in setups with multiple servers, blades, or chassis, triggered via CLI or automation. There is no impact on data traffic during this condition.	There is no known workaround.	4.3(6i)

Open caveats in Release 4.3(6h)

There are no open caveats in release 4.3(6h).

Open Caveats for Release 4.3(6g)

The following caveat is open in release 4.3(6g):

Defect ID	Symptom	Workaround	First Bundle Affected
CSCwt96184	After server decommission and recommission for the Cisco UCS M6 rack servers, the Cisco UCS 15428 VIC adapter remains stuck in the **Inoperable** state. The server fails to receive discovery from Cisco UCS Manager due to a DHCP packet parsing error at the Baseboard Management Controller (BMC). This error occurs because the DHCP packet contains extra fields or characters, causing Cisco UCS Manager initialization to fail with a `FATAL ERROR! Invalid UCSM DHCP mode token` message and aborting the mode change process. This issue prevents proper adapter operation and server discovery.	This issue occurs during the decommission or recommission process while the system is in maintenance mode. To resolve this, reboot the BMC.	4.3(6f)
CSCwd00735	In a setup equipped with Cisco UCS 6300 series Fabric Interconnects or with Cisco UCS Mini, downloading a C-Series bundle larger than 2 GB can fail with an invalid image error.	Upgrade the infrastructure A bundle to release 4.3(6).	4.2(2c)

Open Caveats for Release 4.3(6f)

The following caveats are open in Release 4.3(6f):

Defect ID	Symptom	Workaround	First Bundle Affected
CSCwr21671	Cisco UCS B200 M5 blade servers equipped with 12G RAID controllers, recurring hardware errors may cause storage controller failures and server outages. Affected systems may report L2/L3 cache errors on the RAID controller, trigger Cisco UCS Manager `equipment inoperable` faults, and experience unexpected system crashes or reboots.	**1.** When the error message is displayed during boot, press **x** to allow the server to continue starting. **2.** Power off the server and reseat the RAID controller.	4.3(6f)
CSCwt28631	Telnet remote user sessions cannot execute the `connect nxos` command because Telnet does not establish a secure remote login environment, and the required environment variable `UCSM_IS_REMOTE_LOGIN=1` is not set. This prevents the AAA FSM from completing and causes the system to block the command. SSH sessions successfully execute `connect nxos` as they create a validated remote login context.	Use SSH instead of Telnet, as SSH sets the required environment variable UCSM_IS_REMOTE_LOGIN=1, enabling secure remote login and proper command execution. Disable Telnet access if it is not needed. Limit management access to secure protocols like SSH to ensure secure authentication and system operation.	4.3(6f)

Open Caveats for Release 4.3(6e)

There are no open caveats in Release 4.3(6e).

Open Caveats for Release 4.3(6d)

There are no open caveats in Release 4.3(6d).

Open Caveats for Release 4.3(6c)

The following caveats are open in Release 4.3(6c).

Defect ID	Symptom	Workaround	First Bundle Affected
CSCwj57044	Cisco UCS VIC 1400 and 15000 series adapters configured in EtherChannel mode may experience lower than expected TCP/UDP throughput. Network bandwidth does not scale to the combined line rate of the physical links. This issue is observed with Quad Port adapters when used in port-channel configurations.	There is no known workaround.	4.3(2e)

Defect ID	Symptom	Workaround	First Bundle Affected
CSCws30219	Cisco UCS M7 servers managed by Cisco UCS Manager with server bundle versions 4.3(6c), 4.3(6d), 6.0(1b), 6.0(1c), and 6.0(1d) are susceptible to host lockups triggered by ECC (Error Correcting Code) memory events. This issue is specifically related to how the server BIOS interacts with the Extensible Firmware Interface (EFI) during error conditions. During these events, the BIOS does not correctly retrieve a required variable, causing EFI to return an invalid parameter. As a result, the operating system is unable to continue normal operation and freezes without logging any errors. When this occurs, the host becomes unresponsive and KVM input is not accepted. Single-bit ECC errors—while not logged due to DDR5 specifications—can trigger this condition, resulting in complete loss of host responsiveness.	Downgrade the server bundle to release 4.3(6b) or an earlier server bundle.	4.3(6c) server bundle B/C

Open Caveats for Release 4.3(6b)

There are no open caveats in Release 4.3(6b).

Open Caveats for Release 4.3(6a)

The following caveats are open in Release 4.3(6a).

Defect ID	Symptom	Workaround	First Bundle Affected
CSCwo57642	An issue arises when attempting to power on an Cisco US X210c M7 blade server with a PCIe X440p attached in a chassis within a capped Power Group. The blade fails to boot, displaying the error message **Insufficient power available to power on server.** This problem occurs even if other blades in the chassis are already discovered and operational.	Move the chassis to an unbounded Power Group and then move back to the Capped Power Group once the discovery is done.	4.3(4a)
CSCwo77289	After upgrading Cisco UCS B200 M5 server, equipped with M2 disks with UCS-M2-HWRAID controllers, to release 4.3(5c), a degraded status due to drive temperatures exceeding the 70°C threshold, with recorded temperatures reaching 75°C is reported. This causes instability across UCS domains, resulting in alerts for exceeding temperature limits.	Downgrade to release 4.3(5a).	4.3(5a)B
CSCwm45755	In Cisco UCS C220 M8 servers equipped with M.2 disks connected to a storage controller, the disks are not detected on the Windows Server 2025 installation page. However, the disks are detected during the installation of Windows Server 2022. This issue occurs specifically with Windows Server 2025.	There is no known workaround.	4.3(6a)

Defect ID	Symptom	Workaround	First Bundle Affected
CSCwn99720	On Cisco UCS C-Series M8 servers with Intel processors and an R1S CPU configured in a single CPU setup on the 2S platform, Intel SGX remains disabled even after being enabled in the BIOS. This issue does not occur with a dual CPU configuration.	There is no known workaround.	4.3(6a)
CSCwn51498	Raw OEM SEL records are logged in CIMC SEL during the booting and shutdown of Windows Server 2025 on Cisco UCS C220 M8 servers.	Ignore the Raw OEM SEL records logged while booting Windows 2025.	4.3(6a)

Open Caveats for Release 4.3(5d)

There are no open caveats in Release 4.3(5d).

Open Caveats for Release 4.3(5c)

There are no open caveats in Release 4.3(5c).

Open Caveats for Release 4.3(5a)

There are no open caveats in Release 4.3(5a).

Open Caveats for Release 4.3(4f)

There are no open caveats in Release 4.3(4f).

Open Caveats for Release 4.3(4e)

There are no open caveats in Release 4.3(4e).

Open Caveats for Release 4.3(4d)

There are no open caveats in Release 4.3(4d).

Open Caveats for Release 4.3(4c)

The following caveats are open in Release 4.3(4c).

Defect ID	Symptom	Workaround	First Bundle Affected
CSCwm09720	In Cisco UCS Manager releases 4.3(3) and 4.3(4), the MC Server generates a high volume of delta events in Cisco UCS X9508 chassis, causing a flood of events to Cisco bladeAG. This results in continuous Cisco bladeAG crashes, preventing blade discovery and user SP operations. The issue is due to the mc_delta_psu_fw_version function incorrectly setting the "used" length, generating unnecessary 256KB delta events. Initializing the "used" length to 0 prevents these delta events.	To mitigate this issue, contact Cisco TAC to increase the bladeAG virtual memory limit to 800MB.	4.3(3c)C
CSCwk82692	In Cisco UCS Manager releases 4.3(3a) through 4.3(4b) on Cisco UCS 6454/64108/6536 Fabric Interconnects, bladeAG processes may reach the 400MB memory limit and crash due to memory aborts. This results in blades being stuck in a consistent discovery loop. The bladeAG service experience multiple restarts, causing users to be unable to perform blade operations such as power on/off and complete discovery until the process stabilizes. This issue is observed in domains with a minimum of 16+ Cisco UCS X-Series chassis.	To mitigate this issue, contact Cisco TAC to increase the bladeAG virtual memory limit.	4.3(3c)A

Defect ID	Symptom	Workaround	First Bundle Affected
CSCwk68790	Solidigm NVMe U.2 Drive information is partially inventoried on Cisco UCS M5 Rack servers. Missing details include PID, VID, Vendor name, Product Name, model version, package version, and startup version. This results in incomplete inventory information being displayed.	Solidigm drives are supported on Cisco UCS M5 and M6 rack servers, but the missing data (PID, VID, Vendor name, Product Name, model version, package version, startup version) are not displayed.	4.3(4c)A and C
CSCwm06144	When installing Solidigm NVMe drives in Cisco UCS M7 Blade servers, the PCIe Address property is not visible in the Cisco UCS Manager GUI Inventory under **Inventory** > **Storage** > **Controller**. Despite this, the drives are discovered and usable.	There is no known workaround.	4.3(4c)A

Open Caveats for Release 4.3(4b)

The following caveats are open in Release 4.3(4b).

Defect ID	Symptom	Workaround	First Bundle Affected
CSCwk45543	Cisco UCS C245 M8 Server hybrid display incorrectly shows two Ethernet ports on the rear image of the server; these ports are not physically present and will be removed to reflect the actual hardware configuration.	This is a display only issue. There is no functionality impact.	4.3(4b)

Open Caveats for Release 4.3(4a)

The following caveats are open in Release 4.3(4a):

Defect ID	Symptom	Workaround	First Bundle Affected
CSCwj61708	When performing a warm reboot of multiple servers in a scale-setup of 160 servers and high PV count of greater than 64K in Cisco UCS FI domain, secure boot adapters may not restart instantly under certain situations. This was observed in a scale setup where simultaneous warm reboot of 22 blades across three chassis was initiated. Some blades with Cisco UCS VIC 15000 series secure boot adapters failed to boot from the SAN after a soft reboot. These adapters execute a cleanup process with the Fabric Interconnects to maintain system integrity, which needs to be finished before the server BIOS can recognize the adapters. This issue arises specifically under conditions of very high PV count or exceptionally high CPU utilization on the FI. During these instances, if the server BIOS finalizes the boot sequence before the secure boot adapters finish the cleanup, the adapters may fail to be detected. Consequently, the server may not successfully boot from the SAN. This issue is observed in configurations using Cisco UCS blade servers equipped with Cisco UCS VIC 15000 series adapters.	Reboot the failed servers.	4.3(4a)

Defect ID	Symptom	Workaround	First Bundle Affected
CSCwi70374	If you have configured Cisco UCS Manager to only allow **TLSv1.3** under the **Allowed SSL Protocols** setting, connection to UCS Central fails. Cisco UCS Central connects using an older version of TLS (such as TLSv1.2 or earlier).	Use **TLS 1.2 only**.	4.3(4a)
CSCwj40445	The issue is seen in Cisco UCS Central where updating a Global Service Profile Template with certain number of Service Profiles and analyzing the impact of a host firmware policy change erroneously reports incorrect number of affected servers. This problem occurs when the Service Profiles are from different sub-organizations; however, it does not manifest when Service Profiles are from the same sub-organization.	In Cisco UCS Central, create a new Host Firmware Policy with the same package but ensure it is not in use. Apply this policy to the Service Profile Template in question, run impact analysis, and if the expected number of affected profiles is reported, you may safely save and proceed with the changes.	4.3(2b)A

Defect ID	Symptom	Workaround	First Bundle Affected
CSCwk91747	FC traffic may experience a brief disruption due to the flap of vEth associated with the vFC interfaces in the following scenarios: • Rebooting one of the Fabric Interconnects (affects all servers with vHBAs). • PMON restart (affects all servers with vHBAs). • Making changes to the vNIC or vHBA in the service profile associated with a server (affects the specific server whose service profile is modified). • Loss of CIMC connectivity due to a CIMC reset or other issues (affects the specific server with CIMC connectivity issues). This disruption can cause an FC traffic outage and may result in the operating system hanging, requiring a reset to restore normal functionality. This issue impacts vFC interfaces corresponding to the vHBAs and FC traffic of the servers only. It does not impact the vNIC interfaces and Ethernet traffic of the servers.	The FC traffic recover automatically after a brief disruption. If the operating system hangs, a reset may be required to restore normal functionality.	4.3(4a)

Open Caveats for Release 4.3(3c)

There are no open caveats in Release 4.3(3c).

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
CSCwd35712	A critical defect has been identified in the Cisco UCS Manager where the Data Management Engine (DME) crashes due to an **instance id not found** error. Additional symptoms include the inability to access the Cisco UCS Manager GUI, non-functionality of cluster management services, and a core dump indicated by the **show pmon state** command via SSH. The problem is not firmware-specific and can impact any Cisco UCS Manager domain. Although the data plane and server operations of the domain remain unaffected, there is no workaround for this issue, and affected environments may require restoration from a backup.	There is no known workaround. Restore the domain from backup.	4.2(1d)

Defect ID	Symptom	Workaround	First Bundle Affected
CSCwj01478	During the deployment of Cisco UCSX-9508 chassis equipped with Cisco UCS 6454 FI and Cisco UCS 9108 25G Intelligent Fabric Module (IFM) with Cisco UCS Manager integration, the PSU view displays **Power: Error** and **Input Source: Unknown**, despite the physical server PSU LEDs showing green. Major faults in Cisco UCS Manager persist even after decommissioning and re-acknowledging the chassis.	Reboot the primary IFM.	4.3(2b)A

Open Caveats for Release 4.3(2f)

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

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.
		`cryptoRecoveryKey=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)
CSCwd35712	A critical defect has been identified in the Cisco UCS Manager where the Data Management Engine (DME) crashes due to an **instance id not found** error. Additional symptoms include the inability to access the Cisco UCS Manager GUI, non-functionality of cluster management services, and a core dump indicated by the **show pmon state** command via SSH. The problem is not firmware-specific and can impact any Cisco UCS Manager domain. Although the data plane and server operations of the domain remain unaffected, there is no workaround for this issue, and affected environments may require restoration from a backup.	There is no known workaround. Restore the domain from backup.	4.2(1d)

Known Behavior and Limitations in Release 4.3

Known behaviors and limitations in Release 4.3(6i)

There are no known behaviors and limitations in release 4.3(6i).

Known behaviors and limitations in Release 4.3(6h)

There are no known behaviors and limitations in release 4.3(6h).

Known Behavior and Limitations in Release 4.3(6g)

There are no known behavior and limitations in Release 4.3(6g).

Known Behavior and Limitations in Release 4.3(6f)

There are no known behavior and limitations in Release 4.3(6f).

Known Behavior and Limitations in Release 4.3(6e)

There are no known behavior and limitations in Release 4.3(6e).

Known Behavior and Limitations in Release 4.3(6d)

There are no known behavior and limitations in Release 4.3(6d).

Known Behavior and Limitations in Release 4.3(6c)

There are no known behavior and limitations in Release 4.3(6c).

Known Behavior and Limitations in Release 4.3(6b)

There are no known behavior and limitations in Release 4.3(6b).

Known Behavior and Limitations in Release 4.3(6a)

Defect ID	Symptom	Workaround	First Bundle Affected
CSCwo27237	During Microsoft Windows 2025® operating system installations on any Cisco UCS M8 servers equipped with Intel® processor (both rack and blade configurations) with VMD enabled in the BIOS, the loading of the F6 Intel VMD driver may experience a longer-than-usual delay. The time required to display NVMe drives increases with the number of NVMe drives present in the system.	Once the windows installer screen appears, perform the following steps: 1. Click **Load VMD** driver once and wait upto 3 mins before you hit refresh. 2. If the drives are not listed, load driver the second time. If you see any error message, click the back button to search for the disks again. All the NVMe drive should be visible now.	4.3(6a)

Known Behavior and Limitations in Release 4.3(5d)

There are no known behavior and limitations in Release 4.3(5d).

Known Behavior and Limitations in Release 4.3(5c)

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

Known Behavior and Limitations in Release 4.3(5a)

Defect ID	Symptom	Workaround	First Bundle Affected
CSCwm70985	During or immediately after a firmware upgrade/downgrade on NVIDIA L40s GPUs, no read/write operations should be performed on the card. However, PNUOS performs read operations using the **`nvidia-smi`** utility to check the GPU mode immediately after the upgrade. This issue occurs when upgrading/downgrading firmware on NVIDIA L40 GPUs, causing PNUOS to crash and raise a major fault. As a result, Cisco UCS Manager does not support mode switch for NVIDIA L40 GPUs from release 4.3(5a) onwards.	You can perform mode changes using NVIDIA tools on the host OS if required. This limitation does not affect other L-series GPUs, which continue to support mode changes.	4.3(5a)
CSCwj96037	In an ESXi 8.0U2 environment with VMs running RHEL9.3/RHEL9.4, there are observed issues when hot-pluggable Intel® and Micron® NVMe drives are removed or inserted. Commands such as lsblk, lspci, and nvme list do not update correctly, resulting in incorrect drive information and potential VM power-off. VMs may not properly recognize and update new drive information after NVMe drive removal or insertion.	Perform the following steps to ensure that VM can detect the newly inserted NVME drive: 1. Power off VM. 2. Add PCIe NVME Drive to VM Config. 3. Power on VM.	4.3(5a)

Known Behavior and Limitations in Release 4.3(4f)

There are no known behavior and limitations in Release 4.3(4f).

Known Behavior and Limitations in Release 4.3(4e)

There are no known behavior and limitations in Release 4.3(4e).

Known Behavior and Limitations in Release 4.3(4d)

There are no known behavior and limitations in Release 4.3(4d).

Known Behavior and Limitations in Release 4.3(4c)

There are no known behavior and limitations in Release 4.3(4c).

Known Behavior and Limitations in Release 4.3(4b)

Defect ID	Symptom	Workaround	First Bundle Affected
CSCwk45449	Enhanced VIC-FPGA and Storage PSOC: Once updated to the latest version, the high FPGA/PSOC version is irreversible and cannot be downgraded; however, firmware versions remain flexible for downgrade or upgrade. The PSOC component within any storage controllers is not eligible for downgrade after upgrade; users can only adjust the firmware version as needed.	The PSOC version is fixed post-upgrade and cannot revert to a previous version. Plan your upgrades accordingly, as this change is permanent. Downgrading the PSOC component is intentionally restricted by design. Ensure that all necessary considerations are made before initiating an upgrade.	4.3(4b)

Known Behavior and Limitations in Release 4.3(4a)

Defect ID	Symptom	Workaround	First Bundle Affected
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)

Defect ID	Symptom	Workaround	First Bundle Affected
CSCwc85559	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)

Known Behavior and Limitations in Release 4.3(3c)

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

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(2f)

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

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)
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)

Compatibility

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.

Cisco UCS Equivalency Matrix for Cisco Intersight, Cisco IMC, and Cisco UCS Manager outlines the release timeline for Cisco Intersight, Cisco Integrated Management Controller (IMC), and Cisco UCS Manager (UCSM). It includes essential information such as the date each patch was posted, the specific patch version, and the platforms that are supported by each release. By referring to this matrix, you can identify the appropriate firmware and software versions required for your servers before migrating them to Cisco Intersight. This ensures that your server infrastructure remains supported and operates efficiently during and after the transition.

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

Table 6: 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(6)	4.3(6)	All M8, M7, M6, and S3260 M5
	4.3(2)	All M5
4.3(5)	4.3(5)	All M8, M7, and M6
	4.3(4)	S3260 M5
	4.3(2)	All M5
4.3(4)	4.3(4)	C245 M8 All M7, M6, and S3260 M5
	4.3(2)	All M5
4.3(3)	4.3(3)	All M7, M6, and S3260 M5
	4.3(2)	All 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

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

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

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). To help you quickly verify valid combinations, this release includes an interactive compatibility tool, available here:

Cisco UCS Manager Cross Version Firmware Matrix

By selecting a Fabric Interconnect model along with the desired Infrastructure (A Bundle) and Host Firmware (B and C Bundles) releases, the tool dynamically displays whether each combination is a supported configuration.

You may also view the extended version of the Mixed Cisco UCS Releases Supported on Cisco UCS Fabric Interconnects at Cisco UCS Manager Cross-Version Firmware Support, Release 4.3.

For reference, the Cisco UCS Equivalency Matrix for Cisco Intersight, Cisco IMC, and Cisco UCS Managementoutlines the release timeline for Cisco Intersight, Cisco Integrated Management Controller (Cisco IMC), and Cisco UCS Manager. It includes essential information such as the date each patch was posted, the specific patch version, and the platforms that are supported by each release. By referring to this matrix, you can identify the appropriate firmware and software versions required for your servers before migrating them to Cisco Intersight. This ensures that your server infrastructure remains supported and operates efficiently during and after the transition.



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.

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(6)

- In a setup equipped with Cisco UCS C240 M8 Server, UCS C220 M8 Server, or UCS X210c M8 Compute Node, you cannot downgrade Infrastructure Firmware Version (A Bundle) or Host Firmware Version (C or B Bundle) to any release earlier than 4.3(6a).
- If you enable the Package Power Limit (PPL) feature on Cisco UCS C225 and C245 M8 servers after upgrading to release 4.3(6) and then downgrade to any previous release, the configuration settings for PPL feature, while retained, will not be adjustable from any user interface.

Table 7: Upgrade Paths to Release 4.3(6)

Upgrade from Release	Recommended Upgrade Path
Upgrade from any 4.3(5) release	Direct upgrade to release 4.3(6).
Upgrade from any 4.3(4) release	Direct upgrade to release 4.3(6). **Note** When updating the Cisco UCS-FI-6324 Fabric Interconnect from firmware version 4.3(4), first download Infrastructure A bundle for release 4.3(6) and perform the upgrade. Then, proceed to download the server bundles for version 4.3(6).
Upgrade from any 4.3(3) release	Direct upgrade to release 4.3(6). **Note** When updating the Cisco UCS-FI-6324 Fabric Interconnect from firmware version 4.3(3), first download Infrastructure A bundle for release 4.3(6) and perform the upgrade. Then, proceed to download the server bundles for version 4.3(5).
Upgrade from any 4.3(2) release	Direct upgrade to release 4.3(6). **Note** When updating the Cisco UCS-FI-6324 Fabric Interconnect from firmware version 4.3(2), first download Infrastructure A bundle for release 4.3(6) and perform the upgrade. Then, proceed to download the server bundles for version 4.3(5).
Upgrade from any 4.2(2) or 4.2(3) release	Direct upgrade to release 4.3(6).
Upgrade from any 4.2(1) release	**1.** Upgrade from 4.2(1i) or later patch—Direct upgrade to release 4.3(6). **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(6)A bundle before activating release 4.2(1i)A. **b.** Download and upgrade to release 4.3(6).

Upgrade from Release	Recommended Upgrade Path
Upgrade from any 4.1(3) release	**1.** Upgrade from 4.1(3h) or later patch—Direct upgrade to release 4.3(6). **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(6)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(6).
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(6)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(6).
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(6)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(6).
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(6)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(6).

Upgrade and Downgrade to Release 4.3(5)

- In a setup equipped with Cisco UCS C225 M8 Server or Cisco UCS X215c M8 Compute Node, you cannot downgrade Infrastructure Firmware Version (A Bundle) or Host Firmware Version (C Bundle) to any release earlier than 4.3(5a).
- If your setup includes any of the following components, then you can not downgrade to any release earlier than 4.3(5a):
  - Cisco Tri-mode M1 24G RAID Controller W/4GB FBWC (16 Drives) (UCSC-RAID-M1L16)
  - Cisco Tri-mode M1 24G HBA Controller (16 Drives) (UCSC-HBA-M1L16)
  - Cisco Tri-mode M1 24G RAID Controller W/4GB FBWC (32Drives) (UCSC-RAID-MP1L32)
- MACsec Type-6 keys are supported in releases 4.3(5a) and later. You must remove Type-6 keys or migrate Type-6 keys to supported types, Type-0 or Type-7, before downgrading to any 4.3(4) release. If you wish to downgrade to any release earlier than 4.3(4a), then you must disable MACsec functionality before downgrading.

Table 8: Upgrade Paths to Release 4.3(5)

Upgrade from Release	Recommended Upgrade Path
Upgrade from any 4.3(4) release	Direct upgrade to release 4.3(5). **Note** When updating the Cisco UCS-FI-6324 Fabric Interconnect from firmware version 4.3(4), first download Infrastructure A bundle for release 4.3(5) and perform the upgrade. Then, proceed to download the server bundles for version 4.3(5).
Upgrade from any 4.3(3) release	Direct upgrade to release 4.3(5). **Note** When updating the Cisco UCS-FI-6324 Fabric Interconnect from firmware version 4.3(3), first download Infrastructure A bundle for release 4.3(5) and perform the upgrade. Then, proceed to download the server bundles for version 4.3(5).
Upgrade from any 4.3(2) release	Direct upgrade to release 4.3(5). **Note** When updating the Cisco UCS-FI-6324 Fabric Interconnect from firmware version 4.3(2), first download Infrastructure A bundle for release 4.3(5) and perform the upgrade. Then, proceed to download the server bundles for version 4.3(5).
Upgrade from any 4.2(2) or 4.2(3) release	Direct upgrade to release 4.3(5).

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(5). **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(5)A bundle before activating release 4.2(1i)A. **b.** Download and upgrade to release 4.3(5).
Upgrade from any 4.1(3) release	**1.** Upgrade from 4.1(3h) or later patch—Direct upgrade to release 4.3(5). **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(5)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(5).
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(5)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(5).

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(5)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(5).
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(5)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(5).

Upgrade and Downgrade to Release 4.3(4)

- You cannot downgrade Infrastructure Firmware Version (A Bundle) of a Cisco UCS X-Series Direct setup to any release earlier than 4.3(4b).
- In a setup equipped with Cisco UCS C245 M8 Server, you cannot downgrade Infrastructure Firmware Version (A Bundle) or Host Firmware Version (C Bundle) to any release earlier than 4.3(4b).
- When upgrading the Cisco UCS-FI-6324 Fabric Interconnect from firmware version 4.3(3) or 4.3(2), first download Infrastructure A bundle for release 4.3(4) and perform the upgrade. Then, proceed to download the server bundles for version 4.3(4).
- If your setup includes any of the following components, then you can not downgrade to any release earlier than 4.3(4a):
  - Cisco UCSX-440P PCIe Node
  - Cisco Tri-Mode 24G SAS RAID Controller w/4GB Cache (UCSC-RAID-HP)
- To downgrade to any release earlier than 4.3(4a), you must remove the configuration for ERSPAN source traffic monitoring sessions and ERSPAN Origin Interface configuration.
- If you have enabled MACsec after upgrading to release 4.3(4a) or later, then you must disable it before downgrading to any release earlier than 4.3(4a).
- If your configuration includes any of the following adapters for management connectivity between Rack servers and UCS Fabric Interconnect, then you cannot upgrade to release 4.3(4a) or later:
  - Qlogic QL41132HORJ dual port 10GBase T OCP (UCSC-OCP-QD10GC)
  - QLogic QL41162HLRJ PCIe dual-port 10Gb Base-T PCIe NIC (UCSC-PCIE-QD10GC)

- Cisco FastLinQ QL41212H 25GbE (UCSC-PCIE-QD25GF)
- Qlogic QL41232HOCU dual port 25G OCP (UCSC-OCP-QD25GF)
- Qlogic FastLinQ QL45412H 40GbE (UCSC-PCIE-QD40GF)
- QLogic QL45611HLCU single port 100GbE PCIe NIC (UCSC-PCIE-QS100GF)
- Qlogic FastLinQ QL45631HOCU single port 100G QSFP28 OCP 2.0 (UCSC-OCP-QS100GF)

If these adapters are not used for management connectivity with UCS Fabric Interconnect, then upgrade to release 4.3(4a) is allowed. However, if you need to revert to release 4.3(4a) or an earlier version, then you must re-acknowledge the server to recover the adapter inventory.

Table 9: Upgrade Paths to Release 4.3(4)

Upgrade from Release	Recommended Upgrade Path
Upgrade from any 4.3(3) release	Direct upgrade to release 4.3(4). **Note** When updating the Cisco UCS-FI-6324 Fabric Interconnect from firmware version 4.3(3), first download Infrastructure A bundle for release 4.3(4) and perform the upgrade. Then, proceed to download the server bundles for version 4.3(4).
Upgrade from any 4.3(2) release	Direct upgrade to release 4.3(4). **Note** When updating the Cisco UCS-FI-6324 Fabric Interconnect from firmware version 4.3(2), first download Infrastructure A bundle for release 4.3(4) and perform the upgrade. Then, proceed to download the server bundles for version 4.3(4).
Upgrade from any 4.2(2) or 4.2(3) release	Direct upgrade to release 4.3(4).
Upgrade from any 4.2(1) release	**1.** Upgrade from 4.2(1i) or later patch—Direct upgrade to release 4.3(4). **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(4)A bundle before activating release 4.2(1i)A. **b.** Download and upgrade to release 4.3(4).

Upgrade from Release	Recommended Upgrade Path
Upgrade from any 4.1(3) release	**1.** Upgrade from 4.1(3h) or later patch—Direct upgrade to release 4.3(4). **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(4)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(4).
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(4)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(4).
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(4)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(4).
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(4)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(4).

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 20 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. Refer *New Features in Release 4.3* for minimum supported version for Cisco UCS X-Series chassis and Cisco UCS M7 servers.
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.

Table 10: 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 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(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 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 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(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).

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 11: 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 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 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(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 4.1(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).

Internal Dependencies

In this release, an interactive compatibility lookup tool is available to help you quickly determine supported combinations of Infrastructure Releases, Fabric Interconnects, servers, VICs, and IOM modules based on the selected release.

Cisco UCS Manager Internal Dependencies Matrix

Full version of the Internal Dependencies tables is also available for reference: Cisco UCS Manager Internal Dependencies, Release 4.3

Cisco UCS NVMeoF Support Matrix for 3rd Party Storage Vendors

Table 12: Cisco UCS NVMeoF Support Matrix for 3rd Party Storage Vendors (Updated)

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+
	NVMe-FC	ONTAP 9.7 onwards	Cisco UCS UCSX-S9108-100G	Cisco UCS 15000 Series	ESXi 7.0U3+, ESXi 8.0U2+, RHEL 8.9+, RHEL 9.3+, SLES 15SP4+
	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
	NVMe-TCP	ONTAP 9.10 onwards	Cisco UCS UCSX-S9108-100G	Cisco UCS 15000 Series	ESXi 7.0U3 +, ESXi 8.0 U2+, RHEL 9.3+, SLES 15SP4+
	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				

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 1300 Series	RHEL 8.6+ **Note** Cisco UCS VIC 1300 series is supported only with RHEL 8.6+.
		Purity//FA 6.1 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+, ESXi 8.0+, RHEL 8.6+, RHEL 9.0+, SLES 15SP1+
		Purity//FA onwards 6.6.3	Cisco UCS UCSX-S9108-100G	Cisco UCS 15000 Series	ESXi 7.0U3+, RHEL 8.6+, SLES 15SP3+, ESXi 8.0, RHEL 9.0+
	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+
		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, ESXi 8.0
		Purity//FA onwards 6.6.3	Cisco UCS UCSX-S9108-100G	Cisco UCS 15000 Series	ESXi 7.0U3+, ESXi 8.0U2+, RHEL 8.9+, RHEL 9.3+
	NVMe-TCP	Purity//FA 6.4.2 onwards	Cisco UCS 6300 Series Cisco UCS 6400 Series Cisco UCS 6536		ESXi 7.0U3+, RHEL 9.0+, SLES 15SP3+

Storage Vendor	Feature	Storage Array	Cisco UCS FI	Cisco UCS VIC	Operating System
				Cisco UCS 1400 Series Cisco UCS 14000 Series Cisco UCS 15000 Series	
		Purity//FA onwards 6.6.3	Cisco UCS UCSX-S9108-100G	Cisco UCS 15000 Series	ESXi 7.0U3+, ESXi 8.0U2+, RHEL 8.9+, RHEL 9.3+, SLES 15SP4+
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+
		PowerStore PowerMax	Cisco UCS UCSX-S9108-100G	Cisco UCS 15000 Series	ESXi 7.0U3+, ESXi 8.0U2+, RHEL 8.9+, RHEL 9.3+, SLES 15SP4+
	NVMe-TCP	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+
		PowerStore PowerMax	Cisco UCS UCSX-S9108-100G	Cisco UCS 15000 Series	ESXi 7.0U3+, ESXi 8.0U2+, RHEL 8.9+, RHEL 9.3+, SLES 15SP4+

Storage Vendor	Feature	Storage Array	Cisco UCS FI	Cisco UCS VIC	Operating System
IBM® Information Technology	NVMe-FC	IBM FlashSystem 9500	Cisco UCS 6400 Series Cisco UCS 6500 Series	Cisco UCS 1400 Series Cisco UCS 14000 Series Cisco UCS 15000 Series	ESXi 8.0U2, ESXi 7.0U3, RHEL 8.8, RHEL 9.2
		IBM FlashSystem 9200/R			
		IBM FlashSystem 9100			
		IBM FlashSystem 7300			
		IBM FlashSystem 7200/H			
		IBM FlashSystem 5300			
		IBM FlashSystem 5200			
		IBM FlashSystem 5045			
		IBM FlashSystem 5035			
		IBM FlashSystem 5015			
		IBM SAN Volume Controller SV3			
		IBM SAN Volume Controller SV2			

Storage Vendor	Feature	Storage Array	Cisco UCS FI	Cisco UCS VIC	Operating System
Hitachi, Ltd.	NVMe-FC	HV Hitachi Virtual Storage Platform 5-Series(VSP 5600H)	Cisco UCS 6300 Series Cisco UCS 6400 Series Cisco UCS 6536	Cisco UCS 1400 Series Cisco UCS 14000 Series Cisco UCS 15000 Series	ESXi 8.0U1+, ESXi 8.0U2+, ESXi 7.0U3+ **Note** Cisco UCS Manager versions 4.3(4) and 4.3(2) are supported.
		HV Hitachi Virtual Storage Platform 5-Series(VSP 5600)			
		HV Hitachi Virtual Storage Platform 5-Series(VSP 5500)			
		HV Hitachi Virtual Storage Platform 5-Series(VSP 5100)			
		HV Hitachi Virtual Storage Platform 5-Series(VSP 5200)			
		HV Hitachi Virtual Storage Platform 5-Series(VSP 5500H)			
		HV Hitachi Virtual Storage Platform 5-Series(VSP 5200H)			
		HV Hitachi Virtual Storage Platform 5-Series(VSP 5100H)			

Storage Vendor	Feature	Storage Array	Cisco UCS FI	Cisco UCS VIC	Operating System
		HV Hitachi Virtual Storage Platform E-Series(VSP E1090H)			
		HV Hitachi Virtual Storage Platform E-Series(VSP E1090)			
	NVMe-TCP	HV Hitachi VSP One Block 24	Cisco UCSX-S9108-100G	Cisco UCS 15000 Series	ESXi 8.0U3 **Note** Cisco UCS Manager version 4.3(5) is supported.
		HV Hitachi VSP One Block 26			
		HV Hitachi VSP One Block 28			

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

Cisco UCS Fabric Interconnect and Switch Compatibility Matrix

Compatibility and Support Matrix for Cisco Fabric Interconnects and MDS Switches

Cisco UCS Fabric Interconnect	Older Supported Release of MDS	Recommended Release of MDS
Cisco UCS 6536 FI	9.2	9.4
Cisco UCS 6454 FI	8.4, 9.2	9.4
Cisco UCS 64108 FI	8.4, 9.2	9.4
Cisco UCS X-Series Direct	—	9.4

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

Compatibility and Support Matrix for Cisco Fabric Interconnects and Nexus Switches

Cisco UCS Fabric Interconnect	Older Supported Release of NX-OS	Recommended Release of NX-OS
Cisco UCS 6536 FI	10.3(x), 10.4(x)	10.5(x)
Cisco UCS 6454 FI	10.3(x), 10.4(x)	10.5(x)
Cisco UCS 64108 FI	10.3(x), 10.4(x)	10.5(x)
Cisco UCS X-Series Direct	10.4(x)	10.5(x)

Compatibility and Support Matrix for Cisco Fabric Interconnects and Brocade Switches

Cisco UCS Fabric Interconnect	Older Supported Release of Brocade	Recommended Release of Brocade
Cisco UCS 6536 FI	9.1	9.2
Cisco UCS 6454 FI	9.1	9.2
Cisco UCS 64108 FI	9.1	9.2
Cisco UCS X-Series Direct	NA	9.2

Supported Hardware and Software

Supported Platforms in this Release

4.3(6a)

Support for the following servers is introduced in this release and continues in future releases within the same release train:

- Cisco UCS C240 M8 Server
- Cisco UCS C220 M8 Server
- Cisco UCS X210c M8 Compute Node

4.3(5a)

Support for the following servers is introduced in this release and continues in future releases within the same release train:

- Cisco UCS X215c M8 Compute Node
- Cisco UCS C225 M8 Server

4.3(4b)

Support for the following server is introduced in this release and continues in future releases within the same release train:

- Cisco UCS C245 M8 Server

4.3(2c)

Support for the following server is introduced in this release and continues in future releases within the same release train:

- Cisco UCS X410c M7 Compute Node

4.3(2b)

The following servers are supported in this release and continue to receive support in subsequent releases within the same release train:

- 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

System Requirements

Supported Operating Systems

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

Supported Web Browsers

To access the Cisco UCS Manager GUI, Cisco recommends using the most recent version of one of the following supported browsers for Windows, Linux RHEL, and MacOS:

- Microsoft Edge
- Mozilla Firefox
- Google Chrome
- Apple Safari

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

For the complete list of compatible versions of Cisco UCS Central and Cisco UCS Manager, see *Feature Support Matrix* in Release Notes for Cisco UCS Central.

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 UCSX-S9108-100G	Cisco UCS Manager CLI access
80	XML	HTTP	TCP	UCS 6300 Series UCS 6400 Series UCS 6536 UCSX-S9108-100G	Cisco UCS Manager GUI and third party management stations. Client download

Port	Interface	Protocol	Traffic Type	Fabric Interconnect	Usage
443	XML	HTTP	TCP	UCS 6300 Series UCS 6400 Series UCS 6536 UCSX-S9108-100G	Cisco UCS Manager login page access Cisco UCS Manager XML API access
743	KVM	HTTP	TCP	UCS 6300 Series UCS 6400 Series UCS 6536 UCSX-S9108-100G	CIMC Web Service / Direct KVM
7546	CFS	CFSD	TCP	UCS 6400 Series UCS 6536 UCSX-S9108-100G	Cisco Fabric Service

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

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

Table 13: 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)

Type	Details
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 14: 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
Power Supplies	UCS-PSU-6332-AC UCS-PSU-6332-DC UCS-PSU-64108-AC UCS-PSU-6332-DC

Table 15: 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 16: UCS 6500 Series Fabric Interconnects

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)

Gb Connector Modules	Transceiver Modules and Cables
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-SR1.2 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

Table 17: UCS 6400 Series Fabric Interconnects

Gb Connector Modules	Transceiver Modules and Cables
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
100-Gb for UCS 6400 Series Fabric Interconnects	QSFP-100G-SR1.2 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
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]

Gb Connector Modules	Transceiver Modules and Cables
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 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
8-Gb FC for UCS 6400 Series Fabric Interconnects	DS-SFP-FC8G-SW DS-SFP-FC8G-LW
1-Gb for UCS 6400 Series Fabric Interconnects	GLC-TE GLC-SX-MMD SFP-GE-T

[1] Supported from Cisco UCS Manager, Release 4.1(2)

Table 18: UCS 6300 Series Fabric Interconnects

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
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
4-Gb FC for UCS 6300 Series Fabric Interconnects	DS-SFP-FC4G-SW DS-SFP-FC4G-LW
1-Gb for UCS 6300 Series Fabric Interconnects	GLC-TE GLC-SX-MM GLC-LH-SM
16-Gb for UCS 6332UP Fabric Interconnects	DS-SFP-FC16G-LW DS-SFP-FC16G-SW
8-Gb FC for UCS 6332UP Fabric Interconnects	DS-SFP-FC8G-SW DS-SFP-FC8G-LW

[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.

Table 19: Supported GPU/GPU PCIe Node

GPU/GPU PCIe Node	PID	Supported Servers	Minimum Software Version	Suggested Software Version
NVIDIA A16 GPU on X440p: PCIE 250W 4X16GB, FHFL	UCSX-GPU-A16	Cisco UCS X210c M8 (with PCIe Node)	4.3(6a)	4.3(6i)
	UCSC-GPU-A16	Cisco UCSX215c M8 (with PCIe Node)	4.3(5a)	4.3(6i)
AMD MI210 GPU; 300W 64GB, 2 slot FHFL	UCSX-GPU-MI210	Cisco UCS X215c M8	4.3(6a)	4.3(6i)
NVIDIA H100-NVL GPU 400W, 94GB, 2-slot FHFL	UCSX-GPU-H100-NVL	Cisco UCS X210c M8 (with PCIe Node)	4.3(6a)	4.3(6i)
	UCSC-GPU-H100-NVL	Cisco UCS C240 M8	4.3(6a)	4.3(6i)
		Cisco UCS X210c M7 Cisco UCS X215c M8 (with PCIe Node)	4.3(5a)	4.3(6i)
		Cisco UCS C245 M8	4.3(5a)	4.3(6i)
		Cisco UCS C240 M7	4.3(5a)	4.3(6i)
NVIDIA L4-Mezz GPU 70W, 24GB, 1-slot HHHL	UCSX-GPU-L4-Mezz	Cisco UCS X210c M7 Cisco UCS X215c M8	4.3(5a)	4.3(6i)
UCSX-440P-D GPU PCIe Node	UCSX-440P-D	Cisco UCS X210c M7, X210c M6, and X410c M7	4.3(4a)	4.3(6i)
Intel GPU Flex 140, Gen4x8, HHHL, 75W PCIe (Front Mezz)	UCSX-GPU-FLX140MZ	Cisco UCS X210c M7	4.3(2b)	4.3(6i)

GPU/GPU PCIe Node	PID	Supported Servers	Minimum Software Version	Suggested Software Version
Intel GPU Flex 140, Gen4x8, HHHL, 75W PCIe	UCSX-GPU-FLEX140	Cisco UCS X410c M7 and X210c M7 (with PCIe Node)	4.3(4a)	4.3(6i)
	UCSC-GPU-FLEX140	Cisco UCS C220 M7 and C240 M7	4.3(4a)	4.3(6i)
Intel GPU Flex 170, Gen4x16, HHFL, 150W PCIe	UCSX-GPU-FLEX170	Cisco UCS X410c M7 and X210c M7 (with PCIe Node)	4.3(4a)	4.3(6i)
	UCSC-GPU-FLEX170	Cisco UCS C240 M7	4.3(4a)	4.3(6i)
NVIDIA TESLA A16 PCIE 250W 4X16GB	UCSX-GPU-A16-D	Cisco UCS X210c M7 and X210c M6 (with PCIe Node)	4.3(4a)	4.3(6i)
		Cisco UCS X410c M7 (with PCIe Node)	4.3(4a)	4.3(6i)
	UCSC-GPU-A16	Cisco UCS C240 M8	4.3(6a)	4.3(6i)
		Cisco UCS C240 M6	4.2(1d)	4.3(6i)
		Cisco UCS C245 M6	4.2(1i)	4.3(6i)
NVIDIA L4 Tensor Core, 70W, 24GB	UCSX-GPU-L4	Cisco UCS X210c M8 (with PCIe Node)	4.3(6a)	4.3(6i)
		Cisco UCS X210c M7 (with PCIe Node)	4.3(4a)	4.3(6i)
		Cisco UCS X410c M7 (with PCIe Node)	4.3(4a)	4.3(6i)

GPU/GPU PCIe Node	PID	Supported Servers	Minimum Software Version	Suggested Software Version
NVIDIA L40 300W, 48GB wPWR CBL	UCSX-GPU-L40	Cisco UCS X210c M7 (with PCIe Node)	4.3(4a)	4.3(6i)
		Cisco UCS X410c M7 (with PCIe Node)	4.3(4a)	4.3(6i)
	UCSC-GPU-L40	Cisco UCS C240 M7	4.3(2b)	4.3(6i)
		Cisco UCS X215c M8 (with PCIe Node)	4.3(5a)	4.3(6i)
NVIDIA L40S: 350W, 48GB, 2-slot FHFL GPU	UCSX-GPU-L40S	Cisco UCS X210c M8 (with PCIe Node)	4.3(6a)	4.3(6i)
		Cisco UCS X210c M7 (with PCIe Node) Cisco UCS X410c M7 (with PCIe Node)	4.3(4a)	
	UCSC-GPU-L40S	Cisco UCS C240 M8	4.3(6a)	4.3(6i)
		Cisco UCS C240 M7	4.3(4a)	4.3(6i)
		Cisco UCS X215c M8 (with PCIe Node)	4.3(5a)	4.3(6i)

GPU/GPU PCIe Node	PID	Supported Servers	Minimum Software Version	Suggested Software Version
NVIDIA T4 PCIE 75W 16GB	UCSX-GPU-T4-16	Cisco UCS X210c M6 (with PCIe Node)	4.3(4a)	4.3(6i)
	UCSC-GPU-T4-16	Cisco UCS C220 M6	4.3(2b)	4.3(6i)
		Cisco UCS C245 M6	4.2(1f)	4.3(6i)
		Cisco UCS C225 M6	4.2(1l)	4.3(6i)
		Cisco UCS C240 M5, C220 M5, and C480 M5	3.2(3a)	4.3(6i)
		Cisco UCS S3260 M5	3.1(2b)	4.3(6i)
NVIDIA T4 GPU PCIE 75W 16GB, MEZZ form factor (Front Mezz)	UCSX-GPU-T4-MEZZ	Cisco UCS X210c M7 and X210c M6	4.3(2b)	4.3(6i)
NVIDIA Hopper L4 70W, 24GB, 1-slot HHHL	UCSC-GPU-L4M6	Cisco UCS C220 M6, C240 M6	4.3(4a)	4.3(6i)
NVIDIA H100: 350W, 80GB, 2-slot FHFL GPU	UCSX-GPU-H100-80	Cisco UCS X210c M7 and X410c M7 (with PCIe Node)	4.3(4a)	4.3(6i)
	UCSC-GPU-H100-80	Cisco UCS C240 M7	4.3(4a)	4.3(6i)
NVIDIA L4:70W, 24GB, 1-slot HHHL GPU	UCSC-GPU-L4	Cisco UCS C240 M8 and C220 M8	4.3(6a)	4.3(6i)
		Cisco UCS C245 M8	4.3(5a)	4.3(6i)
		Cisco UCS C220 M7 and C240 M7	4.3(2b)	4.3(6i)
		Cisco UCS X215c M8 (with PCIe Node)	4.3(5a)	4.3(6i)
NVIDIA P4	UCSC-GPU-P4	Cisco UCS C220 M5	3.2(3a)	4.3(6i)

GPU/GPU PCIe Node	PID	Supported Servers	Minimum Software Version	Suggested Software Version
NVIDIA M10	UCSC-GPU-M10	Cisco UCS C240 M5 and C480 M5	3.2(3a)	4.3(6i)
NVIDIA GRID P6 Front Mezzanine	UCSB-GPU-P6-F	Cisco UCS B200 M5	3.2(1d)	4.3(6i)
		Cisco UCS B480 M5	3.2(2b)	4.3(6i)
NVIDIA GRID P6 Rear Mezzanine	UCSB-GPU-P6-R	Cisco UCS B200 M5	3.2(1d)	4.3(6i)
		Cisco UCS B480 M5	3.2(2b)	4.3(6i)
TESLA A30, PASSIVE, 180W, 24GB	UCSC-GPU-A30-D	Cisco UCS C240 M7	4.3(2b)	4.3(6i)
	UCSC-GPU-A30	Cisco UCS C240 M6	4.2(1d)	4.3(6i)
		Cisco UCS C245 M6	4.2(1i)	4.3(6i)
TESLA A40 RTX, PASSIVE, 300W, 48GB	UCSX-GPU-A40-D	Cisco UCS X210c M7 and X210c M6 (with PCIe Node)	4.3(4a)	4.3(6i)
		Cisco UCS X410c M7 (with PCIe Node)	4.3(4a)	4.3(6i)
	UCSC-GPU-A40-D	Cisco UCS C240 M7	4.3(2b)	4.3(6i)
	UCSC-GPU-A40	Cisco UCS C240 M6	4.2(1d)	4.3(6i)
		Cisco UCS C245 M6	4.2(1i)	4.3(6i)
		Cisco UCS C480 M5	3.2(3a)	4.3(6i)

GPU/GPU PCIe Node	PID	Supported Servers	Minimum Software Version	Suggested Software Version
TESLA A100, PASSIVE, 300W, 80GB12	UCSX-GPU-A100-80-D	Cisco UCS X210c M7 and X210c M6 (with PCIe Node)	4.3(4a)	4.3(6i)
		Cisco UCS X410c M7 (with PCIe Node)	4.3(4a)	4.3(6i)
	UCSC-GPUA100-80-D	Cisco UCS C240 M7	4.3(2b)	4.3(6i)
	UCSC-GPU-A100-80	Cisco UCS C240 M6	4.2(1d)	4.3(6i)
		Cisco UCS C245 M6	4.2(1i)	4.3(6i)
		All Cisco UCS C-Series M5	4.2(2c)	4.3(6i)
TESLA A10, PASSIVE, 150W, 24GB	UCSC-GPU-A10	Cisco UCS C240 M6	4.2(1d)	4.3(6i)
		Cisco UCS C245 M6	4.2(1i)	4.3(6i)
NVIDIA H200-NVL GPU	UCSC-GPU-H200-NVL	Cisco UCS C240 M8	4.3(6c)	4.3(6i)

Deprecated Hardware and Software in Cisco UCS Manager

Release 4.3(4a)

Beginning with Cisco UCS Manager release 4.3(4a) following adapters are not supported:

- Qlogic QL41132HORJ dual port 10GBase T OCP (UCSC-OCP-QD10GC)
- QLogic QL41162HLRJ PCIe dual-port 10Gb Base-T PCIe NIC (UCSC-PCIE-QD10GC)
- Cisco FastLinQ QL41212H 25GbE (UCSC-PCIE-QD25GF)
- Qlogic QL41232HOCU dual port 25G OCP (UCSC-OCP-QD25GF)
- Qlogic FastLinQ QL45412H 40GbE (UCSC-PCIE-QD40GF)
- QLogic QL45611HLCU single port 100GbE PCIe NIC (UCSC-PCIE-QS100GF)
- Qlogic FastLinQ QL45631HOCU single port 100G QSFP28 OCP 2.0 (UCSC-OCP-QS100GF)

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.

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 20: Version Mapping

UCS Release	Catalog File Name	Additional PIDs in this Release
4.3(6i)	ucs-catalog.4.3.6i.T.bin	DIMMs: • UCS-MRX16G1RE5 • UCS-MRX32G1RE5 • UCS-MRX64G2RE5 • UCS-MRX96G2RF5 • UCS-MR128G2RG5
4.3(6h)	ucs-catalog.4.3.6h.T.bin	—
4.3(6g)	ucs-catalog.4.3.6g.T.gbin	—
4.3(6f)	ucs-catalog.4.3.6f.T.bin	—
4.3(6e)	ucs-catalog.4.3.6e.T.bin	—
4.3(6d)	ucs-catalog.4.3.6d.T.bin	—
4.3(6c)	ucs-catalog.4.3.6c.T.bin	—
4.3(6b)	ucs-catalog.4.3.6b.T.bin	—

UCS Release	Catalog File Name	Additional PIDs in this Release
4.3(6a)	ucs-catalog.4.3.6a.T.bin	

UCS Release	Catalog File Name	Additional PIDs in this Release
		Cisco UCS X210c M8 Compute Node • UCSX-210C-M8 • UCSX-210C-M8-U Cisco UCS C240 M8 Server • UCSC-C240-M8SX Cisco UCS C220 M8 Server • UCSC-C220-M8S Intel® CPUs: • UCS-CPU-I6748P • UCS-CPU-I6738P • UCS-CPU-I6728P • UCS-CPU-I6505P • UCS-CPU-I6714P • UCS-CPU-I6507P • UCS-CPU-I6788P • UCS-CPU-I6768P GPU: • UCSC-GPU-FLEX170 • UCSX-GPU-MI210 Controllers: • UCSX-RAID-M1L6 • UCSX-X10C-PTE3 • UCSX-M2I-HWRD-FPS Drives: • UCS-HDM8TW1S74K • UCS-HDM20TW1S74K • UCS-SD19TM1X-EV • UCS-SD76TM1X-EV • UCS-SD19TBEM2NK9 • UCS-SD76TS1X-EV • UCS-SD64TS3X-EP • UCS-SD38T63X-EP • UCS-HDB1T8GS10K4K • UCS-HDB2T4GS10K4K

UCS Release	Catalog File Name	Additional PIDs in this Release
		• UCS-HD24T10BNK9 • UCS-S3260-HDW16TR • UCS-NVB12T8O1P • UCS-NVB15T3O1L DIMM: • UCS-MR256G4RG5 Third-party Adapters: • UCSC-O-N6CD100GFO • UCSC-P-M6CD100GFO • UCSC-P-M6DD100GFO • UCSC-O-N6CD25GFO • UCSC-P-N7D200GFO • UCSC-P-N7Q25GFO • UCSC-P-N7S400GFO • 900-9D3B6-00CC-EA0 • UCSC-P-N3220L • UCSC-P-N6D25GFO
4.3(5d)	ucs-catalog.4.3.5d.T.bin	Drives for Cisco UCS B200 M6 servers: • UCS-SDC960SA1V • UCS-SDC1T9SA1V • UCS-SDC3T8SA1V • UCS-SDC7T6SA1V Drives for Cisco UCS B-Series M5 servers: • UCS-SDA960SA1V • UCS-SDA1T9SA1V • UCS-SDA3T8SA1V • UCS-SDA7T6SA1V Drives for Cisco UCS C-Series and X-Series servers: • UCS-SDB960SA1V • UCS-SDB1T9SA1V • UCS-SDB3T8SA1V • UCS-SDB7T6SA1V

UCS Release	Catalog File Name	Additional PIDs in this Release
4.3(5c)	ucs-catalog.4.3.5c.T.bin	CPUs for Cisco UCS C245 M8 servers: • UCS-CPU-A9655 • UCS-CPU-A9575F • UCS-CPU-A9555 • UCS-CPU-A9355 • UCS-CPU-A9135 CPUs for Cisco UCS C225 M8 servers: • UCS-CPU-A9355 • UCS-CPU-A9135 • UCS-CPU-A9655P • UCS-CPU-A9555P\ • UCS-CPU-A9355P CPUs for Cisco UCSX-215C-M8 Compute Node: • UCSX-CPU-A9655 • UCSX-CPU-A9555 • UCSX-CPU-A9355 • UCSX-CPU-A9135 • UCSX-CPU-A9575F GPU Support: • UCSC-GPU-MI210

UCS Release	Catalog File Name	Additional PIDs in this Release
4.3(5a)	ucs-catalog.4.3.5a.T.bin	

UCS Release	Catalog File Name	Additional PIDs in this Release
		Cisco UCS X215c M8 Compute Node • UCSX-215C-M8 • UCSX-215C-M8-U Cisco UCS C225 M8 Server • UCSC-C225-M8S • UCSC-C225-M8N Cisco Tri-Mode M1 24G RAID and HBA controllers: • UCSC-RAID-MP1L32 • UCSC-RAID-M1L16 • o UCSC-HBA-M1L16 GPUs: • UCSC-GPU-A16 • UCSC-GPU-H100-NVL • UCSX-GPU-L4-Mezz Drives: • UCS-NVB1T9O1V • UCSB-NVA1T9O1V • UCS-NVB3T8O1V • UCSB-NVA3T8O1V • UCS-NVB7T6O1V • UCSB-NVA7T6O1V • UCS-NVB15TO1V • UCSB-NVA15TO1V • UCS-NVB1T6O1P • UCSB-NVA1T6O1P • UCS-NVB3T2O1P • UCSB-NVA3T2O1P • UCS-NVB6T4O1P • UCSB-NVA6T4O1P • UCS-NVB12T8O1P • UCS-SDB480OA1V • UCS-SDB960OA1V • UCS-SDB3T8OA1V • UCSB-SDA480OA1V • UCSB-SDA960OA1V

UCS Release	Catalog File Name	Additional PIDs in this Release
		• UCSB-SDA3T8OA1V • UCSB-SDC480OA1V • UCSB-SDC960OA1V • UCSB-SDC3T8OA1V • UCS-SDB480OA1P • UCS-SDB960OA1P • UCS-SDB1T9OA1P • UCS-SDB3T8OA1P • UCSB-SDA480OA1P • UCSB-SDA960OA1P • UCSB-SDA1T9OA1P • UCSB-SDC480OA1P • UCSB-SDC960OA1P • UCSB-SDC1T9OA1P • UCS-M2240OA1V • UCS-M2480OA1V
4.3(4f)	ucs-catalog.4.3.4f.T.bin	—
4.3(4e)	ucs-catalog.4.3.4e.T.bin	—
4.3(4d)	ucs-catalog.4.3.4d.T.bin	—
4.3(4c)	ucs-catalog.4.3.4c.T.bin	—
4.3(4b)	ucs-catalog.4.3.4b.T.bin	Cisco UCS C245 M8 Server • UCSC-C245-M8SX Cisco UCS 9108 100G FI • UCSX-S9108-100G

UCS Release	Catalog File Name	Additional PIDs in this Release
4.3(4a)	ucs-catalog.4.3.4a.T.bin	RAID Controllers: • UCSC-RAID-HP • UCS-M2-NVRAID TPM Module: • UCS-TPM-002D GPU: • UCSX-GPU-FLEX170 • UCSX-GPU-FLEX140 • UCSX-GPU-L40S • UCSC-GPU-L4M6 • UCSX-GPU-H100-80
4.3(3c)	ucs-catalog.4.3.3c.T.bin	—

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-I8592V • UCSX-CPU-I8592+ • UCSX-CPU-I8581V • UCSX-CPU-I8580 • UCSX-CPU-I8571N • UCSX-CPU-I8570 • UCSX-CPU-I8568Y+ • UCSX-CPU-I8562Y+ • UCSX-CPU-I8558U • UCSX-CPU-I8558P • UCSX-CPU-I8558 • UCSX-CPU-I6554S • UCSX-CPU-I6548Y+ • UCSX-CPU-I6548N • UCSX-CPU-I6544Y • UCSX-CPU-I6542Y • UCSX-CPU-I6538Y+ • UCSX-CPU-I6538N • UCSX-CPU-I6534 • UCSX-CPU-I6530 • UCSX-CPU-I6526Y • UCSX-CPU-I5520+ • UCSX-CPU-I5515+ • UCSX-CPU-I5512U • UCSX-CPU-I4516Y+ • UCSX-CPU-I4514Y 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 Release	Catalog File Name	Additional PIDs in this Release
		• 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-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(2f)	ucs-catalog.4.3.2f.T.bin	—
4.3(2e)	ucs-catalog.4.3.2e.T.bin	—

UCS Release	Catalog File Name	Additional PIDs in this Release
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

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
- Release Notes for Cisco UCS Central
- Cisco UCS Manager Upgrade/Downgrade Support Matrix Tool
- Cisco UCS Equivalency Matrix for Cisco Intersight, Cisco IMC, and Cisco UCS Manager Tool
- Cisco UCS Manager Internal Dependencies Matrix Tool
- Cisco UCS Manager Internal Dependencies, Release 4.3
- Cisco UCS Manager Cross Version Firmware Matrix Tool
- Cisco UCS Manager Cross-Version Firmware Support, Release 4.3

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

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

© 2023–2026 Cisco Systems, Inc. All rights reserved.