# Release Notes for Cisco UCS Manager, Release 4.0

**First Published:** 2018-08-14

**Last Modified:** 2023-01-31

# Cisco UCS Manager

Cisco UCS™ Manager, Release 4.0 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 4.0. This document also includes the following:

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

Upgrading directly to Cisco UCS Manager 4.0(x) is supported from Release 2.2(8), and 3.1(3) and later releases. For UCS Mini, upgrading directly to Cisco UCS Manager Release 4.0(x) is supported from Release 3.1(3) and later releases. See *Cisco UCS Manager Firmware Management Guide, Release 4.0* for details.

## Deprecation Notice

### Deprecated Release 4.0(4h)

Release 4.0(4h) is deprecated and firmware files are no longer available. For more information, refer Field Notice: FN - 70595.

Cisco recommends that you upgrade to release 4.0(4i) or later.

## Revision History

| Release | Date | Description |
|---|---|---|
| 4.0(4o) | January 31, 2023 | Created release notes for Cisco UCS Manager Release 4.0(4o). |
| 4.0(4n) | March 21, 2022 | Created release notes for Cisco UCS Manager Release 4.0(4n). |

| Release | Date | Description |
|---|---|---|
| 4.0(4m) | July 7, 2021 | Created release notes for Cisco UCS Manager Release 4.0(4m). |
| | January 13, 2022 | Added section for UCS Manager Health and Pre-Upgrade Check Tool. |
| 4.0(4l). | March 18, 2021 | Created release notes for Cisco UCS Manager Release 4.0(4l). |
| 4.0(4k) | November 3, 2020 | Created release notes for Cisco UCS Manager Release 4.0(4k). |
| | December 17, 2020 | Added the Known limitations in Release 4.0(4). |
| | December 22, 2020 | Added CSCvq17291 to the list of Resolved Caveats for Release 4.0(4k). |
| 4.0(4i) | July 6, 2020 | Created release notes for Cisco UCS Manager Release 4.0(4i). |
| | July 23, 2020 | Added CSCvt64871 and CSCvu11155 to the list of Resolved Caveats for Release 4.0(4i). |
| | July 24, 2020 | Moved CSCvq53066 from Open Caveats to Resolved Caveats. |
| 4.0(4h) | March 23, 2020 | Created release notes for Cisco UCS Manager Release 4.0(4h). |
| | April 03, 2020 | Updated the description for CSCvr79388 in the Resolved Caveats for Release 4.0(4h).<br>Added CSCvt64871 to the list of Open Caveats for Release 4.0(4h). |
| | April 8, 2020 | Added behavior change - Fibre Channel Ports Experiencing txmit Credit Loss Are Now Disabled<br>. |
| | June 12, 2020 | Added CSCvu11155 to the list of Open Caveats for Release 4.0(4h). |

| Release | Date | Description |
|---|---|---|
| 4.0(4g) | December 9, 2019 | Created release notes for Cisco UCS Manager Release 4.0(4g). |
| | January 16, 2020 | Updated the Internal Dependencies table to clarify support for M3 blade servers. |
| | February 27, 2020 | Corrected cable SFP-H25G-CU3M to SFP-H25G-CU5M in CSCvr76930 in Open Caveats |
| 4.0(4f) | November 5, 2019 | Created release notes for Cisco UCS Manager Release 4.0(4f). |
| | December 02, 2019 | Updated the description for CSCvr40744 in the Resolved Caveats for Release 4.0(4f). |
| 4.0(4e) | September 27, 2019 | Created release notes for Cisco UCS Manager Release 4.0(4e). |
| 4.0(4d) | August 19, 2019 | Created release notes for Cisco UCS Manager Release 4.0(4d). |
| 4.0(4c) | August 01, 2019 | Created release notes for Cisco UCS Manager Release 4.0(4c). |
| | October 01, 2019 | Removed CSCvn49417 from the list of Resolved Caveats. |
| 4.0(4b) | May 17, 2019 | Created release notes for Cisco UCS Manager Release 4.0(4b). |
| | May 20, 2019 | Updated **Catalog File Name** for 4.0(4b). |
| | June 3, 2019 | Added a known limitation - UCS 6300 Series Fabric Interconnect ASIC Limitation with Passive Cables. |
| 4.0(4a) | April 26, 2019 | Created release notes for Cisco UCS Manager Release 4.0(4a). |
| | May 15, 2019 | Added CSCvp68182 to the list of Open Caveats.<br>Added the Software Deferral Notice for CSCvp68182. |
| | November 14, 2019 | Added behavior change - Cannot Create Virtual Drives with Cached IO Policy Enabled |

| Release | Date | Description |
|---|---|---|
| 4.0(2e) | May 15, 2019 | Created release notes for Cisco UCS Manager Release 4.0(2e). |
| 4.0(2d) | March 13, 2019 | Created release notes for Cisco UCS Manager Release 4.0(2d). |
| 4.0(2b) | January 19, 2019 | Created release notes for Cisco UCS Manager Release 4.0(2b). |
| | January 22, 2019 | Corrected the UCS Mini model number in the *New Hardware in Release 4.0(2b)* section. |
| 4.0(2a) | January 02, 2019 | Created release notes for Cisco UCS Manager Release 4.0(2a). |
| | January 08, 2019 | Updated the Open Caveats for Release 4.0(2a) to include CSCvk63036. |
| | March 03, 2019 | Added UCSC-GPU-V100-32 to the list of new hardware. |
| 4.0(1d) | December 20, 2018 | Created release notes for Cisco UCS Manager Release 4.0(1d). |
| | September 04, 2019 | Updated the description for CSCvq28261.<br>Added CSCvr08327 to the list of Open Caveats. |
| 4.0(1c) | October 11, 2018 | Created release notes for Cisco UCS Manager Release 4.0(1c). |
| 4.0(1b) | September 13, 2018 | Created release notes for Cisco UCS Manager Release 4.0(1b). |
| 4.0(1a) | August 14, 2018 | Created release notes for Cisco UCS Manager Release 4.0(1a). |
| | August 27, 2018 | Added the L1 Terminal Fault caveats — CSCvm03356, CSCvm03351, and CSCvm03339 — to the list of Security Fixes. |
| | June 7, 2019 | Added behavior change - Allowed WWPN and WWNN Ranges for a WWN Pool |
| | February 04, 2020 | Added CSCvr98210 to the list of Open Caveats. |

## Top Reasons to Move to Cisco UCS Manager Release 4.0

Here are the top reasons to move to Cisco UCS Manager Release 4.0:

- Support for UCS 6454 Fabric Interconnects
- Support for C4200 chassis and Cisco UCS C125 M5 Servers
- Support for VIC 1400 series adapter cards on UCS M5 servers
- Support for Cisco UCS C480 M5 ML Servers
- Support for the Second Generation Intel® Xeon® Scalable processor refresh and Intel® Optane™ Data Center persistent memory modules on UCS Intel-based M5 servers
- Improved memory RAS features on M5 servers
- Support for a new SIOC with S3260 storage servers
- Support for Hyperflex 3.5 and later releases
- Support for new peripherals

## New Features in Release 4.0

Cisco UCS Manager, Release 4.0 is a unified software release for all supported UCS hardware platforms.

### New Hardware Features

- New Hardware in Release 4.0(4o) — None
- New Hardware in Release 4.0(4n) — None
- New Hardware in Release 4.0(4m) — None
- New Hardware in Release 4.0(4l) — None
- New Hardware in Release 4.0(4k) — None
- New Hardware in Release 4.0(4i) — None
- New Hardware in Release 4.0(4h) — None
- New Hardware in Release 4.0(4g) — None
- New Hardware in Release 4.0(4f) — None
- New Hardware in Release 4.0(4e), on page 7
- New Hardware in Release 4.0(4d) — None
- New Hardware in Release 4.0(4c), on page 7
- New Hardware in Release 4.0(4b) — None
- New Hardware in Release 4.0(4a), on page 7
- New Hardware in Release 4.0(2e) — None
- New Hardware in Release 4.0(2d) — None

- New Hardware in Release 4.0(2b) — None
- New Hardware in Release 4.0(2a), on page 9
- New Hardware in Release 4.0(1d) — None
- New Hardware in Release 4.0(1c) — None
- New Hardware in Release 4.0(1b) — None
- New Hardware in Release 4.0(1a), on page 14

### New Software Features

- New Software in Release 4.0(4o) — None
- New Software in Release 4.0(4n) — None
- New Software in Release 4.0(4m) — None
- New Software in Release 4.0(4l) — None
- New Software in Release 4.0(4k) — None
- New Software in Release 4.0(4i) — None
- New Software in Release 4.0(4h) — None
- New Software in Release 4.0(4g) — None
- New Software in Release 4.0(4f) — None
- New Software Features in Release 4.0(4e), on page 17
- New Software in Release 4.0(4d) — None
- New Software Features in Release 4.0(4c), on page 18
- New Software in Release 4.0(4b) — None
- New Software Features in Release 4.0(4a), on page 18
- New Software in Release 4.0(2e) — None
- New Software in Release 4.0(2d) — None
- New Software in Release 4.0(2b) — None
- New Software Features in Release 4.0(2a), on page 20
- New Software in Release 4.0(1d) — None
- New Software in Release 4.0(1c) — None
- New Software in Release 4.0(1b) — None
- New Software Features in Release 4.0(1a), on page 22

## New Hardware in Release 4.0(4e)

### Peripherals

Support for the Cisco UCS 2408 Fabric Extender (UCS-IOM-2408).

## New Hardware in Release 4.0(4c)

### Intel NVMe P4510/4511 and P4610 Drive Support

Cisco UCS Manager Release 4.0(4c) introduces firmware support for the following NVMe drives on blade and rack servers:

| NMVe Drive | PID for Blade Servers | PID for Rack Servers |
|---|---|---|
| Intel P4510 1TB (SSDPE2KX010T8K) | UCSB-NVME2H-I1000 | UCSC-NVME2H-I1000 |
| Intel P4510 2TB (SSDPE2KX020T8K) | UCSB-NVME2H-I2TBV | UCSC-NVME2H-I2TBV |
| Intel P4510 4TB (SSDPE2KX040T8K) | UCSB-NVME2H-I4000 | UCSC-NVME2H-I4000 |
| Intel P4510 8TB (SSDPE2KX080T8K) | UCSB-NVMEHW-I8000 | UCSC-NVMEHW-I8000 |
| Intel P4610 1.6TB (SSDPE2KE016T8K) | UCSB-NVME2H-I1600 | UCSC-NVME2H-I1600 |
| Intel P4610 3.2TB (SSDPE2KE032T8K) | UCSB-NVME2H-I3200 | UCSC-NVME2H-I3200 |

## New Hardware in Release 4.0(4a)

### Second Generation Intel® Xeon® Scalable Processors

Cisco UCS Manager Release 4.0(4a) introduces support for Second Generation Intel® Xeon® Scalable processors on the following servers:

- Cisco UCS B200 M5 Server
- Cisco UCS B480 M5 Server
- Cisco UCS C220 M5 Server
- Cisco UCS C240 M5 Server
- Cisco UCS C480 M5 Server
- Cisco UCS S3260 M5 Server

### Intel® Optane™ Data Center Persistent Memory Modules

Intel® Optane™ Data Center persistent memory modules can be used only with the Second Generation Intel® Xeon® Scalable processors.

Cisco UCS Manager Release 4.0(4a) introduces support for the Intel® Optane™ DC persistent memory modules on the following servers that are based on the Second Generation Intel® Xeon® Scalable processors:

- Cisco UCS B200 M5 Server
- Cisco UCS B480 M5 Server
- Cisco UCS C220 M5 Server
- Cisco UCS C240 M5 Server
- Cisco UCS C480 M5 Server
- Cisco UCS S3260 M5 Server

Intel® Optane™ DC persistent memory modules support 128GB, 256GB and 512GB of persistent memory. This can be configured through Cisco UCS Manager or the host Operating System tools.

### Peripherals

- Support for NVIDIA T4 16GB GPU cards (UCSC-GPU-T4-16) on the following servers:
  - UCS C220 M5
  - UCS C240 M5
  - UCS C480 M5
- Support for AMD Radeon Pro V340, 2X16GB, 300W GPU cards (UCSC-GPU-V340)
- Support for the Cisco UCS 2304V2 Fabric Extender (UCS-IOM-2304V2)
- Support for Mellanox MCX4121A-ACAT Dual Port 10/25G SFP28 NIC (UCSC-P-M4D25GF)
- Support for the QLogic QL45611HLCU single port 100GbE PCIe NIC (UCSC-PCIE-QS100GF) on all UCS M5 servers except Cisco UCS C125 M5 Server.
- Support for the Cisco QSFP 40/100 Gb (QSFP-40/100G-SRBD) dual-rate bi-directional (BiDi) transceiver on UCS 6454 Fabric Interconnects.
- Hardware RAID support for Cisco Boot Optimized M.2 RAID Controller (UCS-M2-HWRAID) on the following servers:
  - Cisco UCS C220 M5 Server
  - Cisco UCS C240 M5 Server
  - Cisco UCS C480 M5 Server
  - Cisco UCS B200 M5 Server
  - Cisco UCS B480 M5 Server

## New Hardware in Release 4.0(2a)

### Cisco UCS C480 M5 ML Server

The Cisco UCS C480 M5 ML Rack Server is a purpose-built server for Deep Learning. It is storage- and I/O-optimized for training models. The Cisco UCS C480 M5 ML Server delivers outstanding levels of storage expandability and performance options for standalone or Cisco UCS-managed environments in a 4RU form factor. It offers these capabilities:

- 8 NVIDIA SXM2 V100 32G modules with NVLink interconnect
- Latest Intel® Xeon® Scalable processors with up to 28 cores per socket and support for two processor configurations
- 2666-MHz DDR4 memory and 24 DIMM slots for up to 3 terabytes (TB) of total memory
- 4 PCI Express (PCIe) 3.0 slots for up to 4 10/25 or 40/100G Cisco VICs (VIC 1455 and VIC 1495)
- Flexible storage options with support for up to 24 Small-Form-Factor (SFF) 2.5-inch, SAS/SATA Solid-State Disks (SSDs) and Hard-Disk Drives (HDDs)
- Up to 6 PCIe NVMe disk drives
- Cisco 12-Gbps SAS Modular RAID Controller in a dedicated slot
- M.2 boot options
- Dual embedded 10 Gigabit Ethernet LAN-On-Motherboard (LOM) ports

### UCS VIC 1400 Series Adapters

Support for the following new UCS VIC 1400 Series adapters on UCS M5 servers and UCS C125 servers:

- VIC 1495 40/100G PCIe for C-Series (UCSC-PCIE-C100-04)
- VIC 1497 40/100G mLOM for C-Series (UCSC-MLOM-C100-04)

This release introduces support for 40G Ethernet connections between the UCS 6300 Series Fabric Interconnects and C-Series servers in direct connect mode while using VIC 1495 or VIC 1497.

In this release, UCS VIC 1400 Series adapters for B-Series are supported on UCS Mini Fabric Interconnects. UCS 6454, UCS 6300 Series, and 6200 Series Fabric Interconnects support all UCS VIC 1400 Series adapters.

**Note** Cisco C-Series servers cannot be integrated with Cisco UCS Manager using a combination of Cisco UCS 6324 Fabric Interconnect and Cisco UCS VIC 14xx.

**Note** You cannot install VIC adapters from different series on the same server. For example, you cannot install UCS VIC 1300 Series adapters and UCS VIC 1400 Series adapters on the same server.

The following tables illustrate the supported VIC 1400 Series adapter/server combinations for Cisco UCS Manager Release 4.0(2):

*Table 1: VIC 1400 Series Adapter Support for M5 B-Series Servers*

| FI | IOM | 1400 Series VIC Adapters | | | |
|---|---|---|---|---|---|
| | | VIC 1440 | VIC 1440 + Port Expander | VIC 1480 | VIC 1440 + VIC 1480 |
| | | **UCSB-MLOM-40G-04** | **UCSB-MLOM-40G-04<br>+<br>UCSB-MLOM-PT-01** | **UCSB-VIC-M84-4P** | **UCSB-MLOM-40G-04<br>+<br>UCSB-VIC-M84-4P** |
| 6200 Series | 2204/2208 | B480 M5, B200 M5 | NA | B480 M5 | B480 M5, B200 M5 |
| 6300 Series | 2304 | B480 M5, B200 M5 | B480 M5, B200 M5 | B480 M5 | B480 M5, B200 M5 |
| | 2204/2208 | B480 M5, B200 M5 | NA | B480 M5 | B480 M5, B200 M5 |
| 6454 | 2204/2208<br>2408<br>Note: Support for 2408 (B-Series M4 and M5 servers) was added in Release 4.0(4e) | B480 M5, B200 M5 | NA | B480 M5 | B480 M5, B200 M5 |
| 6324 (UCS Mini | NA | B480 M5, B200 M5 | NA | B480 M5 | B480 M5, B200 M5 |
| | 2204/2208 | NA | NA | NA | NA |

*Table 2: VIC 1400 Series Adapter Support for M5 C-Series and S-Series Servers*

| FI | FEX | 1400 Series VIC Adapters | | | |
|---|---|---|---|---|---|
| | | VIC 1455 | VIC 1457 | VIC 1495 | VIC 1497 |
| | | UCSC-PCIE-C25Q-04 | UCSC-MLOM-C25Q-04 | UCSC-PCIE-C100-04 | UCSC-MLOM-C100-04 |
| 6200 Series | Direct Attach | C220 M5, C240 M5, C480 M5, C480 M5 ML, S3260 M5 (with UCS-S3260 -PCISIOC) | C220 M5, C240 M5 | NA | NA |
| | 2232 PP | C220 M5, C240 M5, C480 M5, S3260 M5 (with UCS-S3260 -PCISIOC) | C220 M5, C240 M5 | NA | NA |
| | 2232-T | NA | NA | NA | NA |

| FI | FEX | 1400 Series VIC Adapters | | | |
|---|---|---|---|---|---|
| | | VIC 1455 | VIC 1457 | VIC 1495 | VIC 1497 |
| | | UCSC-PCIE-C25Q-04 | UCSC-MLOM-C25Q-04 | UCSC-PCIE-C100-04 | UCSC-MLOM-C100-04 |
| 6300 Series | Direct Attach | C220 M5, C240 M5, C480 M5, C125 M5, C480 M5 ML, S3260 M5 (with UCS-S3260 -PCISIOC) | C220 M5, C240 M5 | C220 M5, C240 M5, C480 M5, C125 M5, C480 M5 ML, S3260 M5 (with UCS-S3260 -PCISIOC) | C220 M5, C240 M5 |
| | Direct Attach (Break-out) | C220 M5, C240 M5, C480 M5, C125 M5, S3260 M5 (with UCS-S3260 -PCISIOC) | C220 M5, C240 M5 | C220 M5, C240 M5, C480 M5, C125 M5, C480 M5 ML, S3260 M5 (with UCS-S3260 -PCISIOC) | C220 M5, C240 M5 |
| | 2232 PP | C220 M5, C240 M5, C480 M5, C125 M5, S3260 M5 (with UCS-S3260 -PCISIOC) | C220 M5, C240 M5 | NA | NA |
| | 2232-T | NA | NA | NA | NA |
| | 2348 | C220 M5, C240 M5, C480 M5, C125 M5, S3260 M5 (with UCS-S3260 -PCISIOC) | C220 M5, C240 M5 | NA | NA |

| FI | FEX | 1400 Series VIC Adapters | | | |
|---|---|---|---|---|---|
| | | VIC 1455 | VIC 1457 | VIC 1495 | VIC 1497 |
| | | UCSC-PCIE-C250-04 | UCSC-MLOM-C250-04 | UCSC-PCIE-C100-04 | UCSC-MLOM-C100-04 |
| 6454 | Direct Attach (10G/25G) | C220 M5, C240 M5, C480 M5, C125 M5, C480 M5 ML, S3260 M5 (with UCS-S3260-PCISIOC) | C220 M5, C240 M5 | NA | NA |
| | 2232 PP | C220 M5, C240 M5, C480 M5, C125 M5, S3260 M5 (with UCS-S3260-PCISIOC) | C220 M5, C240 M5 | NA | NA |
| | 2232-T | NA | NA | NA | NA |
| | 2348 | NA | NA | NA | NA |
| 6324 (UCS Mini | Direct Attach (10G) | NA | NA | NA | NA |
| | Direct Attach (Break-out) | NA | NA | NA | NA |

For more details regarding server and adapter combinations, refer the Server Spec Sheets:

- B-Series Server Spec Sheets
- C-Series Server Spec Sheets
- S-Series Server Spec Sheets

### UCS Mini with UCS VIC 1400 Series Adapters

Starting with Cisco UCS Manager Release 4.0(2), UCS Mini (6324) Fabric Interconnects support the following UCS VIC 1400 Series adapters for B-Series servers on the primary chassis:

- UCSB-MLOM-40G-04 (UCS VIC 1440)
- UCSB-VIC-M84-4P (UCS VIC 1480)

### Peripherals

- Support for NVIDIA V100 PCIe PG500-200 250W 32GB GPU cards (UCSC-GPU-V100-32) for UCS C240 M5 servers.
- Support for TPM2 (UCSX-TPM2-002-C) for all UCS servers.

- Support for hot-plug NVMe drive support on HyperFlex.
- Support for the High Voltage DC 1200 Watt Power Supply (N9K-PUV-1200W) on UCS 6454 Fabric Interconnects
- Support for Intel® Optane™ NVMe Extreme Performance Drives (UCSC-NVMEXP-I750)
- Support for the QLogic 10G Network Adapter card (UCSC-PCIE-QD10GC) on UCS C125.
- Support for the QLogic 25G Network Adapter card (UCSC-PCIE-QD25GF) on UCS C125.
- Support for the QLogic 100G Network Adapter card (UCSC-PCIE-QS100GF) on UCS C480 M5 ML.

## New Hardware in Release 4.0(1a)

### Fourth Generation Fabric Interconnect

The Cisco UCS 6454 Fabric Interconnect is a core part of the Cisco Unified Computing System, providing both network connectivity and management capabilities for the system. The Cisco UCS 6454 offers line-rate, low-latency, lossless 10/25/40/100 Gigabit Ethernet, Fibre Channel over Ethernet (FCoE), and Fibre Channel functions.

The Cisco UCS 6454 54-Port Fabric Interconnect is a one-rack-unit (1RU) 10/25/40/100 Gigabit Ethernet, FCoE and Fibre Channel switch offering up to 3.82 Tbps throughput and up to 54 ports. The switch has 40 10/25-Gbps fixed Ethernet, 8 10/25-Gbps Ethernet or 8/16/32G Fibre Channel ports and 6 40/100-Gbps Ethernet uplink ports. All Ethernet ports are capable of supporting FCoE.

### Cisco UCS C125 M5 Server

Cisco UCS Manager 4.0(1) supports Cisco UCS C125 M5 Servers on UCS 6300 Series and UCS 6454 Fabric Interconnects. The C125 M5 server is Cisco's first server based on AMD EPYC™ processors. Cisco UCS C125 M5 Servers are housed in the Cisco UCS C4200 Series rack server chassis. Each Cisco UCS C4200 Series rack server chassis supports two to four Cisco UCS C125 M5 Server nodes. The Cisco UCS C125 M5 Server supports the following peripherals:

- Dual Port 10Gbase-T and 10G/25G SFP28 OCP cards
- Cisco 12G 9460-8i PCIe 12G SAS RAID controller
- 32 GB, 64 GB, and 128 GB SD cards
- 32GB Micro-SD card

**Note** This is not managed through Cisco UCS Manager.

- 240 GB and 960 GB M.2 SATA SSD drives
- 16 GB Flash USB drive

**Note** This is not managed through Cisco UCS Manager.

- Mini Storage Carriers for SD and M.2 SATA

- On-board AHCI controllers

### New Generation SIOC for Cisco UCS S3260 Storage Servers

Cisco UCS S3260 Storage Server system supports a new server SIOC UCS-S3260-PCISIOC with S3260 M5 servers. This SIOC has PCIe slots to replace the network adapters. These slots support both Cisco VIC and third-party adapters. Additionally, the new SIOC has two NVME slots. For a complete list of supported cards and adapters, see the *Cisco UCS S3260 Server Integration with Cisco UCS Manager, Release 4.0* guide.

### UCS VIC 1400 Series Adapters

Support for the following UCS VIC 1400 Series adapters on UCS M5 servers:

- VIC 1440 10/40G mLOM for B-Series (UCSB-MLOM-40G-04)
- VIC 1480 10/40G PCIe for B-Series (UCSB-VIC-M84-4P)
- VIC 1455 10/25G PCIe for C-Series and S-Series (UCSC-PCIE-C25Q-04)
- VIC 1457 10/25G mLOM for C-Series (UCSC-MLOM-C25Q-04)

In Cisco UCS Manager Release 4.0(1), UCS VIC 1400 Series adapters are supported on UCS 6454, UCS 6300 Series, and 6200 Series Fabric Interconnects. They are not supported on UCS Mini. This release supports 10G/25G Ethernet connections between the UCS 6454 Fabric Interconnect and C-Series servers that have VIC 1455 or VIC 1457.

**Note** You cannot install VIC adapters from different series on the same server. For example, you cannot install UCS VIC 1300 Series adapters and UCS VIC 1400 Series adapters on the same server.

The following tables illustrate the supported VIC 1400 Series adapter/server combinations for Cisco UCS Manager Release 4.0(1):

***Table 3: VIC 1400 Series Adapter Support for M5 B-Series Servers***

| **FI** | **IOM** | **1400 Series VIC Adapters** | | | |
|---|---|---|---|---|---|
| | | **VIC 1440** | **VIC 1440 + Port Expander** | **VIC 1480** | **VIC 1440 + VIC 1480** |
| | | **UCSB-MLOM-40G-04** | **UCSB-MLOM-40G-04 + UCSB-MLOM-PT-01** | **UCSB-VIC-M84-4P** | **UCSB-MLOM-40G-04 + UCSB-VIC-M84-4P** |
| 6200 Series | 2204/2208 | B480 M5, B200 M5 | NA | B480 M5 | B480 M5, B200 M5 |
| 6300 Series | 2304 | B480 M5, B200 M5 | B480 M5, B200 M5 | B480 M5 | B480 M5, B200 M5 |
| | 2204/2208 | B480 M5, B200 M5 | NA | B480 M5 | B480 M5, B200 M5 |

| FI | IOM | 1400 Series VIC Adapters | | | |
|---|---|---|---|---|---|
| | | VIC 1440 | VIC 1440 + Port Expander | VIC 1480 | VIC 1440 + VIC 1480 |
| | | UCSB-MLOM-40G-04 | UCSB-MLOM-40G-04<br>+<br>UCSB-MLOM-PT-01 | UCSB-VIC-M84-4P | UCSB-MLOM-40G-04<br>+<br>UCSB-VIC-M84-4P |
| 6454 | 2204/2208 | B480 M5, B200 M5 | NA | B480 M5 | B480 M5, B200 M5 |

*Table 4: VIC 1400 Series Adapter Support for M5 C-Series and S-Series Servers*

| FI | FEX | 1400 Series VIC Adapters | |
|---|---|---|---|
| | | VIC 1455 | VIC 1457 |
| | | UCSC-PCIE-C25Q-04 | UCSC-MLOM-C25Q-04 |
| 6200 Series | Direct Attach | C220 M5, C240 M5, C480 M5, S3260 M5 (with UCS-S3260-PCISIOC) | C220 M5, C240 M5 |
| | 2232 PP | C220 M5, C240 M5, C480 M5, S3260 M5 (with UCS-S3260-PCISIOC) | C220 M5, C240 M5 |
| | 2232-T | NA | NA |
| 6300 Series | Direct Attach | C220 M5, C240 M5, C480 M5, C125 M5, S3260 M5 (with UCS-S3260-PCISIOC) | C220 M5, C240 M5 |
| | Direct Attach (Break-out) | C220 M5, C240 M5, C480 M5, C125 M5, S3260 M5 (with UCS-S3260-PCISIOC) | C220 M5, C240 M5 |
| | 2232 PP | C220 M5, C240 M5, C480 M5, C125 M5, S3260 M5 (with UCS-S3260-PCISIOC) | C220 M5, C240 M5 |
| | 2232-T | NA | NA |
| | 2348 | C220 M5, C240 M5, C480 M5, C125 M5, S3260 M5 (with UCS-S3260-PCISIOC) | C220 M5, C240 M5 |

| FI | FEX | 1400 Series VIC Adapters | |
|---|---|---|---|
| | | VIC 1455 | VIC 1457 |
| | | UCSC-PCIE-C25Q-04 | UCSC-MLOM-C25Q-04 |
| 6454 | Direct Attach (10G/25G) | C220 M5, C240 M5, C480 M5, C125 M5, S3260 M5 (with UCS-S3260-PCISIOC) | C220 M5, C240 M5 |
| | 2232 PP | C220 M5, C240 M5, C480 M5, C125 M5, S3260 M5 (with UCS-S3260-PCISIOC) | C220 M5, C240 M5 |
| | 2232-T | NA | NA |

**Note** For more details regarding server and adapter combinations, refer the Server Spec Sheets:

- B-Series Server Spec Sheets
- C-Series Server Spec Sheets
- S-Series Server Spec Sheets

### Peripherals

- Support for the HX-PCIE-OFFLOAD-1 co-processor card with C240Hx M5 servers
- Support for the High Voltage DC 1200 Watt Power Supply N9K-PUV-1200W on UCS 6332-16UP fabric interconnects
- Intel Optane NVMe Med. Performance Drives for M5 servers including C220, C240, C480, B200, B480, and S3260 and Hyperflex equivalents.
- Support for the LSI 9400-8e external SAS HBA on UCS C220, C240, C480 M5 servers.

## New Software Features in Release 4.0(4k)

- Support for AMD Platform Secure Boot (PSB) in Cisco UCS C125 M5 servers that implements hardware-rooted boot integrity. PSB ensures the integrity and authenticity of ROM image by using the root of trust integrated in the hardware.

## New Software Features in Release 4.0(4e)

### Support for UCS Fabric Extender 2408

UCS Fabric Extender 2408 (UCS-IOM-2408) enables deployment flexibility by supporting 10/25 GbE connectivity to B-Series M4 and M5 servers only on UCS 6454 Fabric Interconnects.

## New Software Features in Release 4.0(4c)

### ADDDC RAS Changes

- Adaptive Double Device Data Correction (ADDDC) is a memory RAS feature that enables dynamic mapping of failing DRAM by monitoring corrected errors and taking action before uncorrected errors can occur and cause an outage. It is now enabled by default.

  After ADDDC sparing remaps a memory region, the system could incur marginal memory latency and bandwidth penalties on memory bandwidth intense workloads that target the impacted region. Cisco recommends scheduling proactive maintenance to replace a failed DIMM after an ADDDC RAS fault is reported.

### BIOS Updates

- Default for **Select Memory RAS configuration** token changed from `Maximum Performance` to `ADDDC sparing` for all M5 servers.

### Intel ® VMD Enhancements to NVME

Support for Intel Volume Management Devices (VMD) for local storage on 4.0(4c) and later releases. Optional VMD driver .iso packages are available on the Cisco download site for the following Operating Systems:

- RHEL 7.3, 7.4, 7.5, 7.6
- CENTOS 7.3, 7.4, 7.5, 7.6
- SLES-15, SLES-15 v4
- Windows 2016, Windows 2019
- ESXi 6.5U2, 6.7U1, 6.7U2
- Ubuntu 18.04.1

Enhanced features provided by VMD provide support for hot-plugging of PCIe Solid State Drives (SSD), as well as the ability to use a command line interface to configure blinking patterns to indicate drive status.

## New Software Features in Release 4.0(4a)

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

### Intel® Optane™ Data Center Persistent Memory Modules

Cisco UCS Manager Release 4.0(4) introduces support for the Intel® Optane™ Data Center persistent memory modules on the UCS M5 servers that are based on the Second Generation Intel® Xeon® Scalable processors. Intel® Optane™ DC persistent memory modules can be used only with the Second Generation Intel® Xeon® Scalable processors.

This release provides the ability to configure and manage Intel® Optane™ DC persistent memory modules through Cisco UCS Manager. Persistent memory modules are non-volatile memory modules that bring together the low latency of memory and the persistence of storage. Data stored in persistent memory modules can be accessed quickly compared to other storage devices, and is retained across power cycles.

### Cisco UCS 6454 Fabric Interconnect Enhancements

- Multicast MAC-Filtering—This enhancement allows hosts to register for the type of traffic to be received, and facilitates traffic forwarding to vNICs based on this criteria.
- The number of unified ports have been increased from 8 to 16. Beginning with Cisco UCS Manager Release 4.0(4), the port numbering for Cisco UCS 6454 Fabric Interconnects is:

*Table 5: Port Numbering for UCS 6454 Fabric Interconnects*

| Ports | Description | Ports | Description |
|---|---|---|---|
| 1-16 | Unified Ports can operate as 10/25 Gbps Ethernet or 8/16/32 Gbps Fibre Channel. FC ports are converted in groups of 4 ports by the first 4 ports (port 1 to 4) or the first 8 ports (port 1 to 8). | 17-44 | Each port can operate as either a 10 Gbps or 25 Gbps SFP28 port. |
| 45-48 | Each port can operate as a 1 Gbps, 10 Gbps, or 25 Gbps Ethernet or FCoE port. | 49-54 | Each uplink port can operate as either a 40 Gbps or 100 Gbps Ethernet or FCoE port. When using a breakout cable, each of these ports can operate as 4 x 10 Gbps or 4 x 25 Gbps Ethernet or FCoE ports.<br>Ports 49-54 can be used only to connect to Ethernet or FCoE uplink ports, and not to UCS server ports. |

- Support for FCoE uplink ports in Fibre Channel switch mode on the Cisco UCS 6454 Fabric Interconnect.
- Maximum of 8 FCoE SAN uplink port channels are supported per Cisco UCS 6454 Fabric Interconnect, in both FC switch mode and FC end-host mode. A maximum of 4 FC SAN port channels are supported per Cisco UCS 6454 Fabric Interconnect.

  If a Cisco UCS 6454 Fabric Interconnect has a mix of FC SAN port channels and FCoE SAN port channels, they cannot exceed 8 port channels in total.

### Support for UCS Fabric Extender 2304V2

UCS Fabric Extender 2304V2 (UCS-IOM-2304V2) is based on UCS Fabric Extender 2304, I/O module with eight 40-Gigabit backplane ports and four 40-Gigabit uplink ports.

### Feature Enhancements

- Consistent Device Naming (CDN) support for SUSE Linux Enterprise Server (SLES)—CDN support has been expanded to include SLES 12 SP3, SLES 12 SP4, and SLES 15.
- Intel Speed Select—Intel Speed Select allows you to optimize CPU performance by selecting one of three operating profiles, based on the number of logical processor cores, frequency, and TDP thread setting. You can configure Intel Speed Select within a BIOS policy. At boot time, the BIOS discovers the supported CPU and configures it to one of three user-specified profiles.

- MSwitch Disaster Recovery—This enhancement enables you to recover a corrupted MSwitch and roll back to a previous working firmware.
- Alternate KVM Port—You can configure a port number between 1024 and 49151 as the KVM port.
- Disk Scrub for UCS S3260 M4 and M5 servers—This release extends the disk scrub feature for UCS S3260 M4 and M5 servers. For a server associated with a service profile, disk scrub occurs during disassociation, based on the scrub policy used in the service profile.
- Unified driver support for Fibre Channel and NVMe over Fibre Channel on SLES 12 SP4, SLES 15, and RHEL 7.6. This is in addition to being previously supported on SLES 12 SP3. This support is available on UCS 6300 Series Fabric Interconnects and UCS 6454 Fabric Interconnects. NVMe over Fibre Channel now supports up to 16 interfaces.
- Support for signed drivers in all supported Linux platforms. All Cisco Linux drivers are now cryptographically signed, which means that they can be used with UEFI Secure Boot on all supported Linux platforms. UEFI Secure Boot ensures that only trusted firmware and drivers are allowed to run at system boot, decreasing vulnerability to malware at boot time.
- Hardware RAID support for Cisco Boot Optimized M.2 RAID Controller (UCS-M2-HWRAID) on the following servers:
    - Cisco UCS C220 M5 Server
    - Cisco UCS C240 M5 Server
    - Cisco UCS C480 M5 Server
    - Cisco UCS B200 M5 Server
    - Cisco UCS B480 M5 Server

## New Software Features in Release 4.0(2a)

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

### Cisco UCS 6454 Fabric Interconnect Enhancements

This release introduces support for the following features on the Cisco UCS 6454 Fabric Interconnect:

- Support for Ethernet and Fibre Channel switching modes.

  In the Ethernet switching mode:

    - **VLAN Port Count Optimization Enabled** is not supported. Without **VLAN Port Count Optimization Enabled**, the Cisco UCS 6454 Fabric Interconnect supports 16000 PV count.

  In the Fibre Channel switching mode:

    - FCoE uplink is not supported

- Support for splitting a single 40/100G QSFP port into four 10/25G ports using a supported breakout cable. These ports can be used only as Ethernet uplink or FCoE uplink ports connecting to a 10/25G switch. They cannot be configured as server ports, FCoE storage ports, appliance ports or monitoring ports.
- Support for MAC Security on Cisco UCS 6454 Fabric Interconnects

### Cisco UCS C480 M5 ML Server

This release introduces support for Cisco UCS C480 M5 ML Servers.

The following features are not supported on Cisco UCS C480 M5 ML Servers:

- Rear NVME cage and PCIe NVME Switch Card
- Rear auxilliary drive cage
- Cisco 12G 9460-8i RAID controller (UCSC-SAS9460-8i)

### UCS VIC 1400 Series Adapter Enhancements

This release adds support for the newly introduced UCS VIC 1495 and 1497 adapters on UCS M5 servers.

The UCS VIC 1400 Series adapters now support the following features:

- Support for UCS Mini on UCS VIC 1440 and UCS VIC 1480 adapters on the primary chassis.
- Support for NVMe over Fibre Channel, which defines a mapping protocol for applying the NVMe interface to Fibre Channel. This release adds support for the **FC NVME Initiator** adapter policy on UCS 6300 Series Fabric Interconnects and UCS 6454 Fabric Interconnects.

  **FC NVME Target** and **FC Target** are available as Tech Preview options.
- FC Multi Queue—Enhanced I/O queue range support for FC Multi Queue. The new range is between 1 and 64 queues.
- Support for Windows 2016 VMQ and SET.
- Increased Tx and Rx queues for the eNIC driver—Is supported on all VIC 1400, 1300, and 1200 Series adapter cards on B-series and C-series servers. To efficiently use this speed, the number of Tx and Rx queues have been increased from 8 to 256 each. The eNIC driver now supports 256 Tx queues and 256 Rx queues. However, the maximum number of supported Rx and Tx queues cannot be more than the number of CPU cores in the system.

### Out of Band NVME Support on New Generation SIOC for Cisco UCS S3260 Storage Servers

Enhancement to support out of band NVME on the UCS-S3260-PCISIOC new generation SIOC for S3260 M5 servers.

### Feature Enhancements

- UCS Mini Fabric Interconnect Enhancements□Cisco UCS Manager Release 4.0(2) introduces the following enhancements for Cisco UCS Mini:
  - Cisco UCS Mini Fabric Interconnects now support the following VIC 1400 Series adapter cards for B-Series servers on the primary chassis:
    - UCSB-MLOM-40G-04 (UCS VIC 1440)
    - UCSB-VIC-M84-4P (UCS VIC 1480)
  - Cisco UCS Mini Fabric Interconnects with VIC 1300 Series adapter cards now support the following features:
    - usNIC

    - VXLAN
    - NetFlow

- Slow Drain—Cisco UCS Manager Release 4.0(2) introduces the QoS Slow Drain Detection and Mitigation feature on Cisco UCS 6454 Fabric Interconnects. This feature provides various enhancements that enable you to detect slow drain devices that cause congestion in the network, and also mitigate it.
- Simplified RAID0 Configuration—Cisco UCS Manager provides the ability to configure a range of disk slots into individual RAID0 LUNs by using the LUN set option.
- Support for SED security policies on B-Series M5 servers—Cisco UCS Manager Release 4.0(2) extends the SED security policies to UCS B-Series M5 servers.
- Support for Redfish version 1.01 on UCS C-Series servers that are attached to the Fabric Interconnect.
- Life Left on NVMe drives—NVMe statistics are now enhanced to display Life Left on NVMe drives based on their workload.
- Parallel Disk Update—Support for parallel firmware update on multiple disks.
- Support for optimized memory initialization and test processes to reduce boot times on UCS M5 servers—Cisco UCS Manager Release 4.0(2) introduces the following BIOS tokens to improve boot time for UCS M5 servers:
    - Adaptive Memory Training Control
    - OptionROM Launch Optimization Control
    - BIOS Tech Message Level Control

  The default value for all three tokens is **Enabled**.
- Certificate Manager for Device Connector—The Certificate Manager allows you to view a list of trusted certificates and import a valid trusted certificate.

## New Software Features in Release 4.0(1a)

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

### Cisco UCS 6454 Fabric Interconnect

This release introduces Cisco UCS 6454 Fabric Interconnects that support 10/25 Gigabit ports in the fabric with 40/100 Gigabit uplink ports. The *Cisco UCS Manager Getting Started Guide, Release 4.0* provides details about the specific ports.

**New Features Supported**

The Cisco UCS 6454 Fabric Interconnect introduces the following new features:

- Support for 10/25 Gigabit ports in the fabric with 40/100 Gigabit uplink ports
- Support for VIC 1400 Series adapters
- 128 additional VLANs reserved for internal usage
- Forward Error Correction (FEC) configurations for ports

Customer Certificate for KVM Usage— This Cisco UCS Manager release enables the KVM certificate to be changed on Cisco UCS M3 and M4 servers.

**Legacy Features Not Supported**

The following features are not supported on Cisco UCS 6454 Fabric Interconnects:

- Chassis Discovery Policy in Non-Port Channel Mode
- Chassis Connectivity Policy in Non-Port Channel Mode
- Ethernet or FC switching modes
- Service profiles with dynamic vNICs
- Multicast Optimize for QoS
- Netflow
- MAC security
- Port profiles and distributed virtual switches
- VMFEX

**Features Configured Differently**

The following features are configured differently on Cisco UCS 6454 Fabric Interconnects:

- Unified Ports—Cisco UCS 6454 fabric interconnects support up to 8 unified ports, which can be configured as FC.
- VLAN Optimization—On Cisco UCS 6454 Fabric Interconnects, the PV count is as follows:
  - with VLAN port count optimization disabled—16000
  - with VLAN port count optimization enabled—64000

### Cisco UCS C125 M5 Server

This release introduces support for Cisco UCS C125 M5 Servers.

The following are the two main differences between C125 M5 servers and other rack servers.

- Power capping is not supported on Cisco UCS C125 M5 Servers.
- For Cisco UCS C125 M5 Servers, ensure that you select the same **Fan Speed Policy** for all the servers in an enclosure. Cisco UCS Manager applies the **Fan Speed Policy** of the server which gets associated last. Having the same **Fan Speed Policy** for the all the server ensures that the desired **Fan Speed Policy** is applied irrespective of which server is associated last.

### UCS VIC 1400 Series Adapters

Support for UCS VIC 1400 Series adapters on UCS M5 servers.

These adapters introduce support for the following new features:

- Stateless offloads with VxLAN and NVGRE encapsulation for Windows
- VMMQ for Windows

- UDP RSS for ESXi and Linux
- IPv6 Header support
- NetFlow
- QoS support
- Port channel support with UCS VIC 1455 and 1457 adapters

**Note** Cisco UCS Manager Release 4.0(1) supports only single link port channel for FC/FCoE between VIC 1455 or 1457 adapters that are on direct-connect rack-servers, and UCS 6300 Series Fabric Interconnects.

**Note** In the port-channel, both ports should have same speed.

The following features are not supported on UCS VIC 1400 Series adapters:

- VM-FEX for Hyper-V
- VM-FEX for VMware
- Dynamic vNICs
- A port channel with four member ports on UCS VIC 1455 and 1457 adapters
- usNIC on Cisco UCS C125 M5 Servers

### New Generation SIOC for Cisco UCS S3260 Storage Servers

Support for S3260 M5 servers with a new server SIOC UCS-S3260-PCISIOC and the VIC 1400 Series adapter cards.

### Feature Enhancements

- Pre-enablement support for Hyperflex 3.5 release features
- Support for KMIP client on C480 M5 to support integration with key management servers
- Support for the IPv6 option on PXE boot devices on Cisco UCS Manager managed C-Series and S-Series M4 servers.
- Support for the **Login Profile** feature, which provides the ability to block login requests to Cisco UCS Manager for a specific period after failed login attempts. This feature is currently supported only on UCS 6454 Fabric Interconnects and on Cisco UCS Manager Release 4.0(1) and later releases.

## Deprecated Hardware and Software in Cisco UCS Manager Release 4.0

Cisco UCS Manager Release 4.0 does not support UCS B-Series M2 generation blade servers. Cisco UCS Manager Release 4.0 does not support hardware or software that was deprecated in previous releases of Cisco UCS Manager.

## 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 and some previous C-Series standalone releases. For example, Cisco UCS Manager Release 4.0(1) is integrated with C-Series Standalone Release 4.0(1) for the M5 servers and Release 3.0(4) for all M3 and M4 servers. Hence, it supports all the M5, M4 and M3 servers supported by C-Series Standalone releases.

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

*Table 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 |
|---|---|---|
| 4.0(4) | 4.0(4) | C220 M5, C240 M5, C480 M5, S3260 M5, C480 M5 ML only |
| | 4.0(2) | C220 M4, C240 M4, C460 M4, S3260 M4, C125 M5 only |
| | 3.0(4) | All M3 |
| 4.0(2) | 4.0(2) | C220 M4, C240 M4, C460 M4, C220 M5, C240 M5, C480 M5, S3260 M4, S3260 M5, C125 M5, C480 M5 ML only |
| | 3.0(4) | All M3 |
| 4.0(1) | 4.0(1) | C220 M4, C240 M4, C460 M4, C220 M5, C240 M5, C480 M5, S3260 M4, S3260 M5, C125 M5 only |
| | 3.0(4) | All M3 |
| 3.2(3) | 3.1(3) | C220 M5, C240 M5, C480 M5, S3260 M5 only |
| | 3.0(4) | All M3/M4 |
| 3.2(2) | 3.1(2) | C220 M5, C240 M5, C480 M5 only |
| | 3.0(3) | All M3/M4 |
| 3.2(1) | 3.1(1) | C220 M5, C240 M5 only |
| | 3.0(3) | All M3/M4 |

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

# System Requirements

### Cisco UCS Central Integration

Cisco UCS Manager Release 4.0 can only be registered with Cisco UCS Central, Release 2.0(1f) or higher.

### Supported Operating Systems

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

### Supported Web Browsers

| Cisco UCS Manager GUI | Web Browsers |
|---|---|
| HTML5 | Microsoft Internet Explorer 11 or higher<br>Mozilla Firefox 45 or higher<br>Google Chrome 45 or higher<br>Apple Safari version 9 or higher<br>Opera version 35 or higher |

### Network Requirements

For using the device connector feature, you must configure HTTPS proxy settings. The *Cisco UCS Manager Administration Management Guide, Release 4.0* provides detailed information about configuring the device connector.

## Cross-Version Firmware Support

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

The following table lists the mixed A, B, and C bundle versions that are supported on Cisco UCS 6200, 6300, and 6454 fabric interconnects:

*Table 7: Mixed Cisco UCS Releases Supported on Cisco UCS 6200, 6300, 6454 Fabric Interconnects*

| | **Infrastructure Versions (A Bundles)** | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Host FW Versions (B or C Bundles) | 2.2(8) | 3.1(3) | 3.2(1) | 3.2(2) | 3.2(3) | 4.0(1) | 4.0(2) | 4.0(4) |
| 2.2(8) | 6200 | 6200 | 6200 | 6200 | 6200 | 6200 | 6200 | 6200 |
| 3.1(3) | — | 6200,6332, 6332-16UP | 6200,6332, 6332-16UP | 6200,6332, 6332-16UP | 6200,6332, 6332-16UP | 6200,6332, 6332-16UP | 6200,6332, 6332-16UP | 6200,6332, 6332-16UP |
| 3.2(1) | — | — | 6200,6332, 6332-16UP | 6200,6332, 6332-16UP | 6200,6332, 6332-16UP | 6200,6332, 6332-16UP | 6200,6332, 6332-16UP | 6200,6332, 6332-16UP |
| 3.2(2) | — | — | 6200,6332, 6332-16UP | 6200,6332, 6332-16UP | 6200,6332, 6332-16UP | 6200,6332, 6332-16UP | 6200,6332, 6332-16UP | 6200,6332, 6332-16UP |
| 3.2(3) | — | — | 6200,6332, 6332-16UP | 6200,6332, 6332-16UP | 6200,6332, 6332-16UP | 6200,6332, 6332-16UP | 6200,6332, 6332-16UP | 6200,6332, 6332-16UP |
| 4.0(1) | — | — | — | — | — | 6200,6332, 6332-16UP, 6454 | 6200,6332, 6332-16UP, 6454 | 6200,6332, 6332-16UP, 6454 |
| 4.0(2) | — | — | — | — | — | 6200,6332, 6332-16UP, 6454 | 6200,6332, 6332-16UP, 6454 | 6200,6332, 6332-16UP, 6454 |
| 4.0(4) | — | — | — | — | — | 6200,6332, 6332-16UP, 6454 | 6200,6332, 6332-16UP, 6454 | 6200,6332, 6332-16UP, 6454 |

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

*Table 8: Mixed Cisco UCS Releases Supported on Cisco UCS Mini Fabric Interconnects*

| | **Infrastructure Versions (A Bundles)** | | | | | | |
|---|---|---|---|---|---|---|---|
| Host FW Versions (B or C Bundles) | 3.1(3) | 3.2(1) | 3.2(2) | 3.2(3) | 4.0(1) | 4.0(2) | 4.0(4) |
| 3.1(3) | 6324 | 6324 | 6324 | 6324 | 6324 | 6324 | 6324 |
| 3.2(1) | — | 6324 | 6324 | 6324 | 6324 | 6324 | 6324 |
| 3.2(2) | — | 6324 | 6324 | 6324 | 6324 | 6324 | 6324 |
| 3.2(3) | — | 6324 | 6324 | 6324 | 6324 | 6324 | 6324 |
| 4.0(1) | — | — | — | — | 6324 | 6324 | 6324 |
| 4.0(2) | — | — | — | — | 6324 | 6324 | 6324 |
| 4.0(4) | — | — | — | — | 6324 | 6324 | 6324 |

The following table lists the mixed B, C bundles that are supported on all platforms with the 4.0(4)A bundle:

*Table 9: Mixed B, C Bundles Supported on All Platforms with the 4.0(4)A Bundle*

| | **Infrastructure Versions (A Bundles)** | | | |
|---|---|---|---|---|
| **Host FW Versions (B, C Bundles)** | 4.0(4) | | | |
| | 6200 | 6300 | 6324 | 6454 |
| | ucs-k9-bundle-infra. 4.0.x.xxx.A.bin | ucs-6300-k9-bundle-infra. 4.0.x.xxx.A.bin | ucs-mini-k9-bundle-infra. 4.0.x.xxx.A.bin | ucs-6400-k9 -bundle-infra. 4.0.x.xxx.A.bin |
| 2.2(8)<br>(B, C Bundles) | Yes | — | — | — |
| 3.1(3)<br>(B, C Bundles) | Yes | Yes | Yes | — |
| 3.2(1), 3.2(2), 3.2(3)<br>(B, C Bundles) | Yes | Yes | Yes | — |
| 4.0(1), 4.0(2), 4.0(4)<br>(B, C Bundles) | Yes | Yes | Yes | Yes |

The following table lists the mixed B, C bundles that are supported on all platforms with the 4.0(2)A bundle:

*Table 10: Mixed B, C Bundles Supported on All Platforms with the 4.0(2)A Bundle*

| | Infrastructure Versions (A Bundles) | | | |
|---|---|---|---|---|
| **Host FW Versions (B, C Bundles)** | 4.0(2) | | | |
| | 6200 | 6300 | 6324 | 6454 |
| | ucs-k9-bundle-infra. 4.0.x.xxx.A.bin | ucs-6300-k9-bundle-infra. 4.0.x.xxx.A.bin | ucs-mini-k9-bundle-infra. 4.0.x.xxx.A.bin | ucs-6400-k9 -bundle-infra. 4.0.x.xxx.A.bin |
| 2.2(8)<br>(B, C Bundles) | Yes | — | — | — |
| 3.1(3)<br>(B, C Bundles) | Yes | Yes | Yes | — |
| 3.2(1), 3.2(2), 3.2(3)<br>(B, C Bundles) | Yes | Yes | Yes | — |
| 4.0(1), 4.0(2), 4.0(4)<br>(B, C Bundles) | Yes | Yes | Yes | Yes |

The following table lists the mixed B, C bundles that are supported on all platforms with the 4.0(1)A bundle:

*Table 11: Mixed B, C Bundles Supported on All Platforms with the 4.0(1)A Bundle*

| | Infrastructure Versions (A Bundles) | | | |
|---|---|---|---|---|
| **Host FW Versions (B, C Bundles)** | 4.0(1) | | | |
| | 6200 | 6300 | 6324 | 6454 |
| | ucs-k9-bundle-infra. 4.0.x.xxx.A.bin | ucs-6300-k9-bundle-infra. 4.0.x.xxx.A.bin | ucs-mini-k9-bundle-infra. 4.0.x.xxx.A.bin | ucs-6400-k9 -bundle-infra. 4.0.x.xxx.A.bin |
| 2.2(8)<br>(B, C Bundles) | Yes | — | — | — |
| 3.1(3)<br>(B, C Bundles) | Yes | Yes | Yes | — |
| 3.2(1), 3.2(2), 3.2(3)<br>(B, C Bundles) | Yes | Yes | Yes | — |

| | Infrastructure Versions (A Bundles) | | | |
|---|---|---|---|---|
| 4.0(1), 4.0(2), 4.0(4)<br>(B, C Bundles) | Yes | Yes | Yes | Yes |

**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.

# Internal Dependencies

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

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

## 6200 Series, 6332 Series, and 6454 Fabric Interconnects and Components

### Blade Servers

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

*Table 12: Minimum Host Firmware Versions for Blade Servers*

| Servers | Minimum Software Version<br>UCS 6200 Series FI | Minimum Software Version<br>UCS 6332, 6332-16UP FI | Minimum Software Version<br>UCS 6332, 6332-16UP FI | | Minimum Software Version<br>UCS 6454 FI | Suggested Software Version<br>UCS 6200 Series FI<br>UCS 6332, 6332-16UP FI<br>UCS 6454 FI |
|---|---|---|---|---|---|---|
| | UCS-IOM-2204<br>UCS-IOM-2208 | UCS-IOM-2204<br>UCS-IOM-2208 | UCS-IOM-2304 | UCS-IOM-2304V2 | UCS-IOM-2204<br>UCS-IOM-2208<br>UCS-IOM-2408* | UCS-IOM-2204<br>UCS-IOM-2208<br>UCS-IOM-2408* |
| | | | | | * UCS-IOM-2408 supported on M4 and M5 only with UCS 6454 FI & VIC 1300/1400 | |
| B22 M3 E5-2400<br>B22 M3 E5-2400 v2<br>**Note:** M3 servers do not support the 6454 FI and 2408 IOM combination. However, they do support the 6454 FI and 2208 IOM, and 6454 FI and 2204 IOM combinations. | 2.2(8a)<br>2.2(8a) | 3.1(3a)<br>3.1(3a) | 3.1(3a) | 4.0(4o) | 4.0(1a) | 4.0(4o) |
| B200 M3 E5-2600<br>B200 M3 E5-2600 v2<br>**Note:** M3 servers do not support the 6454 FI and 2408 IOM combination. However, they do support the 6454 FI and 2208 IOM, and 6454 FI and 2204 IOM combinations. | 2.2(8a)<br>2.2(8a) | 3.1(3a)<br>3.1(3a) | 3.1(3a) | 4.0(4o) | 4.0(1a) | 4.0(4o) |
| B200 M4 | 2.2(8a) | 3.1(3a) | 3.1(3a) | 4.0(4o) | 4.0(1a) | 4.0(4o) |
| B200 M5 | 3.2(1d) | 3.2(1d) | 3.2(1d) | 4.0(4o) | 4.0(1a) | 4.0(4o) |

| Servers | Minimum Software Version<br>UCS 6200 Series FI | Minimum Software Version<br>UCS 6332, 6332-16UP FI | Minimum Software Version<br>UCS 6332, 6332-16UP FI | | Minimum Software Version<br>UCS 6454 FI | Suggested Software Version<br>UCS 6200 Series FI<br>UCS 6332, 6332-16UP FI<br>UCS 6454 FI |
|---|---|---|---|---|---|---|
| | UCS-IOM-2204<br>UCS-IOM-2208 | UCS-IOM-2204<br>UCS-IOM-2208 | UCS-IOM-2304 | UCS-IOM-2304V2 | UCS-IOM-2204<br>UCS-IOM-2208<br>UCS-IOM-2408* | UCS-IOM-2204<br>UCS-IOM-2208<br>UCS-IOM-2408* |
| | | | | | * UCS-IOM-2408 supported on M4 and M5 only with UCS 6454 FI & VIC 1300/1400 | |
| B260 M4 E7-2800 v2<br>B260 M4 E7-4800 v2<br>B260 M4 E7-8800 v2<br>B260 M4 E7-4800 v3<br>B260 M4 E7-8800 v3 | 2.2(8a)<br>2.2(8a)<br>2.2(8a)<br>2.2(8a)<br>2.2(8a) | 3.1(3a)<br>3.1(3a)<br>3.1(3a)<br>3.1(3a)<br>3.1(3a) | 3.1(3a) | 4.0(4o) | 4.0(1a) | 4.0(4o) |
| B260 M4 E7-4800 v4<br>B260 M4 E7-8800 v4 | 2.2(8b)<br>2.2(8b) | 3.1(3a)<br>3.1(3a) | 3.1(3a)<br>3.1(3a) | 4.0(4o) | 4.0(1a) | 4.0(4o) |
| B420 M3 E5-4600<br>B420 M3 E5-4600 v2 | 2.2(8a)<br>2.2(8a) | 3.1(3a)<br>3.1(3a) | 3.1(3a) | 4.0(4o) | 4.0(1a) | 4.0(4o) |
| B420 M4 E5-4600 v3<br>B420 M4 E5-4600 v4 | 2.2(8a)<br>2.2(8b) | 3.1(3a)<br>3.1(3a) | 3.1(3a)<br>3.1(3a) | 4.0(4o) | 4.0(1a) | 4.0(4o) |

| Servers | Minimum Software Version<br>UCS 6200 Series FI | Minimum Software Version<br>UCS 6332, 6332-16UP FI | Minimum Software Version<br>UCS 6332, 6332-16UP FI | | Minimum Software Version<br>UCS 6454 FI | Suggested Software Version<br>UCS 6200 Series FI<br>UCS 6332, 6332-16UP FI<br>UCS 6454 FI |
|---|---|---|---|---|---|---|
| | UCS-IOM-2204<br>UCS-IOM-2208 | UCS-IOM-2204<br>UCS-IOM-2208 | UCS-IOM-2304 | UCS-IOM-2304V2 | UCS-IOM-2204<br>UCS-IOM-2208<br>UCS-IOM-2408* | UCS-IOM-2204<br>UCS-IOM-2208<br>UCS-IOM-2408* |
| | | | | | * UCS-IOM-2408 supported on M4 and M5 only with UCS 6454 FI & VIC 1300/1400 | |
| B460 M4 E7-4800 v2<br>B460 M4 E7-8800 v2<br>B460 M4 E7-4800 v3<br>B460 M4 E7-8800 v3 | 2.2(8a)<br>2.2(8a)<br>2.2(8a)<br>2.2(8a) | 3.1(3a)<br>3.1(3a)<br>3.1(3a)<br>3.1(3a) | 3.1(3a) | 4.0(4o) | 4.0(1a) | 4.0(4o) |
| B460 M4 E7-4800 v4<br>B460 M4 E7-8800 v4 | 2.2(8b)<br>2.2(8b) | 3.1(3a)<br>3.1(3a) | 3.1(3a) | 4.0(4o) | 4.0(1a) | 4.0(4o) |
| B480 M5 | 3.2(2b) | 3.2(2b) | 3.2(2b) | 4.0(4o) | 4.0(1a) | 4.0(4o) |

### Rack Servers

*Table 13: Minimum Host Firmware Versions for Rack Servers*

| Servers | Minimum Software Version<br>UCS 6200 Series FI | Minimum Software Version<br>UCS 6332, 6332-16UP | Minimum Software Version<br>UCS 6454 | Suggested Software Version<br>UCS 6200 Series FI<br>UCS 6332, 6332-16UP FI<br>UCS 6454 |
|---|---|---|---|---|
| C22 M3 and M3L | 2.2(8a) | 3.1(3a) | 4.0(1a) | 4.0(4o) |

| Servers | Minimum Software Version<br>UCS 6200 Series FI | Minimum Software Version<br>UCS 6332, 6332-16UP | Minimum Software Version<br>UCS 6454 | Suggested Software Version<br>UCS 6200 Series FI<br>UCS 6332, 6332-16UP FI<br>UCS 6454 |
|---|---|---|---|---|
| C24 M3, M3L, and M3S2 | 2.2(8a) | 3.1(3a) | 4.0(1a) | 4.0(4o) |
| C220 M3 | 2.2(8a) | 3.1(3a) | 4.0(1a) | 4.0(4o) |
| C220 M4 | 2.2(8a) | 3.1(3a) | 4.0(1a) | 4.0(4o) |
| C220 M5 | 3.2(1d) | 3.2(1d) | 4.0(1a) | 4.0(4o) |
| C240 M3 | 2.2(8a) | 3.1(3a) | 4.0(1a) | 4.0(4o) |
| C240 M4 | 2.2(8a) | 3.1(3a) | 4.0(1a) | 4.0(4o) |
| C240 M5 | 3.2(1d) | 3.2(1d) | 4.0(1a) | 4.0(4o) |
| C460 M4 E7-2800 v2<br>C460 M4 E7-4800 v2<br>C460 M4 E7-8800 v2<br>C460 M4 E7-4800 v3<br>C460 M4 E7-8800 v3 | 2.2(8a)<br>2.2(8a)<br>2.2(8a)<br>2.2(8a)<br>2.2(8a) | 3.1(3a)<br>3.1(3a)<br>3.1(3a)<br>3.1(3a)<br>3.1(3a) | 4.0(1a) | 4.0(4o) |
| C460 M4 E7-8800 v4 | 2.2(8b) | 3.1(3a) | 4.0(1a) | 4.0(4o) |
| C480 M5 | 3.2(2b) | 3.2(2b) | 4.0(1a) | 4.0(4o) |
| S3260 M4 | 3.1(2b) | 3.1(3a) | 4.0(1a) | 4.0(4o) |
| S3260 M5 | 3.2(3a) | 3.2(3a) | 4.0(1a) | 4.0(4o) |
| C125 M5 | NA | 4.0(1a) | 4.0(1a) | 4.0(4o) (only on UCS 6332, UCS 6332-16UP FI, and UCS 6454 |
| C480 M5 ML | 4.0(2a) | 4.0(2a) | 4.0(2a) | 4.0(4o) |

## Adapters

*Table 14: Minimum Software Versions for Adapters*

| Adapters | Minimum Software Version<br>UCS 6200 Series FI | Minimum Software Version<br>UCS 6332, 6332-16UP | Minimum Software Version<br>UCS 6332, 6332-16UP | Minimum Software Version<br>UCS 6454 | Suggested Software Version<br>UCS 6200 Series FI<br>UCS 6332, 6332-16UP FI<br>UCS 6454 |
|---|---|---|---|---|---|
| | UCS-IOM-2204<br>UCS-IOM-2208 | UCS-IOM-2204<br>UCS-IOM-2208 | UCS-IOM-2304<br>UCS-IOM-2304V2 | UCS-IOM-2204<br>UCS-IOM-2208 | UCS-IOM-2204<br>UCS-IOM-2208<br>UCS-IOM-2408* |
| | | | | * UCS-IOM-2408 supported on M4 and M5 only with UCS 6454 FI | |
| UCSC-P-M4D25GF (Mellanox MCX4121A-ACAT Dual Port 10/25G SFP28 NIC) | 4.0(4o) | 4.0(4o) | 4.0(4o) | 4.0(4o) | 4.0(4o) |
| UCSC-PCIE-QS100GF (QLogic QL45611HLCU 100GbE) | 4.0(4o) | 4.0(4o) | 4.0(4o) | 4.0(4o) | 4.0(4o) |
| UCSC-PCIE-C100-04 (UCS VIC 1495) | NA | 4.0(2a) | 4.0(2a) | NA | 4.0(4o)(only on UCS 6332, 6332-16UP FI) |
| UCSC-MLOM-C100-04 (UCS VIC 1497) | NA | 4.0(2a) | 4.0(2a) | NA | 4.0(4o)(only on UCS 6332, 6332-16UP FI) |
| UCSB-MLOM-40G-04 (UCS VIC 1440) | 4.0(1a) | 4.0(1a) | 4.0(1a) | 4.0(1a) | 4.0(4o) |
| UCSB-VIC-M84-4P (UCS VIC 1480) | 4.0(1a) | 4.0(1a) | 4.0(1a) | 4.0(1a) | 4.0(4o) |
| UCSC-PCIE-C25Q-04 (UCS VIC 1455) | 4.0(1a) | 4.0(1a) | 4.0(1a) | 4.0(1a) | 4.0(4o) |
| UCSC-MLOM-C25Q-04 (UCS VIC 1457) | 4.0(1a) | 4.0(1a) | 4.0(1a) | 4.0(1a) | 4.0(4o) |

| **Adapters** | **Minimum Software Version**<br>**UCS 6200 Series FI** | **Minimum Software Version**<br>**UCS 6332, 6332-16UP** | **Minimum Software Version**<br>**UCS 6332, 6332-16UP** | **Minimum Software Version**<br>**UCS 6454** | **Suggested Software Version**<br>**UCS 6200 Series FI**<br>**UCS 6332, 6332-16UP FI**<br>**UCS 6454** |
|---|---|---|---|---|---|
| | **UCS-IOM-2204**<br>**UCS-IOM-2208** | **UCS-IOM-2204**<br>**UCS-IOM-2208** | **UCS-IOM-2304**<br>**UCS-IOM-2304V2** | **UCS-IOM-2204**<br>**UCS-IOM-2208** | **UCS-IOM-2204**<br>**UCS-IOM-2208**<br>**UCS-IOM-2408*** |
| | | | | *** UCS-IOM-2408 supported on M4 and M5 only with UCS 6454 FI** | |
| UCSC-PCIE-BD16GF (Emulex LPe31002 Dual-Port 16G FC HBA) | 3.2(3a) | 3.2(3a) | 3.2(3a) | 4.0(1a) | 4.0(4o) |
| UCSC-PCIE-ID40GF (Intel XL710 adapter) | 3.2(3a) | 3.2(3a) | 3.2(3a) | 4.0(1a) | 4.0(4o) |
| UCSC-PCIE-IQ10GF (Intel X710-DA4 adapter) | 3.2(3a) | 3.2(3a) | 3.2(3a) | 4.0(1a) | 4.0(4o) |
| UCSC-PCIE-ID10GF (Intel X710-DA2 adapter) | 3.2(3a) | 3.2(3a) | 3.2(3a) | 4.0(1a) | 4.0(4o) |
| XXV710-DA2 (Intel XXV710-DA2 adapter) | 3.2(3a) | 3.2(3a) | 3.2(3a) | 4.0(1a) | 4.0(4o) |
| UCSC-PCIE-ID10GC (Intel X550-T2 adapter) | 3.2(3a) | 3.2(3a) | 3.2(3a) | 4.0(1a) | 4.0(4o) |
| N2XX-AIPCI01 (Intel X520 dual port adapter) | 3.2(3a) | 3.2(3a) | 3.2(3a) | 4.0(1a) | 4.0(4o) |
| UCSC-PCIE-ID25GF (Intel X710 25Gb Dual-port BaseT) | 3.2(3a) | 3.2(3a) | 3.2(3a) | 4.0(1a) | 4.0(4o) |

| Adapters | Minimum Software Version<br>UCS 6200 Series FI | Minimum Software Version<br>UCS 6332, 6332-16UP | Minimum Software Version<br>UCS 6332, 6332-16UP | Minimum Software Version<br>UCS 6454 | Suggested Software Version<br>UCS 6200 Series FI<br>UCS 6332, 6332-16UP FI<br>UCS 6454 |
|---|---|---|---|---|---|
| | UCS-IOM-2204<br>UCS-IOM-2208 | UCS-IOM-2204<br>UCS-IOM-2208 | UCS-IOM-2304<br>UCS-IOM-2304V2 | UCS-IOM-2204<br>UCS-IOM-2208 | UCS-IOM-2204<br>UCS-IOM-2208<br>UCS-IOM-2408* |
| | | | | * UCS-IOM-2408 supported on M4 and M5 only with UCS 6454 FI | |
| UCSC-PCIE-QD25GF (QLogic QL41212H 25GbE) | 3.2(2b) | 3.2(2b) | 3.2(2b) | 4.0(1a) | 4.0(4o) |
| UCSC-PCIE-QD40GF (QLogic QL45212H 40GbE) | 3.2(2b) | 3.2(2b) | 3.2(2b) | 4.0(1a) | 4.0(4o) |
| UCSC-PCIE-IQ10GC (Intel X710-T4) | 3.2(2b) | 3.2(2b) | 3.2(2b) | 4.0(1a) | 4.0(4o) |
| UCSC-PCIE-QD16GF (QLogic QLE2692-CSC) | 3.2(1d) | 3.2(1d) | 3.2(1d) | 4.0(1a) | 4.0(4o) |
| UCSC-PCIE-C40Q-03 (UCS VIC 1385)<br>UCSC-MLOM-C40Q-03 (UCS VIC 1387) | 2.2(8a) | 3.1(3a) | 3.1(3a) | 4.0(1a) | 4.0(4o) |
| UCS-VIC-M82-8P (UCS VIC 1280)<br>UCSB-MLOM-40G-01 (UCS VIC 1240)<br>UCSB-MLOM-PT-01 (Cisco Port Expander Card) | 2.2(8a) | 3.1(3a) | 3.1(3a) | 4.0(1a) | 4.0(4o) |

| Adapters | Minimum Software Version<br>UCS 6200 Series FI | Minimum Software Version<br>UCS 6332, 6332-16UP | Minimum Software Version<br>UCS 6332, 6332-16UP | Minimum Software Version<br>UCS 6454 | Suggested Software Version<br>UCS 6200 Series FI<br>UCS 6332, 6332-16UP FI<br>UCS 6454 |
|---|---|---|---|---|---|
| | UCS-IOM-2204<br>UCS-IOM-2208 | UCS-IOM-2204<br>UCS-IOM-2208 | UCS-IOM-2304<br>UCS-IOM-2304V2 | UCS-IOM-2204<br>UCS-IOM-2208 | UCS-IOM-2204<br>UCS-IOM-2208<br>UCS-IOM-2408* |
| | | | | * UCS-IOM-2408 supported on M4 and M5 only with UCS 6454 FI | |
| UCSB-MLOM-40G-03 (UCS VIC 1340)<br>UCSB-VIC-M83-8P (UCS VIC 1380)<br>UCSC-MLOM-CSC-02 (UCS VIC 1227) | 2.2(8a) | 3.1(3a) | 3.1(3a) | 4.0(1a) | 4.0(4o) |
| UCSC-PCIE-CSC-02 (UCS VIC 1225) | 2.2(8a) | 3.1(3a) | 3.1(3a) | 4.0(1a) | 4.0(4o) |
| UCSC-F-FIO-1000MP (Cisco UCS Fusion ioMemory – PX600, 1.0TB)<br>UCSC-F-FIO-1300MP (Cisco UCS Fusion ioMemory – PX600, 1.3TB)<br>UCSC-F-FIO-2600MP (Cisco UCS Fusion ioMemory – PX600, 2.6TB)<br>UCSC-F-FIO-5200MP (Cisco UCS Fusion ioMemory – PX600, 5.2TB) | 2.2(8a) | 3.1(3a) | 3.1(3a) | 4.0(1a) | 4.0(4o) |

| Adapters | Minimum Software Version<br>UCS 6200 Series FI | Minimum Software Version<br>UCS 6332, 6332-16UP | Minimum Software Version<br>UCS 6332, 6332-16UP | Minimum Software Version<br>UCS 6454 | Suggested Software Version<br>UCS 6200 Series FI<br>UCS 6332, 6332-16UP FI<br>UCS 6454 |
|---|---|---|---|---|---|
| | UCS-IOM-2204<br>UCS-IOM-2208 | UCS-IOM-2204<br>UCS-IOM-2208 | UCS-IOM-2304<br>UCS-IOM-2304V2 | UCS-IOM-2204<br>UCS-IOM-2208 | UCS-IOM-2204<br>UCS-IOM-2208<br>UCS-IOM-2408* |
| | | | | * UCS-IOM-2408 supported on M4 and M5 only with UCS 6454 FI | |
| UCSB-FIO-1600MS (Cisco UCS Fusion ioMemory Mezzanine SX300, 1.6TB)<br>UCSB-FIO-1300MS (Cisco UCS Fusion ioMemory Mezzanine PX600, 1.3TB) | 2.2(8a) | 3.1(3a) | 3.1(3a) | 4.0(1a) | 4.0(4o) |
| UCSC-INVADER-3108<br>UCSC-NYTRO-200GB (Cisco Nytro MegaRAID 200GB Controller) | 2.2(8a) | 3.1(3a) | 3.1(3a) | 4.0(1a) | 4.0(4o) |

| Adapters | Minimum Software Version<br>UCS 6200 Series FI | Minimum Software Version<br>UCS 6332, 6332-16UP | Minimum Software Version<br>UCS 6332, 6332-16UP | Minimum Software Version<br>UCS 6454 | Suggested Software Version<br>UCS 6200 Series FI<br>UCS 6332, 6332-16UP FI<br>UCS 6454 |
|---|---|---|---|---|---|
| | UCS-IOM-2204<br>UCS-IOM-2208 | UCS-IOM-2204<br>UCS-IOM-2208 | UCS-IOM-2304<br>UCS-IOM-2304V2 | UCS-IOM-2204<br>UCS-IOM-2208 | UCS-IOM-2204<br>UCS-IOM-2208<br>UCS-IOM-2408* |
| | | | | * UCS-IOM-2408 supported on M4 and M5 only with UCS 6454 FI | |
| | 2.2(8a) | 3.1(3a) | 3.1(3a) | 4.0(1a) | 4.0(4o) |

| Adapters | Minimum Software Version<br>UCS 6200 Series FI | Minimum Software Version<br>UCS 6332, 6332-16UP | Minimum Software Version<br>UCS 6332, 6332-16UP | Minimum Software Version<br>UCS 6454 | Suggested Software Version<br>UCS 6200 Series FI<br>UCS 6332, 6332-16UP FI<br>UCS 6454 |
|---|---|---|---|---|---|
| | UCS-IOM-2204<br>UCS-IOM-2208 | UCS-IOM-2204<br>UCS-IOM-2208 | UCS-IOM-2304<br>UCS-IOM-2304V2 | UCS-IOM-2204<br>UCS-IOM-2208 | UCS-IOM-2204<br>UCS-IOM-2208<br>UCS-IOM-2408* |
| | | | | * UCS-IOM-2408 supported on M4 and M5 only with UCS 6454 FI | |
| UCSC-MLOM-C10T-02 (UCS VIC 1227T)<br>UCSC-PCIE-C10T-02 (UCS VIC 1225T)<br>UCSC-F-FIO-785M (Cisco UCS 785GB MLC Fusion ioDrive2 for C-Series Servers)<br>UCSC-F-FIO-365M (Cisco UCS 365GB MLC Fusion ioDrive2 for C-Series Servers)<br>UCSC-F-FIO-1205M (Cisco UCS 1205GB MLC Fusion ioDrive2 for C-Series Servers)<br>UCSC-F-FIO-3000M (Cisco UCS 3.0TB MLC Fusion ioDrive2 for C-Series Servers)<br>UCSC-F-FIO-1000PS | | | | | |

| Adapters | Minimum Software Version<br>UCS 6200 Series FI | Minimum Software Version<br>UCS 6332, 6332-16UP | Minimum Software Version<br>UCS 6332, 6332-16UP | Minimum Software Version<br>UCS 6454 | Suggested Software Version<br>UCS 6200 Series FI<br>UCS 6332, 6332-16UP FI<br>UCS 6454 |
|---|---|---|---|---|---|
| | UCS-IOM-2204<br>UCS-IOM-2208 | UCS-IOM-2204<br>UCS-IOM-2208 | UCS-IOM-2304<br>UCS-IOM-2304V2 | UCS-IOM-2204<br>UCS-IOM-2208 | UCS-IOM-2204<br>UCS-IOM-2208<br>UCS-IOM-2408* |
| | | | | * UCS-IOM-2408 supported on M4 and M5 only with UCS 6454 FI | |
| (UCS 1000GB Fusion ioMemory3 PX Performance line for Rack M4)<br>UCSC-F-FIO-1300PS (UCSC-F-FIO-1300PS)<br>UCSC-F-FIO-2600PS (UCS 2600GB Fusion ioMemory3 PX Performance line for Rack M4)<br>UCSC-F-FIO-5200PS (UCS 5200GB Fusion ioMemory3 PX Performance line for Rack M4)<br>UCSC-F-FIO-6400SS (UCS 6400GB Fusion ioMemory3 SX Scale line for C-Series) | | | | | |

| Adapters | Minimum Software Version<br>UCS 6200 Series FI | Minimum Software Version<br>UCS 6332, 6332-16UP | Minimum Software Version<br>UCS 6332, 6332-16UP | Minimum Software Version<br>UCS 6454 | Suggested Software Version<br>UCS 6200 Series FI<br>UCS 6332, 6332-16UP FI<br>UCS 6454 |
|---|---|---|---|---|---|
| | UCS-IOM-2204<br>UCS-IOM-2208 | UCS-IOM-2204<br>UCS-IOM-2208 | UCS-IOM-2304<br>UCS-IOM-2304V2 | UCS-IOM-2204<br>UCS-IOM-2208 | UCS-IOM-2204<br>UCS-IOM-2208<br>UCS-IOM-2408* |
| | | | | * UCS-IOM-2408 supported on M4 and M5 only with UCS 6454 FI | |
| UCSC-F-FIO-3200SS (UCS 3200GB Fusion ioMemory3SX Scale line for C-Series) | | | | | |
| UCSC-PCIE-E14102B (Emulex OCe14102B-F) | 2.2(8a) | 3.1(3a) | 3.1(3a) | 4.0(1a) | 4.0(4o) |
| UCSC-PCIE-IQ10GF (Intel X710-DA4 adapter)<br>UCSC-PCIE-ID10GF (Intel X710-DA2 adapter)<br>UCSC-PCIE-ID40GF (Intel XL710 adapter) | — | — | 3.1(3a) | 4.0(1a) | 4.0(4o) |

| Adapters | Minimum Software Version<br>UCS 6200 Series FI | Minimum Software Version<br>UCS 6332, 6332-16UP | Minimum Software Version<br>UCS 6332, 6332-16UP | Minimum Software Version<br>UCS 6454 | Suggested Software Version<br>UCS 6200 Series FI<br>UCS 6332, 6332-16UP FI<br>UCS 6454 |
|---|---|---|---|---|---|
| | UCS-IOM-2204<br>UCS-IOM-2208 | UCS-IOM-2204<br>UCS-IOM-2208 | UCS-IOM-2304<br>UCS-IOM-2304V2 | UCS-IOM-2204<br>UCS-IOM-2208 | UCS-IOM-2204<br>UCS-IOM-2208<br>UCS-IOM-2408* |
| | | | | * UCS-IOM-2408 supported on M4 and M5 only with UCS 6454 FI | |
| | — | 3.1(3a) | 3.1(3a) | 4.0(1a) | 4.0(4o) |

| Adapters | Minimum Software Version<br>UCS 6200 Series FI | Minimum Software Version<br>UCS 6332, 6332-16UP | Minimum Software Version<br>UCS 6332, 6332-16UP | Minimum Software Version<br>UCS 6454 | Suggested Software Version<br>UCS 6200 Series FI<br>UCS 6332, 6332-16UP FI<br>UCS 6454 |
|---|---|---|---|---|---|
| | UCS-IOM-2204<br>UCS-IOM-2208 | UCS-IOM-2204<br>UCS-IOM-2208 | UCS-IOM-2304<br>UCS-IOM-2304V2 | UCS-IOM-2204<br>UCS-IOM-2208 | UCS-IOM-2204<br>UCS-IOM-2208<br>UCS-IOM-2408* |
| | | | | * UCS-IOM-2408 supported on M4 and M5 only with UCS 6454 FI | |
| UCSC-F-I80010 (Intel P3700 HHHL 800GB NVMe PCIe SSD)<br>UCSC-F-I12003 (Intel P3600 HHHL 1200GB NVMe PCIe SSD)<br>UCSC-F-I160010 (Intel P3700 HHHL 1600GB NVMe PCIe SSD)<br>UCSC-F-I20003 (Intel P3600 HHHL 2000GB NVMe PCIe SSD )<br>UCS-PCI25-40010 (Intel P3700 400GB NVMe PCIe SSD)<br>UCS-PCI25-8003 (Intel P3600 800GB NVMe PCIe SSD)<br>UCS-PCI25-80010 (Intel P3700 800GB NVMe PCIe SSD) | | | | | |

| Adapters | Minimum Software Version<br>UCS 6200 Series FI | Minimum Software Version<br>UCS 6332, 6332-16UP | Minimum Software Version<br>UCS 6332, 6332-16UP | Minimum Software Version<br>UCS 6454 | Suggested Software Version<br>UCS 6200 Series FI<br>UCS 6332, 6332-16UP FI<br>UCS 6454 |
|---|---|---|---|---|---|
| | UCS-IOM-2204<br>UCS-IOM-2208 | UCS-IOM-2204<br>UCS-IOM-2208 | UCS-IOM-2304<br>UCS-IOM-2304V2 | UCS-IOM-2204<br>UCS-IOM-2208 | UCS-IOM-2204<br>UCS-IOM-2208<br>UCS-IOM-2408* |
| | | | | * UCS-IOM-2408 supported on M4 and M5 only with UCS 6454 FI | |
| UCS-PCI25-16003 (Intel P3600 1600GB NVMe PCIe SSD)<br>UCSC-F-H19001 (UCS Rack PCIe/NVMe Storage 1900GB HGST SN150)<br>UCSC-F-H38001 (UCS Rack PCIe/NVMe Storage 3800GB HGST SN150)<br>UCS-PCI25-38001 (UCS PCIe/NVMe2.5"SFF Storage 3800GB HGST SN100) | | | | | |

| **Adapters** | **Minimum Software Version**<br>**UCS 6200 Series FI** | **Minimum Software Version**<br>**UCS 6332, 6332-16UP** | **Minimum Software Version**<br>**UCS 6332, 6332-16UP** | **Minimum Software Version**<br>**UCS 6454** | **Suggested Software Version**<br>**UCS 6200 Series FI**<br>**UCS 6332, 6332-16UP FI**<br>**UCS 6454** |
|---|---|---|---|---|---|
| | **UCS-IOM-2204**<br>**UCS-IOM-2208** | **UCS-IOM-2204**<br>**UCS-IOM-2208** | **UCS-IOM-2304**<br>**UCS-IOM-2304V2** | **UCS-IOM-2204**<br>**UCS-IOM-2208** | **UCS-IOM-2204**<br>**UCS-IOM-2208**<br>**UCS-IOM-2408*** |
| | | | | *** UCS-IOM-2408 supported on M4 and M5 only with UCS 6454 FI** | |
| UCSC-PCIE-QD32GF (Qlogic QLE2742)<br>N2XX-AQPCI05 (Qlogic QLE2562)<br>UCSC-PCIE-Q2672 (Qlogic QLE2672-CSC)<br>UCSC-PCIE-BD32GF (Emulex LPe32002)<br>UCSC-PCIE-BS32GF (Emulex LPe32001)<br>N2XX-AEPCI05 (Emulex LPe12002) | — | 3.1(3a) | 3.1(3a) | 4.0(1a) | 4.0(4o) |
| UCSC-PCIE-E16002 (Emulex LPe16002-M6 16G FC rack HBA) | — | 3.2(1d) | 3.2(1d) | 4.0(1a) | 4.0(4o) |
| UCSC-PCIE-ID10GC (Intel X550 Dual-port 10GBase-T NIC) | 3.1(2b) | 3.1(3a) | 3.1(3a) | 4.0(1a) | 4.0(4o) |

### 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 27. The following is the list of other supported hardware:

*Table 15: Supported Hardware for UCS 6454 Fabric Interconnects*

| Type | Details |
|---|---|
| **Chassis** | UCSC-C4200-SFF<br>N20–C6508<br>UCSB-5108-DC<br>UCSB-5108-AC2<br>UCSB-5108-DC2<br>UCSB-5108-HVDC |
| **Fabric Interconnects** | UCS 6454 |
| **Fabric Extenders** | Cisco UCS 2204XP<br>Cisco UCS 2208XP<br>Cisco Nexus 2232PP<br>Cisco Nexus 2232TM-E<br>Cisco UCS 2408 |
| **Power Supplies** | UCS-PSU-6332-AC<br>UCS-PSU-6332-DC<br>UCS-PSU-64108-AC<br>UCS-PSU-6332-D |

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

| Type | Details |
|---|---|
| **Chassis** | N20–C6508<br>UCSB-5108-DC<br>UCSB-5108-AC2<br>UCSB-5108-DC2<br>UCSB-5108-HVDC |
| **Fabric Interconnects** | UCS 6332UP<br>UCS 6332-16UP |

| Type | Details |
|---|---|
| **Fabric Extenders** | Cisco UCS 2208XP<br>Cisco UCS 2204XP<br>Cisco Nexus 2232PP<br>Cisco Nexus 2232TM-E<br>Cisco UCS 2304<br>Cisco UCS 2304V2<br>Cisco Nexus 2348UPQ |
| **Power Supplies** | UCS-PSU-6332-AC<br>UCS-PSU-6332-DC |

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

*Table 17: Supported Hardware for UCS 6200 Fabric Interconnects*

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

### GB Connector Modules, Transceiver Modules, and Cables

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

**Note**

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

*Table 18: Supported Transceiver Modules and Cables for GB Connector Modules*

| Gb Connector Modules | Transceiver Modules and Cables |
|---|---|
| **FC for UCS 6454 Fabric Interconnects** | DS-SFP-FC8G-SW<br>DS-SFP-FC8G-LW<br>DS-SFP-FC16G-SW<br>DS-SFP-FC16G-LW<br>DS-SFP-FC32G-SW<br>DS-SFP-FC32G-LW |
| **100-Gb for UCS 6454 Fabric Interconnects** | QSFP-40/100G-SRBD<br>QSFP-100G-SR4-S<br>QSFP-100G-LR4-S<br>QSFP-100G-SM-SR<br>QSFP-100G-CU1M<br>QSFP-100G-CU2M<br>QSFP-100G-CU3M<br>QSFP-100G-AOC1M<br>QSFP-100G-AOC2M<br>QSFP-100G-AOC3M<br>QSFP-100G-AOC5M<br>QSFP-100G-AOC7M<br>QSFP-100G-AOC10M<br>QSFP-100G-AOC15M<br>QSFP-100G-AOC20M<br>QSFP-100G-AOC25M<br>QSFP-100G-AOC30M |

| Gb Connector Modules | Transceiver Modules and Cables |
|---|---|
| **40-Gb for UCS 6454 Fabric Interconnects** | QSFP-40G-SR4<br>QSFP-40G-SR4-S<br>QSFP-40G-SR-BD<br>QSFP-40G-LR4<br>QSFP-40G-LR4-S<br>QSFP-40G-ER4<br>WSP-Q40GLR4L<br>QSFP-H40G-CU1M<br>QSFP-H40G-CU3M<br>QSFP-H40G-CU5M<br>QSFP-H40G-ACU7M<br>QSFP-H40G-ACU10M<br>QSFP-H40G-AOC1M<br>QSFP-H40G-AOC2M<br>QSFP-H40G-AOC3M<br>QSFP-H40G-AOC5M<br>QSFP-H40G-AOC10M<br>QSFP-H40G-AOC15M |

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

| Gb Connector Modules | Transceiver Modules and Cables |
|---|---|
| **32-Gb FC for UCS 6454 Fabric Interconnects** | DS-SFP-FC32G-SW<br>DS-SFP-FC32G-LW |
| **25-Gb for UCS 6454 Fabric Interconnects** | SFP-25G-SR-S<br>SFP-H25G-CU1M<br>SFP-H25G-CU2M<br>SFP-H25G-CU3M<br>SFP-H25G-CU5M<br>SFP-H25G-AOC1M<br>SFP-H25G-AOC2M<br>SFP-H25G-AOC3M<br>SFP-H25G-AOC5M<br>SFP-H25G-AOC7M<br>SFP-H25G-AOC10M |
| **16-Gb for UCS 6454 and UCS 6332UP Fabric Interconnects** | DS-SFP-FC16G-LW<br>DS-SFP-FC16G-SW |

| Gb Connector Modules | Transceiver Modules and Cables |
|---|---|
| **10-Gb for UCS 6454 Fabric Interconnects** | SFP-10G-SR<br>SFP-10G-SR-S<br>SFP-10G-LR<br>SFP-10G-LR-S<br>SFP-10G-ER<br>SFP-10G-ER-S<br>SFP-10G-ZR<br>SFP-10G-ZR-S<br>FET-10G<br>**Note** FET-10G is only supported between Fabric Interconnects and IOMs/FEXs.<br>SFP-10G-LRM<br>SFP-H10GB-CU1M<br>SFP-H10GB-CU2M<br>SFP-H10GB-CU3M<br>SFP-H10GB-CU5M<br>SFP-H10GB-ACU7M<br>SFP-H10GB-ACU10M<br>SFP-10G-AOC1M<br>SFP-10G-AOC2M<br>SFP-10G-AOC3M<br>SFP-10G-AOC5M<br>SFP-10G-AOC7M<br>SFP-10G-AOC10M |

| Gb Connector Modules | Transceiver Modules and Cables |
|---|---|
| **10-Gb for UCS 6300 and 6200 Series Fabric Interconnects** | SFP-10G-SR<br>SFP-10G-SR-S<br>SFP-10G-LR<br>SFP-10G-LR-S<br>SFP-H10GB-CU1M<br>SFP-H10GB-CU2M<br>SFP-H10GB-CU3M<br>SFP-H10GB-CU5M<br>SFP-H10GB-ACU7M<br>SFP-H10GB-ACU10M<br>FET-10G<br>[1]SFP-10G-AOC1M<br>SFP-10G-AOC2M<br>SFP-10G-AOC3M<br>SFP-10G-AOC5M<br>SFP-10G-AOC7M<br>SFP-10G-AOC10M |
| **8-Gb FC for UCS 6454 and UCS 6332UP Fabric Interconnects** | DS-SFP-FC8G-SW<br>DS-SFP-FC8G-LW |
| **4-Gb FC for UCS 6300 and 6200 Series Fabric Interconnects** | DS-SFP-FC4G-SW<br>DS-SFP-FC4G-LW |
| **1-Gb for UCS 6454 Fabric Interconnects** | GLC-TE<br>GLC-SX-MMD<br>SFP-GE-T |
| **1-Gb for UCS 6300 and 6200 Series Fabric Interconnects** | GLC-TE<br>GLC-SX-MM<br>GLC-LH-SM |

[1] SFP-10G-AOC cables are only supported for Cisco 1455 and 1457 VIC cards.

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

## Cisco UCS Mini and Components

### UCS Mini Supported Chassis

*Table 19: Minimum Software Versions for UCS Mini Chassis*

| Chassis | Minimum Software Version | Suggested Software Version |
|---|---|---|
| UCSB-5108-AC2 | 3.0(1e) | 4.0(4o) |
| UCSB-5108-DC2 | 3.0(2c) | 4.0(4o) |

### UCS Mini Supported Blade and Rack Servers

*Table 20: Minimum Host Firmware Versions for Blade and Rack Servers on UCS Mini*

| Servers | Minimum Software Version | Suggested Software Version |
|---|---|---|
| B200 M5 | 3.2(1d) | 4.0(4o) |
| B200 M3 | 3.1(3a) | 4.0(4o) |
| B200 M4 | 3.1(3a) | 4.0(4o) |
| B260 M4 | 3.1(3a) | 4.0(4o) |
| B420 M3 | 3.1(3a) | 4.0(4o) |
| B420 M4 | 3.1(3a) | 4.0(4o) |
| B460 M4 | 3.1(3a) | 4.0(4o) |
| B480 M5 | 3.1(3a) | 4.0(4o) |
| B22 M3 | 3.1(3a) | 4.0(4o) |
| C220 M3 | 3.1(3a) | 4.0(4o) |
| C240 M3 | 3.1(3a) | 4.0(4o) |
| C220 M4 | 3.1(3a) | 4.0(4o) |
| C240 M4 | 3.1(3a) | 4.0(4o) |
| C460 M4 | 3.1(3a) | 4.0(4o) |
| C220 M5 | 3.2(1d) | 4.0(4o) |

| Servers | Minimum Software Version | Suggested Software Version |
|---|---|---|
| C240 M5 | 3.2(1d) | 4.0(4o) |
| C480 M5 | 3.2(2b) | 4.0(4o) |

### UCS Mini Supported Adapters

| Adapters | Minimum Software Version | Suggested Software Version |
|---|---|---|
| UCSB-MLOM-40G-04 (UCS VIC 1440)<br>UCSB-VIC-M84-4P (UCS VIC 1480) | 4.0(2a) | 4.0(4o) |
| UCSC-PCIE-IQ10GC (Intel X710-T4)<br>UCSC-PCIE-QD25GF (QLogic QL41212H 25GbE)<br>UCSC-PCIE-QD40GF (QLogic QL45212H 40GbE) | 3.2(2b) | 4.0(4o) |
| UCSC-PCIE-C40Q-03 (UCS VIC 1385)<br>UCSC-MLOM-C40Q-03 (UCS VIC 1387) | 3.1(3a) | 4.0(4o) |
| UCS-VIC-M82-8P (UCS VIC 1280)<br>UCSB-MLOM-40G-01 (UCS VIC 1240)<br>UCSB-MLOM-PT-01 (Cisco Port Expander Card) | 3.1(3a) | 4.0(4o) |
| UCSB-MLOM-40G-03 (UCS VIC 1340)<br>UCSB-VIC-M83-8P (UCS VIC 1380)<br>UCSC-MLOM-CSC-02 (UCS VIC 1227) | 3.1(3a) | 4.0(4o) |
| UCSC-PCIE-CSC-02 (UCS VIC 1225) | 3.1(3a) | 4.0(4o) |

### UCS Mini Supported Fabric Interconnects

| Fabric Interconnects | Minimum Software Version | Suggested Software Version |
|---|---|---|
| Cisco UCS 6324 | 3.1(3a) | 4.0(4o) |

### UCS Mini Supported Fabric Extenders for Secondary Chassis

| Fabric Extenders | Minimum Software Version | Suggested Software Version |
|---|---|---|
| UCS 2204 XP | 3.1(3a) | 4.0(4o) |
| UCS 2208 XP | 3.1(3a) | 4.0(4o) |

### UCS Mini Supported Power Supplies

| Power Supplies | Minimum Software Version | Suggested Software Version |
|---|---|---|
| UCSB-PSU-2500ACDV<br>UCSB-PSU-2500DC48<br>UCSC-PSU-930WDC<br>UCSC-PSU2V2-930WDC<br>UCSC-PSUV2-1050DC<br>UCSC-PSU1-770W<br>UCSC-PSU2-1400<br>UCSC-PSU2V2-1400W<br>UCSC-PSU2V2-650W<br>UCSC-PSU2V2-1200W | 3.1(3a) | 4.0(4o) |

### UCS Mini Supported Gb Connector Modules

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

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

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

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

## UCS Manager Health and Pre-Upgrade Check Tool

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

## Upgrade and Downgrade Guidelines

- In a system with Cisco UCS 6454 Fabric Interconnects, you cannot downgrade from Cisco UCS Manager Release 4.0.

  See the *Cisco UCS Manager Firmware Management Guide*, Release 4.0 section Firmware Upgrade to Cisco UCS Manager Release 4.0 for detailed upgrade paths.

- Do not downgrade systems equipped with LITE-ON 1050W PSUs to a Cisco UCS Manager release earlier than Release 4.0(2). Board controller activation for UCS C240 M5 servers with LITE-ON 1050W PSU may fail during the discovery process when it is downgraded from Cisco UCS Manager Release 4.0(2).

- In a system with Cisco UCS 6454 Fabric Interconnects, you cannot downgrade from Cisco UCS Manager Release 4.0(2) when Ethernet or FC switch mode is enabled on the Fabric Interconnect because this mode is not supported in versions earlier than 4.0(2).

  Also, if port-security is enabled in the network control policy, it is disabled during downgrade from Cisco UCS Manager Release 4.0(2) because it is not supported in versions earlier than 4.0(2).

- When upgrading or downgrading systems using Intel Volume Management Device (VMD) for NVMe, the system will fail to boot if VMD is enabled or disabled in the BIOS after OS installation. Do not change the BIOS setting after OS installation.

- When upgrading Fabric Interconnects or servers (B-Series and C-Series) from Cisco UCS Manager Release 4.0(4c) to 4.0(4d), the FSM skips validation, and firmware upgrades complete without reboot.

### Downgrade Limitation for Cisco UCS C125 M5 Servers

Starting with Release 4.0(4k), AMD Platform Secure Boot (PSB) is introduced in Cisco UCS C125 M5 servers that implements hardware-rooted boot integrity. Once you upgrade, you cannot downgrade Cisco UCS C125 M5 Rack Server Node based on AMD EPYC 7001 (Naples) to any release earlier than 4.0(4k).

# 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 21: Version Mapping*

| UCS Release | Catalog File Name | Additional PIDs In This Release |
|---|---|---|
| 4.0(4o) | ucs-catalog.4.0.4q.T.bin | — |
| 4.0(4n) | ucs-catalog.4.0.4o.T.bin | — |
| 4.0(4m) | ucs-catalog.4.0.4f.T.bin | — |
| 4.0(4l) | ucs-catalog.4.0.4f.T.bin | — |
| 4.0(4k) | ucs-catalog.4.0.4k.T.bin | Micro-SD Card:<br>• UCS-S-MSD960K9 |
| 4.0(4i) | ucs-catalog.4.0.4i.T.bin | Drives for C220 M5 and C240 M5 servers:<br>• UCS-HD14TT7KL4KN<br>• UCS-HD16T7KL4KN<br>Drives for S3260 M5 server:<br>• UCS-S3260-HDT14T<br>• UCS-S3260-HDT14TR<br>• UCS-S3260-HD16T<br>• UCS-S3260-HD16TR |

| UCS Release | Catalog File Name | Additional PIDs In This Release |
|---|---|---|
| 4.0(4h) | ucs-catalog.4.0.4h.T.bin | CPUs for UCS B200 M5, C220 M5, and C240 M5 servers:<br>• UCS-CPU-I6238R<br>• UCS-CPU-I6240R<br>• UCS-CPU-I6242R<br>• UCS-CPU-I6246R<br>• UCS-CPU-I6248R<br>• UCS-CPU-I6226R<br>• UCS-CPU-I6258R<br>• UCS-CPU-I5220R<br>CPUs for UCS B200 M5, C220 M5, C240 M5, and UCS S3260 M5 servers:<br>• UCS-CPU-I6230R<br>• UCS-CPU-I5218R<br>• UCS-CPU-I4214R<br>• UCS-CPU-I4215R<br>CPUs for UCS B200 M5, UCS B480 M5, C220 M5, C240 M5, and C480 M5 servers:<br>• UCS-CPU-I8253 |
| 4.0(4g) | ucs-catalog.4.0.4g.T.bin | CPUs for UCS B200 M5, C220 M5, and C240 M5 servers:<br>• UCS-CPU-I4214R<br>• UCS-CPU-I4210R<br>• UCS-CPU-I3206R |
| 4.0(4f) | ucs-catalog.4.0.4f.T.bin | — |

| UCS Release | Catalog File Name | Additional PIDs In This Release |
|---|---|---|
| 4.0(4e) | ucs-catalog.4.0.4e.T.bin | CPUs for UCS B200 M5, B480 M5, C220 M5, C240 M5, and C480 M5 servers:<br>• UCS-CPU-I6238<br>• UCS-CPU-I6238M<br>• UCS-CPU-I6238L<br>• UCS-CPU-I5220S<br>• UCS-CPU-I6226<br>• UCS-CPU-I6234<br>• UCS-CPU-I6240L<br>• UCS-CPU-I6240M<br>• UCS-CPU-I6246<br>• UCS-CPU-I5218B<br>CPUs for UCS C220 M5, C240 M5, B200 M5, B480 M5, C480 M5, and S3260-M5 servers:<br>• UCS-CPU-I6222V<br>• UCS-CPU-I6262V<br>CPUs for UCS C220 M5, C240 M5, and B200 M5 servers:<br>• UCS-CPU-I5218N<br>CPUs for UCS C220 M5, C240 M5, B480 M5, and B200 M5 servers:<br>• UCS-CPU-I6230N<br>CPUs for UCS C220 M5, C240 M5, C480 M5, and B200 M5 servers:<br>• UCS-CPU-I6252N<br>Drives:<br>• UCS-SD76TSB61X-EV<br>• UCS-SD76T61X-EV<br>**Fabric Extender**:<br>• UCS-IOM-2408 |

| UCS Release | Catalog File Name | Additional PIDs In This Release |
|---|---|---|
| 4.0(4d) | ucs-catalog.4.0.4d.T.bin | Drives:<br>• UCS-SD480G2HNK9<br>• UCS-SD480G2HBNK9<br>• UCS-SD960G2HTNK9<br>• UCS-SD960G2HBNK9<br>• UCS-SD38T2HTNK9<br>• UCS-SD38T2HBNK9<br>• UCS-S3260-2SD38K9 |
| 4.0(4c) | ucs-catalog.4.0.4c.T.bin | • UCSC-NVME2H-I1000<br>• UCSB-NVME2H-I1000<br>• UCSC-NVME2H-I2TBV<br>• UCSB-NVME2H-I2TBV<br>• UCSC-NVME2H-I4000<br>• UCSB-NVME2H-I4000<br>• UCSC-NVMEHW-I8000<br>• UCSB-NVMEHW-I8000<br>• UCSC-NVME2H-I1600<br>• UCSB-NVME2H-I1600 |
| 4.0(4b) | ucs-catalog.4.0.4b.T.bin | — |

| UCS Release | Catalog File Name | Additional PIDs In This Release |
|---|---|---|
| 4.0(4a) | ucs-catalog.4.0.4a.T.bin | |

| UCS Release | Catalog File Name | Additional PIDs In This Release |
|---|---|---|
| | | CPUs for UCS B200 M5, C220 M5, C240 M5 servers:<br>• UCS-CPU-I3204<br>• UCS-CPU-I4208<br>• UCS-CPU-I4210<br>• UCS-CPU-I4214<br>• UCS-CPU-I4215<br>• UCS-CPU-I4216<br>• UCS-CPU-I5215<br>• UCS-CPU-I5217<br>• UCS-CPU-I5218<br>• UCS-CPU-I5220<br>• UCS-CPU-I5222<br>• UCS-CPU-I6230<br>• UCS-CPU-I6240<br>• UCS-CPU-I6242<br>• UCS-CPU-I6244<br>• UCS-CPU-I6248<br>• UCS-CPU-I6254<br>• UCS-CPU-I6252<br>• UCS-CPU-I8260<br>• UCS-CPU-I8268<br>• UCS-CPU-I8270<br>• UCS-CPU-I8276<br>• UCS-CPU-I8280<br>• UCS-CPU-I5215M<br>• UCS-CPU-I8260M<br>• UCS-CPU-I8276M<br>• UCS-CPU-I8280M<br>• UCS-CPU-I5215L<br>• UCS-CPU-I8260L |

| UCS Release | Catalog File Name | Additional PIDs In This Release |
|---|---|---|
| | | • UCS-CPU-I8276L<br>• UCS-CPU-I8280L<br>• UCS-CPU-I4214Y<br>• UCS-CPU-I6240Y<br>• UCS-CPU-I8260Y<br>CPUs for UCS B480 M5 and C480 M5: |

| UCS Release | Catalog File Name | Additional PIDs In This Release |
|---|---|---|
| | | • UCS-CPU-I5215<br>• UCS-CPU-I5217<br>• UCS-CPU-I5218<br>• UCS-CPU-I5220<br>• UCS-CPU-I5222<br>• UCS-CPU-I6230<br>• UCS-CPU-I6240<br>• UCS-CPU-I6242<br>• UCS-CPU-I6244<br>• UCS-CPU-I6248<br>• UCS-CPU-I6254<br>• UCS-CPU-I6252<br>• UCS-CPU-I8260<br>• UCS-CPU-I8268<br>• UCS-CPU-I8270<br>• UCS-CPU-I8276<br>• UCS-CPU-I8280<br>• UCS-CPU-I5215M<br>• UCS-CPU-I8260M<br>• UCS-CPU-I8276M<br>• UCS-CPU-I8280M<br>• UCS-CPU-I5215L<br>• UCS-CPU-I8260L<br>• UCS-CPU-I8276L<br>• UCS-CPU-I8280L<br>• UCS-CPU-I6240Y<br>• UCS-CPU-I8260Y<br>CPUs for UCS S3260 M5: |

| UCS Release | Catalog File Name | Additional PIDs In This Release |
|---|---|---|
| | | • UCS-CPU-I4214<br>• UCS-CPU-I5218<br>• UCS-CPU-I5220<br>• UCS-CPU-I6240<br>Memory:<br>• UCS-MR-X16G1RT-H<br>• UCS-MR-X32G2RT-H<br>• UCS-MR-X64G2RT-H<br>• UCS-ML-X64G4RT-H<br>• UCS-ML-128G4RT-H<br>Intel® Optane™ DC persistent memory:<br>• UCS-MP-128GS-A0<br>• UCS-MP-256GS-A0<br>• UCS-MP-512GS-A0<br>Fabric Extender:<br>• UCS-IOM-2304V2<br>GPUs:<br>• UCSC-GPU-T4-16 on UCS C240 M5, C220 M5, C480 M5<br>• UCSC-GPU-V340<br>Network Interface Cards:<br>• UCSC-P-M4D25GF<br>• UCSC-PCIE-QS100GF<br>Hardware RAID Controller:<br>• UCS-M2-HWRAID |
| 4.0(2e) | ucs-catalog.4.0.2e.T.bin | — |
| 4.0(2d) | ucs-catalog.4.0.2d.T.bin | — |
| 4.0(2b) | ucs-catalog.4.0.2a.T.bin | — |

| UCS Release | Catalog File Name | Additional PIDs In This Release |
|---|---|---|
| 4.0(2a) | ucs-catalog.4.0.2a.T.bin | |

| UCS Release | Catalog File Name | Additional PIDs In This Release |
|---|---|---|
| | | Cisco UCS Rack-Mount Servers:<br>• UCSC-C480-M5ML<br>CPUs for UCSC-C480-M5ML:<br>• UCS-CPU-8180<br>• UCS-CPU-8176<br>• UCS-CPU-8170<br>• UCS-CPU-8164<br>• UCS-CPU-8160<br>• UCS-CPU-8153<br>• UCS-CPU-6152<br>• UCS-CPU-6148<br>• UCS-CPU-6138<br>• UCS-CPU-6140<br>• UCS-CPU-6130<br>• UCS-CPU-8168<br>• UCS-CPU-8158<br>• UCS-CPU-8156<br>• UCS-CPU-6154<br>• UCS-CPU-6150<br>• UCS-CPU-6142<br>• UCS-CPU-6132<br>• UCS-CPU-6144<br>• UCS-CPU-6136<br>• UCS-CPU-6126<br>• UCS-CPU-6146<br>• UCS-CPU-6134<br>• UCS-CPU-6128<br>• UCS-CPU-5122<br>• UCS-CPU-4116<br>• UCS-CPU-6142M<br>• UCS-CPU-8180M |

| UCS Release | Catalog File Name | Additional PIDs In This Release |
|---|---|---|
| | | Memory for UCSC-C480-M5ML:<br>• UCS-MR-128G8RS-H<br>• UCS-MR-X64G4RS-H<br>• UCS-ML-X64G4RS-H<br>• UCS-MR-X32G2RS-H<br>• UCS-ML-X32G2RS-H<br>• UCS-MR-X16G1RS-H<br>• UCS-MR-X16G2RS-H<br>PSU for UCSC-C480-M5ML:<br>• UCSC-PSU1-1600W<br>Fan module for UCSC-C480-M5ML:<br>• UCSC-FAN-C480M5<br>Cisco VICs for UCSC-C480-M5ML:<br>• VIC 1455 10/25G PCIe for C-Series and S-Series (UCSC-PCIE-C25Q-04)<br>• VIC 1495 40/100G PCIe for C-Series (UCSC-PCIE-C100-04)<br>NIC for UCSC-C480-M5ML:<br>• Qlogic QLE45611HLCU single port 100G NIC (UCSC-PCIE-QS100GF)<br>HDDs for UCSC-C480-M5ML:<br>• UCS-HD900G15K12N<br>• UCS-HD12TB10K12N<br>• UCS-HD18TB10K4KN<br>• UCS-HD2T7K12N<br>SSDs for UCSC-C480-M5ML: |

| UCS Release | Catalog File Name | Additional PIDs In This Release |
|---|---|---|
| | | • UCS-SD16T123X-EP<br>• UCS-SD32T123X-EP<br>• UCS-SD120GM1X-EV<br>• UCS-SD240GM1X-EV<br>• UCS-SD480GM1X-EV<br>• UCS-SD960GM1X-EV<br>• UCS-SD16TM1X-EV<br>• UCS-SD19TM1X-EV<br>• UCS-SD38TM1X-EV<br>• UCS-SD76TM1X-EV<br>Flash drive for UCSC-C480-M5ML:<br>• UCS-USBFLSHB-16GB<br>GPU for UCSC-C480-M5ML:<br>• NVIDIA SXM2 V100 32GB Nvlink Modules (UCSC-GPUV100SXM32)<br>NVMe drives for UCSC-C480-M5ML:<br>• UCSC-NVMEHW-H3200<br>Mini Storage Carriers for UCSC-C480-M5ML:<br>• UCS-MSTOR-SD<br>• UCS-MSTOR-M2<br>SD Cards for UCSC-C480-M5ML:<br>• UCS-SD-64G-S<br>• UCS-SD-128G<br>Micro SD Card for UCSC-C480-M5ML:<br>• UCS-MSD-32G<br>M.2 SATA SSD for UCSC-C480-M5ML:<br>• UCS-M2-240GB<br>• UCS-M2-960GB<br>RAID Controller for UCSC-C480-M5ML:<br>• UCSC-RAID-M5HD |

| UCS Release | Catalog File Name | Additional PIDs In This Release |
|---|---|---|
| | | Cisco VIC Adapters:<br>• VIC 1495 40/100G PCIe for C-Series (UCSC-PCIE-C100-04)<br>• VIC 1497 40/100G mLOM for C-Series (UCSC-MLOM-C100-04)<br>TPM2 for all UCS servers:<br>• UCSX-TPM2-002-C<br>High Voltage DC 1200 Watt Power Supply on UCS 6454 Fabric Interconnects:<br>• N9K-PUV-1200W<br>Intel Optane NVMe Extreme Performance Drive for M5 servers:<br>• UCSC-NVMEXP-I750<br>GPU for C240 M5 servers:<br>• UCSC-GPU-V100-32G—NVIDIA V100 PCIe PG500-200 250W 32GB GPU<br>QLogic Network Adapter cards for UCSC-C125:<br>• UCSC-PCIE-QD10GC—10G Network Adapter card<br>• UCSC-PCIE-QD25GF—25G Network Adapter card |
| 4.0(1d) | ucs-catalog.4.0.1c.T.bin | Drives:<br>• UCS-SD480GBHBNK9<br>• UCS-SD960GBHBNK9<br>• UCS-SD38TBHBNK9<br>• UCS-SD480GBHTNK9<br>• UCS-SD960GBHTNK9<br>• UCS-SD38TBHTNK9 |
| 4.0(1c) | ucs-catalog.4.0.1a.T.bin | — |
| 4.0(1b) | ucs-catalog.4.0.1a.T.bin | — |

| UCS Release | Catalog File Name | Additional PIDs In This Release |
|---|---|---|
| 4.0(1a) | ucs-catalog.4.0.1a.T.bin | |

| UCS Release | Catalog File Name | Additional PIDs In This Release |
|---|---|---|
| | | Cisco UCS 6454 Fabric Interconnect:<br>• UCS-FI-6454<br>Cisco UCS Rack-Mount Servers:<br>• UCSC-C125<br>Chassis for C125 M5:<br>• UCSC-C4200-SFF<br>CPUs for UCSC-C125:<br>• UCS-CPU-7601<br>• UCS-CPU-7551<br>• UCS-CPU-7501<br>• UCS-CPU-7451<br>• UCS-CPU-7401<br>• UCS-CPU-7351<br>• UCS-CPU-7301<br>• UCS-CPU-7281<br>• UCS-CPU-7261<br>• UCS-CPU-7251<br>• UCS-CPU-7551P<br>• UCS-CPU-7401P<br>• UCS-CPU-7351P<br>Memory for UCSC-C125:<br>• UCS-MR-128G8RS-H<br>• UCS-MR-X64G4RS-H<br>• UCS-ML-X64G4RS-H<br>• UCS-MR-X32G2RS-H<br>• UCS-MR-X16G1RS-H<br>• UCS-MR-X16G2RS-H<br>• UCS-MR-X8G1RS-H<br>OCP NICs for UCSC-C125:<br>• UCSC-OCP-QD10GC |

| UCS Release | Catalog File Name | Additional PIDs In This Release |
|---|---|---|
| | | • UCSC-OCP-QD25GF<br>Storage Controller for UCSC-C125:<br>• UCSC-SAS9460-8i<br>SD Cards for UCSC-C125:<br>• UCS-SD-32G-S<br>• UCS-SD-64G-S<br>• UCS-SD-128G<br>Micro SD Card for UCSC-C125:<br>• UCS-MSD-32G<br>M.2 SATA SSD for UCSC-C125:<br>• UCS-M2-240GB<br>• UCS-M2-960GB<br>Flash USB Drive for UCSC-C125:<br>• UCS-USBFLSHB-16GB<br>Mini Storage Carriers for UCSC-C125:<br>• UCS-MSTOR-SD<br>• UCS-MSTOR-M2<br>Cisco VIC Adapters:<br>• VIC 1440 10/40G mLOM for B-Series (UCSB-MLOM-40G-04)<br>• VIC 1480 10/40G PCIe for B-Series (UCSB-VIC-M84-4P)<br>• VIC 1455 10/25G PCIe for C-Series and S-Series (UCSC-PCIE-C25Q-04)<br>• VIC 1457 10/25G mLOM for C-Series (UCSC-MLOM-C25Q-04)<br>HX NVMe Server:<br>• HXAF220C-M5SN<br>PCIe compression and cryptographic CPU offload card with C240HX M5 servers<br>• HX-PCIE-OFFLOAD-1 |

| UCS Release | Catalog File Name | Additional PIDs In This Release |
|---|---|---|
| | | Intel Optane NVMe Med. Performance Drives for M5 servers:<br>• UCSC-NVMEXP-I375<br>• UCSB-NVMEXP-I375<br>• UCSC-NVMEXP-I750<br>• UCSB-NVMEXP-I750 |

## Security Fixes

The following security issues are resolved:

| Release | Defect ID | Common Vulnerability and Exposures (CVE) ID | Description |
|---|---|---|---|
| 4.0(4o) | CSCwb74497<br>CSCwb74513 | CVE-2022-20824 | A vulnerability in the Cisco Discovery Protocol feature of Cisco FXOS Software and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to execute arbitrary code with root privileges or cause a denial of service (DoS) condition on an affected device.<br>For more information, see Cisco FXOS and NX-OS Software Cisco Discovery Protocol Denial of Service and Arbitrary Code Execution Vulnerability |

| Release | Defect ID | Common Vulnerability and Exposures (CVE) ID | Description |
|---|---|---|---|
| 4.0(4n) | CSCvy95840 | CVE-2022-20624 | In UCS 6400 Series Fabric Interconnects, the Cisco Fabric Services over IP (CFSoIP) is affected by the vulnerability identified by the following Common Vulnerability and Exposures (CVE) ID:<br>• CVE-2022-20624: A vulnerability in the Cisco Fabric Services over IP (CFSoIP) feature of Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of incoming CFSoIP packets. An attacker could exploit this vulnerability by sending crafted CFSoIP packets to an affected device. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition. |

| Release | Defect ID | Common Vulnerability and Exposures (CVE) ID | Description |
|---|---|---|---|
| 4.0(4n) | CSCvz72466 | CVE-2022-20625 | In Cisco UCS 6400 Series Fabric Interconnects, the Cisco Discovery Protocol service of Cisco NX-OS Software is affected by the vulnerability identified by the following Common Vulnerability and Exposures (CVE) ID:<br>• CVE-2022-20625: A vulnerability in the Cisco Discovery Protocol service of Cisco FXOS Software and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause the service to restart, resulting in a denial of service (DoS) condition. This vulnerability is due to improper handling of Cisco Discovery Protocol messages that are processed by the Cisco Discovery Protocol service. An attacker could exploit this vulnerability by sending a series of malicious Cisco Discovery Protocol messages to an affected device. A successful exploit could allow the attacker to cause the Cisco Discovery Protocol service to fail and restart. In rare conditions, repeated failures of the process could occur, which could cause the entire device to restart. |

| Release | Defect ID | Common Vulnerability and Exposures (CVE) ID | Description |
|---|---|---|---|
| 4.0(4n) | CSCvz74433 | CVE-2022-20625 | In Cisco UCS 6300 Series, UCS 6200 Series, and UCS-FI-6324 Fabric Interconnects, the Cisco Discovery Protocol service of Cisco NX-OS Software is affected by the vulnerability identified by the following Common Vulnerability and Exposures (CVE) ID:<br>• CVE-2022-20625: A vulnerability in the Cisco Discovery Protocol service of Cisco FXOS Software and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause the service to restart, resulting in a denial of service (DoS) condition. This vulnerability is due to improper handling of Cisco Discovery Protocol messages that are processed by the Cisco Discovery Protocol service. An attacker could exploit this vulnerability by sending a series of malicious Cisco Discovery Protocol messages to an affected device. A successful exploit could allow the attacker to cause the Cisco Discovery Protocol service to fail and restart. In rare conditions, repeated failures of the process could occur, which could cause the entire device to restart. |
| 4.0(4k) | CSCvu53094 | CVE-2020-11022 | Cisco UCS Manager and UCS 6400 Series Fabric Interconnects using the jQuery software package with versions from 1.2 to 3.5.0, is affected by the following Common Vulnerability and Exposures (CVE) ID:<br>• CVE-2020-11022: In jQuery versions greater than or equal to 1.2 and before 3.5.0, passing HTML from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0. |

| Release | Defect ID | Common Vulnerability and Exposures (CVE) ID | Description |
|---|---|---|---|
| 4.0(4i) | CSCvt86093 | • CVE-2020-0548<br>• CVE-2020-0549 | Cisco UCS M5 servers that are based on Intel® processors are affected by the vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) ID(s):<br>• CVE-2020-0548: Clean-up errors in some Intel® Processors may allow an authenticated user to potentially enable information disclosure via local access.<br>• CVE-2020-0549: Clean-up errors in some data cache evictions for some Intel® Processors may allow an authenticated user to potentially enable information disclosure via local access.<br>This release includes BIOS revisions for Cisco UCS M5 servers. These BIOS revisions include Microcode update for Cisco UCS M5 servers, which is a required part of the mitigation for these vulnerabilities. |
| 4.0(4i) | CSCvq33385 | CVE-2016-2183 | The latest CiscoSSL 1.0.2r.6.2.341 now includes mitigations for the OpenSSL vulnerabilities in Cisco UCS Manager identified by the Common Vulnerability and Exposures (CVE) ID listed. |

| Release | Defect ID | Common Vulnerability and Exposures (CVE) ID | Description |
|---|---|---|---|
| 4.0(4h) | CSCvs81686 | • CVE-2020-0548<br>• CVE-2020-0549 | Cisco UCS M5 servers that are based on Intel® processors are affected by vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) IDs:<br>• CVE-2020-0548 Cleanup errors in some Intel® Processors may allow an authenticated user to potentially enable information disclosure via local access.<br>• CVE-2020-0549 Cleanup errors in some data cache evictions for some Intel® Processors may allow an authenticated user to potentially enable information disclosure via local access.<br>This release includes BIOS revisions for Cisco UCS M5 servers. These BIOS revisions include the updated SINIT ACM for Cisco UCS M5 servers, which is a required part of the mitigation for these vulnerabilities. |

| Release | Defect ID | Common Vulnerability and Exposures (CVE) ID | Description |
|---|---|---|---|
| 4.0(4g) | CSCvr54409<br>CSCvr54415 | • CVE-2019-11135<br>• CVE-2019-0151<br>• CVE-2019-0152<br>• CVE-2019-11136<br>• CVE-2019-11137<br>• CVE-2019-11139<br>• CVE-2019-11109 | |

| Release | Defect ID | Common Vulnerability and Exposures (CVE) ID | Description |
|---|---|---|---|
| | | | Cisco UCS M5 servers that are based on Intel® processors are affected by vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) IDs:<br>• CVE-2019-11135 (TSX Asynchronous Abort Advisory) condition affects certain 2nd Generation Intel® Xeon® Scalable Processors, 8th Generation Intel® Core™ Processor Family, 9th Generation Intel® CoreTM Processor Family, and 10th Generation Intel® Core™ Processor Family that utilize speculative execution, and may allow an authenticated user to potentially enable information disclosure through a side-channel with local access.<br>• CVE-2019-0151 (CPU Local Privilege Escalation Advisory) affects certain Intel® 4th Generation Intel® Core™ Processors, 5th Generation Intel® Core™ Processors, 6th Generation Intel® Cores Processors, 7th Generation Intel® Core™ Processors, 8th Generation Intel® Core™ Processors, Intel® Xeon® Processors E3 v2/v3/v4/v5/v6 Family, Intel® Xeon® Processors E5 v3/v4 Family, Intel® Xeon® Processors E7 v3/v4 Family, Intel® Xeon® Scalable Processors 2nd Generation, Intel® Xeon® Scalable Processors, Intel® Xeon® Processors D-1500/D-2100), Intel® Xeon® Processors E-2100/E3100, and, Intel® Xeon® Processors W-2100/W-3100 when insufficient memory protection in Intel® TXT may allow a privileged user to potentially enable escalation of privilege through local access. This could result in bypassing Intel® TXT protections. |

| Release | Defect ID | Common Vulnerability and Exposures (CVE) ID | Description |
|---|---|---|---|
|  |  |  | • CVE-2019-0152 (CPU Local Privilege Escalation Advisory) affects certain Intel® Xeon® Scalable Processors, Intel® Xeon® Processor D-2100, D-3100, Intel® Xeon® Processor W-2100, W-3100 when insufficient memory protection may allow a privileged user to potentially enable an escalation of privilege through local access. This could result in bypassing System Management Mode (SMM) and Intel® TXT protections.<br>• CVE-2019-11136 (BIOS 2019.2 IPU Advisory) affects 2nd Generation Intel® Xeon® Scalable Processors, Intel® Xeon® Scalable Processors, Intel® Xeon® Processor D Family when insufficient access control in the system firmware may allow a privileged user to potentially enable an escalation of privilege, denial of service, or information disclosure through local access.<br>• CVE-2019-11137 (BIOS 2019.2 IPU Advisory) affects 2nd Generation Intel® Xeon® Scalable Processors, Intel® Xeon® Scalable Processors, Intel® Xeon® Processor D Family, Intel® Xeon® Processor E5 v4 Family, Intel® Xeon® Processor E7 v4 Family, Intel® Atom® Processor C Series when insufficient input validation in the system firmware may allow a privileged user to potentially enable an escalation of privilege, denial of service, or information disclosure through local access. |

| Release | Defect ID | Common Vulnerability and Exposures (CVE) ID | Description |
|---|---|---|---|
| | | | • CVE-2019-11139 (Voltage Modulation Technical Advisory) vulnerability in voltage modulation of certain Intel® Xeon® Scalable Processors may allow a privileged user to potentially enable denial of service through local access.<br>• CVE-2019-11109: Logic issue in subsystem in Intel® Server Platform Services before versions SPS_E5_04.01.04.297.0, SPS_SoC-X_04.00.04.101.0, and SPS_SoC-A_04.00.04.193.0 may allow a privileged user to potentially enable Denial of Service through local.<br>This release includes BIOS revisions for Cisco UCS M5 servers. These BIOS revisions include the updated microcode and Secure Initialization (SINIT) Authenticated Code Modules (ACM), which are required parts of the mitigation for these vulnerabilities. |

| Release | Defect ID | Common Vulnerability and Exposures (CVE) ID | Description |
|---|---|---|---|
| 4.0(4g) | CSCvr54413<br>CSCvr54414<br>CSCvr54416 | • CVE-2019-0151<br>• CVE-2019-11137 | |

| Release | Defect ID | Common Vulnerability and Exposures (CVE) ID | Description |
|---|---|---|---|
| | | | Cisco UCS M4 servers that are based on Intel® processors are affected by vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) IDs:<br>• CVE-2019-0151 (CPU Local Privilege Escalation Advisory) affects certain Intel® 4th Generation Intel® Core™ Processors, 5th Generation Intel® Core™ Processors, 6th Generation Intel® Cores Processors, 7th Generation Intel® Core™ Processors, 8th Generation Intel® Core™ Processors, Intel® Xeon® Processors E3 v2/v3/v4/v5/v6 Family, Intel® Xeon® Processors E5 v3/v4 Family, Intel® Xeon® Processors E7 v3/v4 Family, Intel® Xeon® Scalable Processors 2nd Generation, Intel® Xeon® Scalable Processors, Intel® Xeon® Processors D-1500/D-2100), Intel® Xeon® Processors E-2100/E3100, and, Intel® Xeon® Processors W-2100/W-3100 when insufficient memory protection in Intel® TXT may allow a privileged user to potentially enable escalation of privilege through local access. This could result in bypassing Intel® TXT protections.<br>• CVE-2019-11137 (BIOS 2019.2 IPU Advisory) affects 2nd Generation Intel® Xeon® Scalable Processors, Intel® Xeon® Scalable Processors, Intel® Xeon® Processor D Family, Intel® Xeon® Processor E5 v4 Family, Intel® Xeon® Processor E7 v4 Family, Intel® Atom® Processor C Series when insufficient input validation in the system firmware may allow a privileged user to potentially enable an escalation of privilege, denial of service, or information disclosure through local access. |

| Release | Defect ID | Common Vulnerability and Exposures (CVE) ID | Description |
|---|---|---|---|
| | | | This release includes BIOS revisions for Cisco UCS M4 servers. These BIOS revisions include the updated microcode and SINIT ACM for Cisco UCS M4 servers, which are required parts of the mitigation for these vulnerabilities. |
| 4.0(4g) | CSCvr54411 | CVE-2019-0151 | Cisco UCS B-Series and C-Series M3 servers that are based on Intel® processors are affected by vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) ID:<br>• CVE-2019-0151 (CPU Local Privilege Escalation Advisory) affects certain Intel® 4th Generation Intel® Core$^{TM}$ Processors, 5th Generation Intel® Core$^{TM}$ Processors, 6th Generation Intel® Cores Processors, 7th Generation Intel® Core$^{TM}$ Processors, 8th Generation Intel® Core$^{TM}$ Processors, Intel® Xeon® Processors E3 v2/v3/v4/v5/v6 Family, Intel® Xeon® Processors E5 v3/v4 Family, Intel® Xeon® Processors E7 v3/v4 Family, Intel® Xeon® Scalable Processors 2nd Generation, Intel® Xeon® Scalable Processors, Intel® Xeon® Processors D-1500/D-2100), Intel® Xeon® Processors E-2100/E3100, and, Intel® Xeon® Processors W-2100/W-3100 when insufficient memory protection in Intel® TXT may allow a privileged user to potentially enable escalation of privilege through local access. This could result in bypassing Intel® TXT protections.<br>This release includes BIOS revisions for Cisco UCS B-Series and C-Series M3 servers. These BIOS revisions include the updated SINIT ACM for Cisco UCS M3 servers, which is a required part of the mitigation for these vulnerabilities. |

| Release | Defect ID | Common Vulnerability and Exposures (CVE) ID | Description |
|---|---|---|---|
| 4.0(4f) | CSCvq19565 | CVE-2019-11479<br>CVE-2019-11478 | This bug was filed to evaluate the product against the vulnerability affecting Linux kernel, identified by the following CVE IDs:<br>• CVE-2019-11479: Excess Resource Consumption Due to Low MSS Values<br>• CVE-2019-11478: SACK Slowness or Excess Resource Usage<br>TCP networking vulnerabilities have been identified affecting Linux kernel. The vulnerabilities specifically relate to the minimum segment size (MSS) and TCP Selective Acknowledgement (SACK) capabilities. The most serious, dubbed "SACK Panic" allows a remotely-triggered kernel panic on recent Linux kernels.<br>Cisco UCS servers with 6200 Series Fabric Interconnects have been determined to contain a vulnerable version of Linux Kernel. However the product is not affected by the following vulnerability:<br>CVE-2019-11477: SACK Kernel Panic<br>Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.<br>Additional details about the vulnerabilities listed above can be found at http://cve.mitre.org/cve/cve.html |

| Release | Defect ID | Common Vulnerability and Exposures (CVE) ID | Description |
|---|---|---|---|
| 4.0(4f) | CSCvq21317 | CVE-2019-11477<br>CVE-2019-11478<br>CVE-2019-11479 | This bug was filed to evaluate the product against the vulnerability affecting Linux kernel, identified by the following CVE IDs:<br>• CVE-2019-11477: SACK Panic<br>• CVE-2019-11478: SACK Slowness or Excess Resource Usage<br>• CVE-2019-11479: Excess Resource Consumption Due to Low MSS Values<br>TCP networking vulnerabilities have been identified affecting Linux kernel. The vulnerabilities specifically relate to the minimum segment size (MSS) and TCP Selective Acknowledgement (SACK) capabilities. The most serious, dubbed "SACK Panic" allows a remotely-triggered kernel panic on recent Linux kernels.<br>Cisco UCS servers with 6400 Series Fabric Interconnects have been determined to contain a vulnerable version of Linux Kernel.<br>Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.<br>Additional details about the vulnerabilities listed above can be found at http://cve.mitre.org/cve/cve.html |

| Release | Defect ID | Common Vulnerability and Exposures (CVE) ID | Description |
|---|---|---|---|
| 4.0(4f) | CSCvm80093 | CVE-2019-1966 | A vulnerability in the CLI implementation of a specific command for the Cisco UCS Fabric Interconnect could have allowed an authenticated, local attacker to escape the CLI and gain unauthorized access to the underlying operating system of the device.<br>An attacker could have exploited this vulnerability to escape the CLI and execute arbitrary commands on the underlying operating system with the privileges of the root user. The attacker would need valid device credentials.<br>Additional information on Cisco's security vulnerability policy can be found at the following URL:<br>Security Vulnerability Policy. |
| 4.0(4f) | CSCvp56979 | CVE-2019-9213 | Cisco UCS servers with 6400 Series Fabric Interconnects have been determined to contain third-party software that is affected by the vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) IDs:<br>CVE-2019-9213: Linux Kernel expand_downwards Function NULL Pointer Dereference Vulnerability<br>Cisco has released software updates that address this vulnerability.<br>Additional details about the vulnerabilities listed above can be found at http://cve.mitre.org/cve/cve.html. |

| Release | Defect ID | Common Vulnerability and Exposures (CVE) ID | Description |
|---|---|---|---|
| 4.0(4e) | CSCvp62709<br>CSCvp69717 | CVE-2019-11358 | Cisco UCS Manager and UCS 6200 Series Fabric Interconnects included a version of the jQuery software package that is affected by the cross-site scripting vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) IDs:<br>CVE-2019-11358<br>Additional information on Cisco's security vulnerability policy can be found here:<br>Security Vulnerability Policy |
| 4.0(4e) | CSCvn23535<br>CSCvn23538 | CVE-2019-1963 | A vulnerability in the Simple Network Management Protocol (SNMP) input packet processor of Cisco FXOS Software and Cisco NX-OS Software could allow an authenticated, remote attacker to cause the SNMP application on an affected device to restart unexpectedly.<br>The vulnerability is due to improper validation of Abstract Syntax Notation One (ASN.1) encoded variables in SNMP packets. An attacker could exploit this vulnerability by sending a crafted SNMP packet to the SNMP daemon on the affected device. A successful exploit could allow the attacker to cause the SNMP application to restart multiple times, leading to a system-level restart and a denial of service (DoS) condition.<br>Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.<br>This advisory is available at the following link:<br>Cisco FXOS and NX-OS Software Authenticated Simple Network Management Protocol Denial of Service Vulnerability |

| Release | Defect ID | Common Vulnerability and Exposures (CVE) ID | Description |
|---|---|---|---|
| 4.0(4c) | CSCvp27917 | CVE-2018-12126<br>CVE-2018-12127<br>CVE-2018-12130<br>CVE-2019-11091 | |

| Release | Defect ID | Common Vulnerability and Exposures (CVE) ID | Description |
|---|---|---|---|
| | | | Cisco UCS B-Series M3 Blade Servers are based on Intel® Xeon® Sandy Bridge E5-2600 and Ivy Bridge E5 2600 v2 Product Family processors that are vulnerable to variants of exploits that use Microarchitectural Data Sampling (MDS) to gain access to data being processed in the CPU by other applications.<br>• CVE-2018-12126 (Microarchitectural Store Buffer Data Sampling) affects store buffers in the CPU, and is addressed by applying the updated microcode included in the UCS Manager release as well as the relevant Operating System and Hypervisor patches from the appropriate vendors.<br>• CVE-2018-12127 (Microarchitectural Load Port Data Sampling) affects load buffers in the CPU, and is addressed by applying the updated microcode included in the UCS Manager release as well as the relevant Operating System and Hypervisor patches from the appropriate vendors.<br>• CVE-2018-12130 (Microarchitectural Fill Buffer Data Sampling) affects line fill buffers in the CPU, and is addressed by applying the updated microcode included in the UCS Manager release as well as the relevant Operating System and Hypervisor patches from the appropriate vendors.<br>• CVE-2019-11091 (Microarchitectural Data Sampling Uncacheable Memory) affects uncacheable memory in the CPU, and is addressed by applying the updated microcode included in the UCS Manager release as well as |

| Release | Defect ID | Common Vulnerability and Exposures (CVE) ID | Description |
|---|---|---|---|
| | | | the relevant Operating System and Hypervisor patches from the appropriate vendors.<br>This release includes BIOS revisions for Cisco UCS M3 generation servers. These BIOS revisions include the updated microcode that is a required part of the mitigation for these vulnerabilities.<br>Additional details about the vulnerabilities listed above can be found at http://cve.mitre.org/cve/cve.html |
| 4.0(4c) | CSCvq66225 | CVE-2019-9836 | On the Cisco UCS C-Series servers that are based on AMD EPYC™ processors, using the user-selectable AMD secure encryption feature on a virtual machine running the Linux operating system, an encryption key could be compromised by manipulating the encryption technology's behavior. This release includes the BIOS revision to mitigate this risk. For more information about this vulnerability, see https://www.amd.com/en/corporate/product-security. |
| 4.0(4c) | CSCvp12424 | CVE-2019-1559 | Cisco UCS Manager includes a version of the OpenSSH Protocol that is affected by the vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) ID:<br>• CVE-2019-1559<br>If an application encounters a fatal protocol error and then calls SSL_shutdown() twice, it could behave like a padding oracle that could be used to decrypt data.<br>This issue is resolved through the OpenSSL software updates. For more information, go to https://tools.cisco.com/security/center/viewAlert.x?alertId=59697. |

| Release | Defect ID | Common Vulnerability and Exposures (CVE) ID | Description |
|---|---|---|---|
| 4.0(4b)<br>4.0(2e) | CSCvo21412<br>CSCvp30013 | CVE-2018-12126<br>CVE-2018-12127<br>CVE-2018-12130<br>CVE-2019-11091 | |

| Release | Defect ID | Common Vulnerability and Exposures (CVE) ID | Description |
|---|---|---|---|
| | | | Cisco UCS M4 servers and Hyperflex M4 servers are based on Intel® Xeon® Processor E7 v2, v3, and v4 Product Family processors that are vulnerable to variants of exploits that use Microarchitectural Data Sampling (MDS) to gain access to data being processed in the CPU by other applications.<br>• CVE-2018-12126 (Microarchitectural Store Buffer Data Sampling) affects store buffers in the CPU, and is addressed by applying the updated microcode included in the UCS Manager release as well as the relevant Operating System and Hypervisor patches from the appropriate vendors.<br>• CVE-2018-12127 (Microarchitectural Load Port Data Sampling) affects load buffers in the CPU, and is addressed by applying the updated microcode included in the UCS Manager release as well as the relevant Operating System and Hypervisor patches from the appropriate vendors.<br>• CVE-2018-12130 (Microarchitectural Fill Buffer Data Sampling) affects line fill buffers in the CPU, and is addressed by applying the updated microcode included in the UCS Manager release as well as the relevant Operating System and Hypervisor patches from the appropriate vendors.<br>• CVE-2019-11091 (Microarchitectural Data Sampling Uncacheable Memory) affects uncacheable memory in the CPU, and is addressed by applying the updated microcode included in the UCS Manager release as well as |

| Release | Defect ID | Common Vulnerability and Exposures (CVE) ID | Description |
|---|---|---|---|
|  |  |  | the relevant Operating System and Hypervisor patches from the appropriate vendors.<br>This release includes BIOS revisions for Cisco UCS M4 generation servers. These BIOS revisions include the updated microcode that is a required part of the mitigation for these vulnerabilities. |

| Release | Defect ID | Common Vulnerability and Exposures (CVE) ID | Description |
|---|---|---|---|
| 4.0(4b)<br>4.0(2e) | CSCvp28016 | CVE-2018-12126<br>CVE-2018-12127<br>CVE-2018-12130<br>CVE-2019-11091 | |

| Release | Defect ID | Common Vulnerability and Exposures (CVE) ID | Description |
|---|---|---|---|
| | | | Cisco UCS M4 servers and Hyperflex M4 servers are based on Intel® Xeon® Processor E5 v3 and v4 Product Family processors that are vulnerable to variants of exploits that use Microarchitectural Data Sampling (MDS) to gain access to data being processed in the CPU by other applications.<br>• CVE-2018-12126 (Microarchitectural Store Buffer Data Sampling) affects store buffers in the CPU, and is addressed by applying the updated microcode included in the UCS Manager release as well as the relevant Operating System and Hypervisor patches from the appropriate vendors.<br>• CVE-2018-12127 (Microarchitectural Load Port Data Sampling) affects load buffers in the CPU, and is addressed by applying the updated microcode included in the UCS Manager release as well as the relevant Operating System and Hypervisor patches from the appropriate vendors.<br>• CVE-2018-12130 (Microarchitectural Fill Buffer Data Sampling) affects line fill buffers in the CPU, and is addressed by applying the updated microcode included in the UCS Manager release as well as the relevant Operating System and Hypervisor patches from the appropriate vendors.<br>• CVE-2019-11091 (Microarchitectural Data Sampling Uncacheable Memory) affects uncacheable memory in the CPU, and is addressed by applying the updated microcode included in the UCS Manager release as well as |

| Release | Defect ID | Common Vulnerability and Exposures (CVE) ID | Description |
|---|---|---|---|
| | | | the relevant Operating System and Hypervisor patches from the appropriate vendors.<br>This release includes BIOS revisions for Cisco UCS M4 generation servers. These BIOS revisions include the updated microcode that is a required part of the mitigation for these vulnerabilities. |

| Release | Defect ID | Common Vulnerability and Exposures (CVE) ID | Description |
|---|---|---|---|
| 4.0(4b)<br>4.0(2e) | CSCvp31847 | CVE-2018-12126<br>CVE-2018-12127<br>CVE-2018-12130<br>CVE-2019-11091 | |

| Release | Defect ID | Common Vulnerability and Exposures (CVE) ID | Description |
|---|---|---|---|
| | | | Cisco UCS M5 servers and Hyperflex M5 servers are based on Intel® Xeon® Scalable processors that are vulnerable to variants of exploits that use Microarchitectural Data Sampling (MDS) to gain access to data being processed in the CPU by other applications.<br>• CVE-2018-12126 (Microarchitectural Store Buffer Data Sampling) affects store buffers in the CPU, and is addressed by applying the updated microcode included in the UCS Manager release as well as the relevant Operating System and Hypervisor patches from the appropriate vendors.<br>• CVE-2018-12127 (Microarchitectural Load Port Data Sampling) affects load buffers in the CPU, and is addressed by applying the updated microcode included in the UCS Manager release as well as the relevant Operating System and Hypervisor patches from the appropriate vendors.<br>• CVE-2018-12130 (Microarchitectural Fill Buffer Data Sampling) affects line fill buffers in the CPU, and is addressed by applying the updated microcode included in the UCS Manager release as well as the relevant Operating System and Hypervisor patches from the appropriate vendors.<br>• CVE-2019-11091 (Microarchitectural Data Sampling Uncacheable Memory) affects uncacheable memory in the CPU, and is addressed by applying the updated microcode included in the UCS Manager release as well as the relevant Operating System and |

| Release | Defect ID | Common Vulnerability and Exposures (CVE) ID | Description |
|---|---|---|---|
| | | | Hypervisor patches from the appropriate vendors.<br>This release includes BIOS revisions for Cisco UCS M5 generation servers. These BIOS revisions include the updated microcode that is a required part of the mitigation for these vulnerabilities. |
| 4.0(2a) | CSCvm35067 | CVE-2018-3655 | Cisco UCS C-Series servers include a version of the Intel® Converged Security Management Engine (CSME) that maybe affected by the vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) ID:<br>• CVE-2018-3655<br>An attacker with physical access could use these vulnerabilities to do the following:<br>• Bypass Intel® CSME anti-replay protection, thus allowing potential brute force attacks on secrets stored inside the Intel CSME<br>• Gain unauthorized access to the Intel® MEBX password<br>• Tamper with the integrity of the Intel® CSME file system directories or the Server Platform Services and Trusted Execution Environment (Intel® TXE) data files<br>This release includes BIOS revisions for Cisco UCS M5 generation C-Series servers. |

| Release | Defect ID | Common Vulnerability and Exposures (CVE) ID | Description |
|---|---|---|---|
| 4.0(1d) | CSCvm19864 | CVE-2016-3115 | Cisco UCS Manager and UCS 6200 Series Fabric Interconnects include a version of the OpenSSH Protocol that is affected by the vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) IDs:<br>• CVE-2016-3115<br>Cisco has released software updates that address this vulnerability. |
| 4.0(1c) | CSCvk20775 | CVE-2018-3655 | Cisco UCS B-Series servers include a version of the Intel® Converged Security Management Engine (CSME) that maybe affected by the vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) ID:<br>• CVE-2018-3655<br>An attacker with physical access could use these vulnerabilities to do the following:<br>• Bypass Intel® CSME anti-replay protection, thus allowing potential brute force attacks on secrets stored inside the Intel CSME<br>• Gain unauthorized access to the Intel® MEBX password<br>• Tamper with the integrity of the Intel® CSME file system directories or the Server Platform Services and Trusted Execution Environment (Intel® TXE) data files<br>This release includes BIOS revisions for Cisco UCS M5 generation B-Series servers. |

| Release | Defect ID | Common Vulnerability and Exposures (CVE) ID | Description |
|---|---|---|---|
| 4.0(1a) | CSCvm03356 | CVE-2018-3615<br>CVE-2018-3620<br>CVE-2018-3646 | Cisco UCS B-Series M3 servers and C-Series M3 servers are based on Intel® processors that are vulnerable to exploits that use CPU speculative processing and data cache timing to potentially identify privileged information. These exploits are collectively known as L1 Terminal Fault (L1TF).<br>• CVE-2018-3615 (affecting SGX), also known as Foreshadow, is not known to affect any existing Cisco UCS servers because Cisco UCS M5 and earlier generation servers, and HyperFlex M5 and earlier generation servers do not use Intel® SGX technology.<br>• CVE-2018-3620 (affecting OS/System Management Mode) and CVE-2018-3646 (affecting Virtual Machine Monitors) are referred to as L1 Terminal Fault attacks by Intel®. These vulnerabilities are mitigated by applying the updated processor microcode from Intel® included in the server firmware bundle, and the relevant Operating System and Hypervisor patches from the appropriate vendors.<br>This release includes BIOS revisions for Cisco UCS M3 generation servers. These BIOS revisions include the updated processor microcode that is a required part of the mitigation for CVE-2018-3620 (OS/SMM) and CVE-2018-3646 (VMM). Operating System and Hypervisor patches from the appropriate vendors may also be required to mitigate these vulnerabilities.<br>For more information, please see the Cisco Security Advisory available here:<br>CPU Side-Channel Information Disclosure Vulnerabilities: August 2018 |

| Release | Defect ID | Common Vulnerability and Exposures (CVE) ID | Description |
|---|---|---|---|
| 4.0(1a) | CSCvm03351 | CVE-2018-3615<br>CVE-2018-3620<br>CVE-2018-3646 | Cisco UCS B-Series M4 servers, C-Series M4 servers, S3260 M4 storage servers, and HyperFlex M4 servers are vulnerable to exploits that use CPU speculative processing and data cache timing to potentially identify privileged information. These exploits are collectively known as L1 Terminal Fault (L1TF).<br>• CVE-2018-3615 (affecting SGX), also known as Foreshadow, is not known to affect any existing Cisco UCS servers because Cisco UCS M5 and earlier generation servers, and HyperFlex M5 and earlier generation servers do not use Intel® SGX technology.<br>• CVE-2018-3620 (affecting OS/System Management Mode) and CVE-2018-3646 (affecting Virtual Machine Monitors) are referred to as L1 Terminal Fault attacks by Intel®. These vulnerabilities are mitigated by applying the updated processor microcode from Intel® included in the server firmware bundle, and the relevant Operating System and Hypervisor patches from the appropriate vendors.<br>This release includes BIOS revisions for Cisco UCS M4 generation servers. These BIOS revisions include the updated processor microcode that is a required part of the mitigation for CVE-2018-3620 (OS/SMM) and CVE-2018-3646 (VMM). Operating System and Hypervisor patches from the appropriate vendors may also be required to mitigate these vulnerabilities.<br>For more information, please see the Cisco Security Advisory available here:<br>CPU Side-Channel Information Disclosure Vulnerabilities: August 2018 |

| Release | Defect ID | Common Vulnerability and Exposures (CVE) ID | Description |
|---|---|---|---|
| 4.0(1a) | CSCvm03339 | CVE-2018-3615<br>CVE-2018-3620<br>CVE-2018-3646 | |

| Release | Defect ID | Common Vulnerability and Exposures (CVE) ID | Description |
|---|---|---|---|
|  |  |  | Cisco UCS B-Series M5 servers, C-Series M5 servers, and HyperFlex M5 servers are based on Intel® processors that are vulnerable to exploits that use CPU speculative processing and data cache timing to potentially identify privileged information. These exploits are collectively known as L1 Terminal Fault (L1TF).<br>• CVE-2018-3615 (affecting SGX), also known as Foreshadow, is not known to affect any existing Cisco UCS servers because Cisco UCS M5 and earlier generation servers, and HyperFlex M5 and earlier generation servers do not use Intel® SGX technology.<br>• CVE-2018-3620 (affecting OS/System Management Mode) and CVE-2018-3646 (affecting Virtual Machine Monitors) are referred to as L1 Terminal Fault attacks by Intel®. These vulnerabilities are mitigated by applying the updated processor microcode from Intel® included in the server firmware bundle, and the relevant Operating System and Hypervisor patches from the appropriate vendors.<br>This release includes BIOS revisions for Cisco UCS M5 generation servers. These BIOS revisions include the updated processor microcode that is a required part of the mitigation for CVE-2018-3620 (OS/SMM) and CVE-2018-3646 (VMM). Operating System and Hypervisor patches from the appropriate vendors may also be required to mitigate these vulnerabilities.<br>For more information, please see the Cisco Security Advisory available here:<br>CPU Side-Channel Information |

| Release | Defect ID | Common Vulnerability and Exposures (CVE) ID | Description |
|---|---|---|---|
| | | | Disclosure Vulnerabilities: August 2018 |
| 4.0(1a) | CSCvg58650 | • CVE-2017-5718 | Cisco UCS 6200 Series and 6300 Series Fabric Interconnects include a version of Intel system firmware for Intel Core Processors that is affected by the vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) ID:<br>• CVE-2017-5718 is addressed by applying the updated processor microcode from Intel included in the server firmware bundle, and the relevant Operating System and Hypervisor patches from the appropriate vendors.<br>This release includes BIOS revisions to address the vulnerabilty. |

| Release | Defect ID | Common Vulnerability and Exposures (CVE) ID | Description |
|---|---|---|---|
| 4.0(1a) | CSCvh25150 | CVE-2017-3883 | A vulnerability in the authentication, authorization, and accounting (AAA) implementation of Cisco Firepower Extensible Operating System (FXOS) and NX-OS System Software could allow an unauthenticated, remote attacker to cause an affected device to reload.<br>The vulnerability occurs because AAA processes prevent the NX-OS System Manager from receiving keepalive messages when an affected device receives a high rate of login attempts, such as in a brute-force login attack. System memory can run low on the FXOS devices under the same conditions, which could cause the AAA process to unexpectedly restart or cause the device to reload.<br>An attacker could exploit this vulnerability by performing a brute-force login attack against a device that is configured with AAA security services. A successful exploit could allow the attacker to cause the affected device to reload.<br>Cisco has released software updates that address this vulnerability. There are workarounds that address this vulnerability.<br>For more information, see the Cisco Security Advisory available here:<br>Cisco FXOS and NX-OS System Software Authentication, Authorization, and Accounting Denial of Service Vulnerability |

| Release | Defect ID | Common Vulnerability and Exposures (CVE) ID | Description |
|---|---|---|---|
| 4.0(1a) | CSCva61699 | Common Weakness Enumeration (CWE) IDs:<br>• 525<br>• 933<br>• 16<br>• 311<br>• 200 | The following security vulnerabilities were identified for HTTP response and affected Cisco UCS Manager:<br>• Incomplete or no cache-control and Pragma HTTP header set<br>• Web browser XSS protection not enabled<br>• X-Content-Type-Options header missing<br>• Secure pages include mixed content<br>• Private IP disclosure<br>Of these security vulnerabilities, Cisco has addressed the following in this release:<br>• Web browser XSS protection not enabled<br>• X-Content-Type-Options header missing<br>The **Incomplete or no cache-control and Pragma HTTP header set** vulnerability vulnerability will not be fixed because of the following:<br>• Disabling of caching results in a sluggish GUI experience<br>• KVM launch is impacted if we disable caching |
| 4.0(1a) | CSCvi95784 | • CVE-2017-15715<br>• CVE-2018-1303<br>• CVE-2018-1301<br>• CVE-2018-1302<br>• CVE-2018-1283<br>• CVE-2018-1312<br>• CVE-2017-15710 | The Apache version used with previous Cisco UCS Manager releases was affected by the Common Vulnerability and Exposures (CVE) IDs listed. Most of these CVE IDs are low risk, or not applicable to Cisco UCS Manager. |

## Default Open Ports

The following table lists the default open ports used in Cisco UCS Manager Release 4.0.

| Port | Interface | Protocol | Traffic Type | Fabric Interconnect | Usage |
|---|---|---|---|---|---|
| 22 | CLI | SSH | TCP | UCS 6200 Series<br>UCS 6300 Series<br>UCS 6400 Series<br>UCS 6500 Series | Cisco UCS Manager CLI access |
| 80 | XML | HTTP | TCP | UCS 6200 Series<br>UCS 6300 Series<br>UCS 6400 Series<br>UCS 6500 Series | Cisco UCS Manager GUI and third party management stations.<br>Client download |
| 443 | XML | HTTP | TCP | UCS 6200 Series<br>UCS 6300 Series<br>UCS 6400 Series<br>UCS 6500 Series | Cisco UCS Manager login page access<br>Cisco UCS Manager XML API access |
| 743 | KVM | HTTP | TCP | UCS 6200 Series<br>UCS 6300 Series<br>UCS 6400 Series | CIMC Web Service / Direct KVM |
| 843 | xmlPolicy | Adobe Flash | TCP | UCS 6200 Series<br>UCS 6300 Series | Adobe Flash port used by KVM launcher |

| Port | Interface | Protocol | Traffic Type | Fabric Interconnect | Usage |
|---|---|---|---|---|---|
| 5661 | | HTTPD | TCP | UCS 6400 Series | Internal communication<br>Disabled in Cisco UCS Manager Release 4.0(4f) |
| 7162 | | HTTPD | TCP | UCS 6400 Series | Internal communication<br>Disabled in Cisco UCS Manager Release 4.0(4g) |
| 7546 | CFS | CFSD | TCP | UCS 6400 Series<br>UCS 6500 Series | Cisco Fabric Service |

*Cisco UCS Manager Network Management Guide, Release 4.0* provides a complete list of open TCP and UDP ports.

## Libfabric and Open MPI

Cisco usNIC support in the Libfabric and Open MPI open source packages is readily available from their community web sites (http://libfabric.org/ and http://www.open-mpi.org/, respectively).

Cisco UCS Manager Release 3.1(3) and later releases no longer include Open MPI binary packages. Future UCS software driver bundles distributed through the usual Cisco software channels may not include binaries for the libfabric packages. Cisco engineers continue to be active, core contributors in both the Libfabric and Open MPI communities, and will actively develop and support users through the usual community or commercial ISV support mechanisms (e.g., IBM Spectrum MPI).

## Resolved Caveats

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

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

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

### Resolved Caveats for this Release 4.0(4o)

The following caveats are resolved in Release 4.0(4o):

| Defect ID | Symptom | First Bundle Affected | Resolved in Release |
|---|---|---|---|
| CSCvy52458 | The system time on Cisco UCS Manager is not in synchronization with the NTP servers. This issue is seen when:<br>• The NTP server configuration is present in Cisco UCS Manager but missing in the NXOS configuration.<br>• The NTP server is configured with domain name.<br>This issue is resolved. | 4.0(4g)A | 4.0(4o)A |
| CSCwa85770 | Cisco UCS M4 servers show additional remote NDIS compatible devices in the Ethernet interfaces.<br>This issue is resolved. | 4.1(3h)C | 4.0(4o)C |
| CSCvx37634 | Cisco UCS B200 M5 server discovery fails with the following fault message: `Setup of Vmediafailed(sam:dme:ComputeBladeDiscover`<br>`:SetupVm`<br>This issue is resolved. | 4.1(1c)B | 4.0(4o)B |
| CSCwa85667 | BMC reset is observed on Cisco UCS C-Series and B-Series M5/M6 servers due to kernel crash and watchdog reset.<br>This issue is resolved. | 4.0(4m)A | 4.0(4o)A |
| CSCwc99962 | Unable to form san-port-channel between UCS and Nexus 9000 switch in a setup equipped with Cisco UCS 6200 series FI.<br>This issue is resolved. | 4.1(3h)A | 4.0(4o)A |
| CSCwb89732 | In a setup with 6400 FIs, while accessing the KVM IP address, you are redirected to Cisco UCS Manager GUI.<br>This issue is resolved. | 4.1(3f)A | 4.0(4o)A |
| CSCvv57606 | Cisco UCS Manager fails to associate Service Profile for Cisco UCS servers connected to Cisco UCS 6400 FI through 2408 IOMs. Following error message is displayed:<br>`Connection Placement Error`<br>This issue is resolved. | 4.0(4e)B | 4.0(4o)B |

| Defect ID | Symptom | First Bundle Affected | Resolved in Release |
|---|---|---|---|
| CSCwd19078 | Cisco UCS Blade servers lose SAN connectivity when one of the FC up-link or FI is down because of the following reasons:<br>• FC link is congested<br>• Peer FC link is down due to peer system crash or errors on the receiving side<br>This issue is resolved. | 4.2(1f)A | 4.0(4o)A |

## Resolved Caveats for this Release 4.0(4n)

The following caveats are resolved in Release 4.0(4n):

| Defect ID | Symptom | First Bundle Affected | Resolved in Release |
|---|---|---|---|
| CSCvz44891 | During the firmware upgrade on the 2300 series IOMs, the Power Supply Unit (PSU) shut down on the IOM unexpectedly powers off the entire chassis.<br>This issue is resolved. | 4.1(2b)A | 4.0(4n)A |
| CSCvw64214 | The Azure Stack Hub server failed due to a failure in the QLogic NIC driver.<br>This issue is resolved. | 4.0(4i)C | 4.0(4n)C |
| CSCvx99711 | In Cisco UCS 6300 series Fabric Interconnects, the `show version` command on NXOS prompt does not show complete information. The two fields below show empty strings:<br>• SSD Model<br>• SSD Firmware version<br>This issue is resolved. | 3.2(3a)A | 4.0(4n)A |
| CSCvz08447 | The Cisco UCS 6400 series Fabric Interconnects running on 4.0(4x) unexpectedly resets the Fabric Interconnect B. The NXOS logs show the following reset reason: `Reset triggered due to HA policy of Reset Service: sysmgr stateful recovery.`<br>This issue is resolved. | 4.0(4a)A | 4.0(4n)A |
| CSCvz64536 | The Cisco UCS C240 M5 Rack server discovery fails with `HBA Firmware Version Error` when all 6x PCIE adapter slots and MLOM adapter slots are populated.<br>This issue is resolved. | 4.1(3c)A | 4.0(4n)A |

| Defect ID | Symptom | First Bundle Affected | Resolved in Release |
|---|---|---|---|
| CSCwa97427 | When upgrading to 4.2(2) CIMC software from 4.0(4m) or older versions, the update process fails and runs into an endless retry loop. The issue is because of the CIMC 4.0(4m) or older contains an incorrect size limit check for new images and it prevents the upgrade.<br>This issue is resolved. | 4.0(4m)B | 4.0(4n)B |
| CSCvx54145 | Unable to expand the UCS Manager when navigating through Firmware Management > Installed Firmware > Activate Firmware and clicking on the + sign to open the list view. The issue is observed only on Chrome and Edge browsers.<br>This issue is resolved. | 4.2(1d) | 4.0(4n) |
| CSCvz01679 | On a UCSM domain, when an SNMP walk is using Object Identifier (OIDs), discrepancy in return values between Fabric Interconnect A and Fabric Interconnect B is observed.<br>This issue is resolved. | 4.1(3b)A | 4.0(4n)A |
| CSCvz86823 | In Cisco UCS B200 M4 server, the host demands multiple reboots to ensure the UEFI boot option is not written to BIOS NVRAM when the OS is installed.<br>This issue is resolved. | 4.1(1) | 4.0(4n) |
| CSCwa85770 | On Cisco UCS C220 M4 and C240 M4 server with 4.1.3h firmware and Qlogic adapter displays the error `remote NDIS compatible device in Ethernet devices`.<br>This issue is resolved. | 4.1(3h)C | 4.0(4n)C |
| CSCvz49048 | In Cisco UCS-IOM-2408, I2C bus corruption error results wrong temperature reading with LED color in Amber though the Fan shows as normal.<br>This issue is resolved. | 4.1(2b)A | 4.0(4n)A |
| CSCvx88769 | In the scenario where Cisco UCS Manager is downgraded from 4.2 to 4.1 or any other previous release version, but if the switch fails to downgrade to the previous release version and gets rebooted, that is, the switch remains at 4.2 version, the user will not be able to login and all the UCS management services will be down.<br>This issue is resolved. | 4.1(3c) | 4.0(4n) |

| Defect ID | Symptom | First Bundle Affected | Resolved in Release |
|---|---|---|---|
| CSCvw24269 | During UCS firmware upgrade, the UCS Manager was unable to download and extract an A-bundle with a size larger than 2 GB and shows the following failure message `Unable to open downloaded image`<br>This issue is resolved. | 4.2(33.329)A | 4.0(4n)A |
| CSCvz45878 | During UCS firmware upgrade, when the UCSM Infrastructure bundle image size exceeds 2 GB, the image size shows 0 KB after download.<br>This issue is resolved. | 4.2(1.39)A | 4.0(4n)A |
| CSCvu77511 | An issue in the Cisco Discovery Protocol (CDP) feature of Cisco FXOS Software and Cisco NX-OS Software can allow an out-of-bounds read condition for certain CDP TLVs, impacting multiple Cisco products. The issue is due to incomplete error checking of the CDP packet header fields.<br>This issue is resolved. | 3.2(3o)C | 4.0(4n)C |

## Resolved Caveats for this Release 4.0(4m)

The following caveats are resolved in Release 4.0(4m):

| Defect ID | Symptom | First Bundle Affected | Resolved in Release |
|---|---|---|---|
| CSCvw64214 | The Azure Stack Hub server failed due to a failure in the QLogic NIC driver.<br>This issue is resolved. | 4.0(4i)C | 4.0(4m)C |
| CSCvx42342 | Correct Port-ID was not inserted in LLDP packets sent to virtual Ethernet.<br>This issue is resolved. | 4.0(4l) | 4.0(4m) |
| CSCvt94075 | On a Cisco UCS blade server with a VIC 6400 series fabric interconnect, IOM discovery failed after chassis decommission/recommission.<br>This issue is resolved. | 4.1(200.18)A | 4.0(4m) |
| CSCvx50196 | On a UCS-managed blade server connected to a Cisco VIC 6400 Series fabric interconnect, configuration of the Smart Call Home could not be modified.<br>This issue is resolved. | 4.0(2b)A | 4.0(4m)A |

| Defect ID | Symptom | First Bundle Affected | Resolved in Release |
|---|---|---|---|
| CSCvy26765 | When the UCS KVM IP assignment was accepted (seen under `Equipment > Chassis x > Server x > Inventory > CIMC > Modify Outband Static Management IP`), a single LLDP packet was sent to neighbor devices with the MGMT TLV containing the recently changed KVM IP instead of the Fabric Interconnect Mgmt IP.<br>This issue is resolved. | 4.1(2b)A | 4.0(4m)A |
| CSCvx50196 | Configuration of the Smart Call Home could not be modified.<br>This issue is resolved. | 4.0(2b)A | 4.0(4m)A |
| CSCvx74585 | A Nexus 9 5K switch became unresponsive in AAA process after multiple login failures.<br>This issue is resolved. | 4.0(4l) | 4.0(4m) |
| CSCvm48433 | The error message `CLI session limit 32 reached. Exiting.` appeared when the **`connect nxos`** command is invoked from the UCS Manager command interface.<br>This issue is resolved. | 4.0(4l)A | 4.0(4m)A |
| CSCvv57606 | When installing a Cisco UCS M5 server attached to a 6400 Series fabric interconnect for the first time, the service profile could fail association and display `Connection Placement Error`.<br>This issue is resolved. | 4.0(4e)A | 4.0(4m)A |
| CSCvx66360 | On a UCS-managed blade server connected to a Cisco VIC 6454 fabric interconnect, an invalid object ID was found in the SNMP traps.<br>This issue is resolved. | 4.0(4b)A | 4.0(4m)A |
| CSCvu87523 | The management interface on Fabric Interconnect B was down and the error was not being cleared<br>This issue is resolved. | 4.0(4h)A | 4.0(4m)A |
| CSCvv91560 | On a UCS Managed B- series server with a Cisco UCS-FI-6248UP fabric interconnect with a 2200 series fabric extender, C-bundle upload failed due to slow SSD and timeout on the fabric interconnect.<br>This issue is resolved. | 4.0(4h)A and B | 4.0(4m)A and B |

| Defect ID | Symptom | First Bundle Affected | Resolved in Release |
|---|---|---|---|
| CSCvw20428 | On a Cisco UCS B480-M5 server with 2x960GB M.2 on PCH controller as RAID 0, the UCS Manager GUI and CLI did not display the correct LUN size.<br>This issue is resolved. | 4.0(4l)A | 4.0(4m)A |
| CSCvw55803 | A Cisco UCS U6454 fabric interconnect rebooted and recovered during normal operation. The system displayed the message:<br>`Last reset at 591270 usecs after Fri Nov 20 13:49:23 2020`<br>`Reason: Kernel Panic`<br>This issue is resolved. | 4.0(4e)A | 4.0(4m)A |
| CSCvr02371 | After upgrading UCS Manager to Release 4.0(4b), passwords for local users where first character of password was a special character did not work.<br>This issue is resolved. | 4.0(4b)A | 4.0(4m)A |

## Resolved Caveats for this Release 4.0(4l)

The following caveats are resolved in Release 4.0(4l):

| Defect ID | Symptom | First Bundle Affected | Resolved in Release |
|---|---|---|---|
| CSCvv58989 | After a management port interface flap on a Cisco UCS 6400 Series fabric interconnect, KVM OOB IPs were sent as the management address towards multiple CDP packet management addresses.<br>This issue is resolved. | 4,1(2,21)A | 4.0(4l)A |
| CSCvw54180 | Cisco UCS 6454 Fabric Interconnects reboot sequentially due to a `policyelem` failure..<br>This issue is resolved. | 4.1(2b)A | 4.0(4l)A |
| CSCvw01292 | A Cisco UCS 6400 Series fabric interconnect rebooted during upgrade and displayed the message `lldp hap reset`.<br>This issue is resolved. | 4.1(1c)A | 4.0(4l)A |
| CSCvw51222 | Cisco UCS M6324 Fabric Interconnects with Micron's M500IT model would reboot after ~3.2 years power-on hours. then reboot every 1.5 months thereafter.<br>This issue is resolved. | 4.0(1a)A | 4.0(4l)A |

| Defect ID | Symptom | First Bundle Affected | Resolved in Release |
|---|---|---|---|
| CSCvw79335 | SNMP timeouts occurred when polling `dot1dTpPortTable` on a Cisco UCS 6332 Fabric Interconnect.<br>This issue is resolved. | 4.0(4e)A | 4.0(4l)A |
| CSCvx01828 | SNMPd becomes unresponsive and SNMP commands on the IP of a Cisco UCS 6454 timed out with no response. Error messages showed messages like the following.<br>`[12679086.760577] [sap 28][pid 15470][comm:snmpd] WARNING: possible memory leak is detected on pers queue (len=729,bytes=208265168) - kernel`<br>This issue is resolved. | 4.0(4i)A | 4.0(4l)A |
| CSCvw23303 | Old internal IPs were not cleared correctly on the IOMs when migrating from Cisco UCS 2200 and 2300 series Fabric Interconnects to 6400 Series Fabric Interconnects.<br>This issue is resolved. | 4.0(4k)A | 4.0(4l)A |
| CSCvv26230 | After upgrade of firmware to version 4.1(1x), chassis is reporting that the health LED and connection LED are OFF even though the chassis and hardware components within the chassis are in the working condition.<br>This issue is resolved. | 4.0(1b)A | 4.0(4l)A |
| CSCvw73506 | Failure of module 3 in a Cisco UCS 6296 Fabric Interconnect resulted in the ASIC error:`show hardware internal sunny counters interrupts all`.<br>This issue is resolved. | 4.0(4h)A | 4.1(2c)A |
| CSCvq17291 | For Cisco UCS 6200 Series fabric interconnects, you can now run the e2fsck command with reboot option. | 4.0(4i)A | 4.0(4l)A |
| CSCvw93034 | The original firmware shipped with Cisco UCS 6300 Series Fabric Interconnects caused the SSD to become unresponsive after a certain threshhold of power-on hours, until the system was rebooted.<br>This issue is now resolved. | 4.0(4k)A | 4.0(4l)A |

| Defect ID | Symptom | First Bundle Affected | Resolved in Release |
|---|---|---|---|
| CSCvx18169 | In Cisco UCS 6248UP Fabric Interconnects, fans were not detected by the switch, even though the fans were present in the system and spinning. Messages like the following were displayed and the switch shut down even though the fans are present and spinning.<br>`2021 Jan 27 15:02:33 FLEXUCS01-B %$ VDC-1 %$ %NOHMS-2-NOHMS_ENV_ERR_FAN_DOWN: System minor alarm on fans: One fan missing or failed`<br>`2021 Jan 27 15:02:33 FLEXUCS01-B %$ VDC-1 %$ %CALLHOME-2-EVENT: FAN_FAILURE`<br>`2021 Jan 27 15:02:33 FLEXUCS01-B %$ VDC-1 %$ %PFMA-2-PFMA_FAN_REMOVED: Fan module 2 UCS-FAN-6248UP removed`<br>`2021 Jan 27 15:02:34 FLEXUCS01-B %$ VDC-1 %$ %CALLHOME-2-EVENT: HARDWARE_REMOVAL`<br>This issue is now resolved. | 3.2(3o)A | 4.0(4l)A |
| CSCvv36591 | The Cisco UCS KVM Console could not be accessed from the Cisco UCS KVM Direct login, but only by going through the Cisco UCS Manager link to KVM. | 4.0(4g)A and B | 4.0(4l)A and B |

## Resolved Caveats for this Release 4.0(4k)

The following caveats are resolved in Release 4.0(4k):

| Defect ID | Symptom | First Bundle Affected | Resolved in Release |
|---|---|---|---|
| CSCvu10837<br>CSCvu23828 | A UCS managed Cisco UCS C240 M5 rack server failed to complete discovery and showed the following error messages.<br>• In the rsdAG logs: `Error getting chassis inventory, details: ERROR: Error adding TLV`<br>• In the PortAG logs: `Error getting chassis inventory, details: ERROR: Error adding TLV`<br>This issue is now resolved. | 4.0(4g) | 4.0(4k) |

| Defect ID | Symptom | First Bundle Affected | Resolved in Release |
|---|---|---|---|
| CSCvu79969 | A Cisco UCS B200 M4 server running ESXi 6.5 reported a `P2_TEMP_SENS` alarms even though no `P2_TEMP_SENS` alarms could be found.<br>This issue is resolved. | 4.0(1a)B | 4.0(4k)B |
| CSCvp99161 | When SFP-H25G-CU5M cable is used between Cisco VIC 1455/1457 adapters using a VIC firmware version lower than 5.1(2a) and 6400 series FI or N9K, signals may not be correctly reported.<br>This issue is resolved. | 4.0(1a) | 4.0(4k) |
| CSCvu03323 | A reboot of a Cisco UCS 6454 Fabric Interconnect resulted in loss of all the SAN and LAN traffic to the directly attached Cisco UCS B Series and C series servers.<br>This issue is resolved. | 4.0(4h)B and C | 4.0(4k)B and C |
| CSCvp07587 | On Cisco UCS B Series servers using Cisco UCS 2400 Series Fabric Interconnects, all fans were marked as inoperable due to a I2C bus issue.<br>This issue is now resolved. | 4.0(4h)A | 4.0(4k)A |
| CSCvt35661 | Cisco UCS 3260 Blade servers connected via FEX lost connectivity due to incomplete port configuration on upgrade.<br>This issue is now resolved. | 4.0(4g) | 4.0(4k) |
| CSCvu25519 | For Cisco UCS C Series Rack Servers with VIC 1400 Series adapters, discovery would stop at 0% and response slowed in both Cisco UCS Manager GUI and CLI interfaces.<br>This issue is now resolved. | 4.0(4g)<br>A and C | 4.0(4k) |
| CSCvt27869 | In rare situations, on Cisco UCS 6200 Series Fabric Interconnects, the data sent from IOM was corrupted.<br>This issue is now resolved. | 2.2(8f)A | 4.0(4k)A |
| CSCvp46152 | An MCM core dump with signal failure.caused a Cisco UCS 6332 Fabric Interconnect to reload. | 4.0(2a)A | 4.0(4k) |
| CSCvu25233 | A Cisco UCS 6400 Fabric Interconnect connected to a VIC 1455/1457 using SFP-H25G-CU3M or SFP-H25G-CU5M or a VIC 1455/1457 connected to 2232PP using SFP-10GB-CUxM cable experienced link flaps.<br>This issue is now resolved. | 4.0(1a) | 4.0(4k) |

| Defect ID | Symptom | First Bundle Affected | Resolved in Release |
|---|---|---|---|
| CSCvh30116 | When a hot plug drive is replaced due to RAID 0 drive failure, the virtual drive is now re-initialized to automatically bring the failed RAID 0 back online. | 3.1(2b)A | 4.0(4k) |
| CSCvu52479 | A Cisco UCS 6454 Fabric Interconnect was rebooted due to an nbproxy process crash, resulting in loss of all the SAN and LAN traffic to the directly attached C Series rack and B Series blade servers.<br>This issue is resolved. | 4.0(4e)A | 4.0(4k)A |
| CSCvr95393 | A remote user was able to login to Cisco UCS Manager even when the Role policy was set to **No Login**.<br>This issue is now resolved. | 4.0(4e)A | 4.0(4k)A |
| CSCvp75416 | Using ssh keys for authentication to UCS Manager no longer causes a buffer overflow. | 4.0(1b)A | 4.0(4k)A |
| CSCvt35015 | When filesystem health was checked with **`debugfs -R show_super_stats`**, it would only check for and log `not clean` status.<br>It now logs `clean with errors` conditions as well. | 4.0(4g)A | 4.0(4k)A |
| CSCvt35661 | After upgrade of Cisco UCS Infrastructure from release 4.0(4e) to release 4.0(4g), fabric extender (FEX) ports connected to System I/O Controller (SIOC) of Cisco UCS S3260 Storage server remained in the administratively down state with incomplete configuration. Hence, the Cisco UCS S3260 Storage Server cannot be discovered.<br>This issue is now resolved. | 4.0(4g)A | 4.0(4k)A |
| CSCuy05744 | A Cisco UCS B260/B460 blade server using V2 CPUs (UCSB-EX-M4-1) displayed a voltage threshhold warning.<br>The threshold for UCSB-EX-M4-1 has now been changed. | 4.0(4i)B | 4.0(4k)B |
| CSCvs72258 | After changing the Best Effort weight or MTU value in the Cisco UCS Manager QOS configuration on Cisco UCS 6332 Fabric Interconnect, an unexpected extended storage traffic disruption was experienced.<br>This issue is resolved. | 4.0(4c)A | 4.0(4k)A |

| Defect ID | Symptom | First Bundle Affected | Resolved in Release |
|---|---|---|---|
| CSCvt76668 | Cisco UCS S3260 storage servers equipped with SAS expander fail to upgrade the expander and report it as inoperable.<br>This issue is resolved. | 4.0(4h) | 4.0(4k) |
| CSCvr04665 | When SFP-H25G-CU5M cable is used between VIC 1455/1457 adaptors with a VIC firmware version lower than 5.1(2a) and 6400 series fabric interconnects, the link between the adaptor and the 6400 Series fabric interconnect could fail.<br>This issue is resolved. | 4.0(1a) | 4.0(4k) |
| CSCvv80576 | On a UCS Managed B or C Series server or UCS Mini connected to either 6200 Series or 6300 Series Fabric Interconnects, after a vNIC fail-over, traffic did not switch to the second Fabric Interconnect, resulting in dropped traffic. Servers with 6400 Series Fabric Interconnects were not affected.<br>This issue is resolved. | 4.0(4i)A<br>3.2(3o)A | 4.0(4k)A |
| CSCvv55541 | On C240 M4 C Series and C220 M4 C Series servers running Azure Stack on Windows 2019, UCS Manager was booting into the Bitlock Recovery screen.<br>This issue is resolved for the C240 M4 and C220 M4 servers. | 4.0(2c)C | 4.0(4k)C |
| CSCvq17291 | During the reboot of Cisco UCS 6200 and 6300 Series Fabric Interconnects, you can run the e2fsck command to clean up the file systems. | 4.0(3)A | 4.0(4k)A |

## Resolved Caveats in Release 4.0(4i)

The following caveats are resolved in Release 4.0(4i):

| Defect ID | Symptom | First Bundle Affected | Resolved in Release |
|---|---|---|---|
| CSCvt55829 | SanDisk Lightning II Solid State Drives (SSDs) LT0400MO and LT1600MO with respect to PIDS listed below, report 0 GB of available storage space remaining under normal operation at 40,000 power on hours. SSDs go offline and become unusable after power cycle event resulting in data loss, potentially on multiple drives if they are placed in service at the same time.<br>The PIDs of affected SSDs are:<br>• (400GB) UCS-SD400G1KHY-EP, UCS-SD400G12S4-EP, UCS-C3X60-12G240<br>• (1.6TB) UCS-SD16TG1KHY-EP, UCS-SD16TB12S4-EP, UCS-C3X60-12G2160<br>This issue is resolved. | 3.2(1d)C | 4.0(4i)C |
| CSCvt37895 | Cisco C-series integrated server that is connected to Fabric Interconnect through Fabric extender, encounters fabric ports link flaps during cluster failover or shallow discovery.<br>This issue is resolved. | 4.0(4e)A | 4.0(4i)A |
| CSCvq80554 | On Cisco Model M4 servers, the BMC failed to send notification of HCL file change.<br>This issue is resolved. | 4.0(1c)A | 4.0(4i)A |
| CSCvs61735 | UCS Manager didn't provide correct overall status for the IOM on a Cisco 6400 Series Fabric Interconnect.<br>This issue is resolved. | 4.0(1a)A | 4.0(4i)A |
| CSCvm59040 | Loss of network connectivity due to running out of memory after an uptime of over 180 days was sometimes encountered on hosts on Cisco standalone C-Series servers equipped with a VIC 1225 adapter.<br>This issue is resolved. | 4.0(1a)B and C | 4.0(4i)B and C |
| CSCvt27869 | A 6200 series Fabric Interconnect encountered an OOB memory access causing the Fabric Interconnect to reboot.<br>This issue is resolved. | 4.0(1a)A | 4.0(4i)A |

| Defect ID | Symptom | First Bundle Affected | Resolved in Release |
|---|---|---|---|
| CSCvt08435 | On the 6300 Series Fabric Interconnect, while monitoring SNMP on IOM 2304, HIF ports counts intermittently dropped to zero, causing high traffic indications on the third party monitoring applications. | 4.0(4b)A | 4.0(4i)A |
| CSCvu07675 | Auto-install of firmware on a UCS-managed integrated C-Series rack server failed to activate the SAS Controller. | 4.0(4b)C | 4.0(4i)C |
| CSCvt65210 | On a 1400 Series Fabric Interconnect, vif_vifid_reserve failed during the uplink port flap. | 4.0(4h)A | 4.0(4i)A |
| CSCvs46320 | UCS servers connected to 6400 Fabric Interconnects may lose synchronization with the time and/or timezone set in UCS Manager. | 4.0(1a)A | 4.0(4i)A |
| CSCvu14656 | On upgrade of BIOS to one of the following versions, the booting of M5 servers get stuck at the memory testing step:<br>• C220M5.4.1.1c.0.0404202345<br>• C240M5.4.1.1c.0.0405200025<br>• B200M5.4.1.1c.0.0404202345 | 4.0(4h)C | 4.0(4i)C |
| CSCvu16418 | On Cisco UCS 6400 Series Fabric Interconnect running with Cisco UCS Manager 4.0(4g) firmware, UCS fibre channel (FC) ports can stay online when upstream MDS experiences a Kernel panic. Depending on configuration, this situation can cause UCS FC uplinks to stay online even though MDS is inoperable. Thereby, causing pinned vHBAs to stay up which leads to the OS being unaware that FC interfaces are not functioning properly.<br>This issue is resolved. | 4.0(4g)A | 4.0(4i)A |
| CSCvt29474 | On Cisco UCS 6332-16UP Fabric Interconnect (FI) in switched mode direct attached to a Fibre Channel (FC) storage unit, a large number of link reset (LR) or link reset response (LRR) in FC interface can make any FI link to become unusable.<br>This issue is resolved. | 4.0(2a)A | 4.0(4i)A |

| Defect ID | Symptom | First Bundle Affected | Resolved in Release |
|---|---|---|---|
| CSCvt44506 | Cisco UCS Manager receives multiple delta events for Graphics Processing Units (GPU) card.<br>This issue is resolved. | 4.0(4h)C | 4.0(4i)C |
| CSCvs35747 | In rare situations, during loss of FC Uplink connectivity and credit on 6300 series Fabric Interconnect, the key information such as port/link/speed FSM information needed for troubleshooting in the FC port may be lost.<br>The logging of FC port issues is enhanced to display the port/link/speed FSM information in the fc-mac output. | 4.0(1b)A | 4.0(4i)A |
| CSCvt38091 | After upgrading to Cisco UCS Manager release 4.0(4e), a B200-M5 blade server displayed messages similar to the following:<br>`Model UCS-FI-6332-16UP with Host Name (host name) reported following Diagnostics test failure:`<br>`'Recovered : Server 1/6 (service profile: (profile name) inaccessible'`<br>This issue is resolved. | 4.0(4e)B | 4.0(4i)B |
| CSCvs97236 | When an C460 M4 C-Series Rack Server detects an uncorrectable ECC error during Patrol Scrub, it logs a truncated system address (4KB page boundary) to the Machine Check Banks. When the iMC Demand Scrubber detects an Uncorrectable ECC error, it logs the full 'cache line' (non-truncated) address to the Machine Check Banks.<br>This truncated memory address is used to forward translate the address to a physical DIMM. Depending on system population and configuration, it is possible that the SEL message logging the Uncorrectable ECC error will not point to the correct DIMM.<br>This issue is resolved.<br>Uncorrectable ECC errors detected during Demand scrub are correctly translated to physical DIMM. | 4.0(4h)C | 4.0(4i)C |

| Defect ID | Symptom | First Bundle Affected | Resolved in Release |
|---|---|---|---|
| CSCvs73313 | On a prolonged usage of Cisco UCS M5 servers, the bladeAG process could crash and customer may observe a shallow discovery triggered on the servers.This condition is seen due to the internal memory leakage.<br>This issue is resolved. | 4.0(4a)A | 4.0(4i)A |
| CSCvt64871 | In rare situations, Cisco UCS C480 M5 servers and Cisco UCS 480 M5 ML servers stop responding and reboot after ADDDC virtual lockstep is activated. This results in #IERR and M2M timeout in the memory system.<br>For more information, see:<br>• Intel® Xeon® Processor Scalable FamilySpecification Update (Errata > SKX108)<br>• Second Generation Intel® Xeon® Scalable Processors Specification Update (Errata > CLX37) | 4.0(4c)B | 4.0(4i)B |
| CSCvu11155 | On upgrade of BIOS to one of the following versions, you might experience performance degradation on Cisco UCS B-Series, C-series, and S- series M5 servers running with second Generation Intel® Xeon® Scalable Processors:<br>• C240M5.4.0.4r.0.0305200743<br>• C220M5.4.0.4p.0.0224200755<br>• B200M5.4.0.4l.0.0305202307<br>• B480M5.4.0.4m.0.0305202307<br>• S3X60M5.4.0.4o.0.0224200755 | 4.0(4h)B and C | 4.0(4i)B and C |
| CSCvq53066 | During auto-upgrade of firmware from Cisco UCS Manager 4.0(2d) to Cisco UCS Manager 4.0(4b), the SAS controller firmware is not activated on an integrated rack server. | 4.0(4b) | 4.0(4i) |

## Resolved Caveats in Release 4.0(4h)

The following caveats are resolved in Release 4.0(4h):

| Defect ID | Symptom | First Bundle Affected | Resolved in Release |
|---|---|---|---|
| CSCvr83759 | After upgrading from UCS Manager 3.2(3c) to 4.0(4c), blade server access to UCS Manager Fabric Interconnects fails when using openSSH or SecureCRT with "password" authentication.<br>This issue is resolved. | 4.0(1a)A | 4.0(4h)A |
| CSCvr98210 | When upgrading from Cisco UCS Manager Release 3.2 to Release 4.0 on a system with appliance ports or FCoE storage ports, LLDP becomes disabled by default. FCoE or any connectivity that requires LLDP may stop working.<br>This issue is resolved. | 4.0(4b)<br>A | 4.0(4h)A |
| CSCvr91399 | The following BIOS tokens were reset to Platform Default when they were pushed from Cisco UCS Central to UCS Manager.<br>SelectMemoryRASConfiguration<br>LocalX2Apic<br>BMEDMAMitigation<br>This issue is resolved. | 4.0(1a)A | 4.0(4h)A |
| CSCvq76790 | After firmware upgrade of Cisco IMC or Fabric Interconnect, the connectivity between Cisco IMC and Fabric Interconnect is lost due to a Physical Layer 1 issue or misconfiguration of port mode on the Fibre Channel port.<br>This issue is resolved. | 4.0(2b)A | 4.0(4h)A |
| CSCvr74792 | Cisco UCS 6454 Fabric Interconnect running with Cisco UCS Manager Release 4.0(2d), is rebooted due to kernel panic and watchdog timer timeout caused by a PSU FAN data access causing a kernel spin lock.<br>This issue is resolved. | 4.0(1a)A | 4.0(4h)A |
| CSCvr95365 | After firmware upgrade from Cisco UCS Manager Release 4.0(1a) to Release 4.0(4b), discovery of a Cisco UCS C240 M5 server that is equipped with a Cisco 12G Modular SAS HBA controller failed with the error:<br>`mc_attrib_set_suboem_id failed to set the SubOEM ID`<br>This issue is resolved. | 4.0(4a)C | 4.0(4h)A |

| Defect ID | Symptom | First Bundle Affected | Resolved in Release |
|---|---|---|---|
| CSCvp71363 | In a system where a UCS C240 M5 server with a VIC 1457 adapter is managed by Cisco UCS Manager through a direct connect integration with UCS Fabric Interconnects, the following fault is displayed on unused or unconnected ports:<br>`Adapter uplink interface x/y/z link state: unavailable. Please verify connectivity to Fabric Interconnect. Acknowledging FEX might be required.`<br>This issue is resolved. | 4.0(2d)A | 4.0(4h)A |
| CSCvr15733 | Under load, Cisco vNIC 1400 Series running with UCSC-MLOM-C25Q-04 version 4.0(4b) is stalled permanently due to known issues with the rate limit shutoff.<br>This issue is resolved. | 4.0(1a)B | 4.0(4h)A |
| CSCvs35789 | When there is a failover in UCS 6454 Fabric Interconnect, the HIF ports are down, causing the traffic to disrupt for some time. Hence, fabric interconnect reboot takes more time to regain connectivity.<br>The average delay has been reduced. | 4.0(4c)A | 4.0(4h)A |
| CSCvs63073 | While running QoS script, Cisco UCS 6400 Series Fabric Interconnects crashed due to system watchdog timeout which is occurred on spinlock situation.<br>The spinlock condition that led to system watchdog timeout is resolved. | 4.0(1a)A | 4.0(4h)A |
| CSCvr46327 | When replacing a UCS 2208 IOM with a UCS 2408 IOM, virtual ethernet interfaces became unavailable. Virtual Ethernet interfaces are not available in the output of the `show interface virtual` status command, but are available in the output of the `show interface brief` command in NXOS.<br>This issue is resolved. | 4.0(4d)A | 4.0(4h)A |

| Defect ID | Symptom | First Bundle Affected | Resolved in Release |
|---|---|---|---|
| CSCvs51200 | On Cisco UCS C-Series M5 servers, UEFU boot LUNs become non-functional under the following conditions:<br>• When the OS is ESXi release 6.0 update 3 or 6.5 update 1<br>• When IQN is defined at the profile level<br>• When at least one iSCSI vNIC is configured in boot with more than one target<br>This issue is resolved. | 4.0(4f)A | 4.0(4h)A |
| CSCvr79388 | In rare situations, Cisco UCS Intel® processor based M5 servers stop responding and reboot after ADDDC virtual lockstep is activated. This results in #IERR and M2M timeout in the memory system.<br>For more information, see:<br>• Intel® Xeon® Processor Scalable FamilySpecification Update (Errata > SKX108)<br>• Second Generation Intel® Xeon® Scalable Processors Specification Update(Errata > CLX37)<br>**Note** This issue still persist in Cisco UCS C480 M5 and Cisco UCS 480 M5 ML servers. For more information, see CSCvt64871 in the Open Caveats for Release 4.0(4h) section. | 4.0(4c)B | 4.0(4h)B |
| CSCvr79396 | On Cisco UCS M5 servers, the Virtual lock step (VLS) sparing copy finishes early, leading to incorrect values in the lock step region .<br>This issue is resolved. | 4.0(4e)B | 4.0(4h)B |

| Defect ID | Symptom | First Bundle Affected | Resolved in Release |
|---|---|---|---|
| CSCvs25524 | On Cisco UCS 6300 Series Fabric Interconnect, as the VDC debug logs keep filling up the temp directory, the following message has appeared in the console logs:<br>`FI6332-DC3-A %SYSMGR-2-TMP_DIR_FULL: System temporary directory usage is unexpectedly high at 80%.`<br>This issue is resolved. | 4.0(4b)A | 4.0(4h)A |
| CSCvs88880 | When standalone Cisco IMC or Cisco UCS Manager managed C-series server is rebooted while the Cisco VIC 1455/1457/1495/1497 adapter is still powered On:<br>• Cisco IMC may not be able to manage the VIC adapters and display/modify the adapter configuration.<br>• Cisco UCS Manager may lost connectivity with Cisco IMC when the Cisco VIC 1455/1457/1495/1497 adapter is used to provide connectivity between Cisco IMC and Cisco UCSM. | 4.0(1a) | 4.0(4h)A |
| CSCvr70687 | New Cisco UCS C240 M5 server discovery fails or does not respond with the following error message:<br>`CimcVMedia Error: Error retrieving vmedia attributes list-MC Error(-6)`<br>The same issue may occur for any Cisco UCS C240 M5 server after an FI reboot or upgrade.<br>This issue is resolved. | 4.0(4d)A | 4.0(4h)A |

## Resolved Caveats in Release 4.0(4g)

The following caveats are resolved in Release 4.0(4g):

| Defect ID | Symptom | First Bundle Affected | Resolved in Release |
|---|---|---|---|
| CSCvr43466 | Cisco UCS Manager integrated Cisco UCS B-Series and C-Series M5 servers reported the following hardware inventory mismatch fault even though the hardware had not changed: `hardware inventory mismatch`<br>This issue is resolved. | 4.0(4b)B | 4.0(4g)B |
| CSCvr67027 | When upgrading Red Hat Linux on a Cisco UCS Manager integrated S3260 M4 rack server with UCS-C3K-M4RAID RAID controller running driver 07.702.06.00-rh2, the boot drive becomes inoperable.<br>This issue is resolved. | 3.2(3k)C | 4.0(4g)C |
| CSCvo49554 | When a blade server is connected to ports 27-32 on a UCS 6332 Fabric Interconnect, or ports 35-40 on a UCS 6332-16UP Fabric Interconnect, numerous pings are lost during Fabric Interconnect reboot.<br>This issue is resolved. | 4.0(1a)A | 4.0(4g)A |
| CSCvj70519 | Port 7162, available only if only if registered with UCS Central, was open on 6400 Series Fabric Interconnects. This port is now closed. | 4.0(1a)A | 4.0(4g)A |
| CSCvs25058 | UCS 6454 Fabric Interconnect could not switch traffic between a pair of servers that were discovered after the 31st locally connected UCS rack servers when the respective vNIC of the server used an identical vntag. This resulted in servers discovered later not being able to communicate with each other if the vNICs that were communicating had same vntag. Only traffic that was switched in-fabric, such as between vNICs pinned on the Fabric Interconnect, was affected.<br>This issue is resolved. | 4.0(4f)A | 4.0(4g)A |
| CSCvr06387 | The SNMP process on the UCS 6324 Fabric Interconnect crashed repeatedly.<br>This issue is resolved. | 4.0(1a)A | 4.0(4g)A |

| Defect ID | Symptom | First Bundle Affected | Resolved in Release |
|---|---|---|---|
| CSCvq37888 | On UCS M4 blade servers, connectivity between Cisco UCS Manager and the Cisco IMC was lost when the Cisco IMC ran out of memory. Connectivity could not be restored until the blade server was re-seated.<br>This issue is resolved. | 4.0(1a)B and C | 4.0(4g)B and C |
| CSCvr78701 | Cisco UCS Manager integrated C220 M5 rack servers experienced a Cisco IMC kernel panic during Cisco UCS Manager activation.<br>This issue is resolved. | 4.0(4c)C | 4.0(4g)C |

## Resolved Caveats in Release 4.0(4f)

The following caveats are resolved in Release 4.0(4f):

| Defect ID | Symptom | First Bundle Affected | Resolved in Release |
|---|---|---|---|
| CSCvr01259 | With a UCS 6400 Series Fabric Interconnect connected to a UCS 2408, the HIF port interface counters were not updated on the Fabric Interconnect, even though the virtual ethernet scounters showed the correct packet count.<br>This issue is resolved. | 4.0(4e)A | 4.0(4f)A |
| CSCvq92352 | In the very rare circumstance when a message with a corrupted length field from an attached FEX was received by the Fabric Interconnect `fwm` process, a Fabric Interconnect reboot was triggered.<br>This issue is resolved. | 2.2(8f)A | 4.0(4f)A |
| CSCvq57262 | During an A-bundle upgrade of a UCS 6454 Fabric Interconnect with RDMA enabled, one of the rack servers showed a pending reboot acknowledgement.<br>This issue is resolved. | 4.0(4b)A | 4.0(4f)A |
| CSCvp52336 | A UCS 6454 Fabric Interconnect was unable to receive the DHCP IP address during initial setup.<br>This issue is resolved. | 4.0(2d)A | 4.0(4f)A |

| Defect ID | Symptom | First Bundle Affected | Resolved in Release |
|---|---|---|---|
| CSCvq51008 | UCS B460 M4 blade servers on a single adapter could not find an adapter to place the vCon. This prevented association and displayed the error message `configuration failed due to insufficient-resources,connection-placement`.<br>This issue is resolved. | 4.0(4b)A and B | 4.0(4f)A and B |
| CSCvr35735 | UCS 6454 Fabric Interconnects were not able to switch traffic between a pair of UCS rack servers when vNICs were pinned to the Fabric Interconnect.<br>This issue is now resolved. | 4.0(4b)A | 4.0(4f)A |
| CSCvq98090 | SAN paths on UCS 6454 Fabric Interconnects went offline when the Fabric Interconnect was power-cycled.<br>This issue is now resolved. | 4.0(4b)A | 4.0(4f)A |
| CSCvr47266 | During migration from a UCS 6248 Fabric Interconnect to a UCS 6454 Fabric Interconnect,UCS 2208 IOMs silently failed.<br>This issue is now resolved. | 4.0(4b)A | 4.0(4f)A |
| CSCvr34407 | UCS 6300 Series Fabric Interconnects on UCS M4 and M5 rack servers lost their VLAN configuration after an enable/disable operation from Cisco UCS Manager.<br>This issue is now resolved. | 4.0(4b)A | 4.0(4f)A |
| CSCvq90219 | Cisco UCS Manager activation failed on a blade server with UCS 6200 Series Fabric Interconnects during manual upgrade from Cisco UCS Manager 3.2(3k) to Cisco UCS Manager 4.0(4d).<br>This issue is now resolved. | 4.0(4d)A | 4.0(4f)A |
| CSCvr40744 | Port 5661 on a UCS 6454 Fabric Interconnect was open.<br>Port 5661 is now disabled. | 4.0(4d)A | 4.0(4f)A |

| Defect ID | Symptom | First Bundle Affected | Resolved in Release |
|---|---|---|---|
| CSCvr67352 | The management instance on blade and rack servers with UCS 6454 Fabric Interconnects lost access to the OOB KVM connection under specific conditions, such as if the IO Module or FEX was rebooted or one of the Fabric Interconnects became unreachable.<br>This issue is now resolved. | 4.0(4e)A | 4.0(4f)A |
| CSCvn49417 | When powering on a UCS 6454 Fabric Interconnect and booting to the initial configuration dialog screen, the network uplinks came online prematurely and may have caused a broadcast storm in rare instances.<br>This issue is now resolved. | 4.0(1a)A | 4.0(4f)A |
| CSCvr68316 | In a standalone C-Series server, when a UCS VIC 1455/1457 adapter was connected to a switch with port-channel enabled on both the VIC and switch side, the Ethernet and Fibre Channel data paths did not work. | 4.0(4e)C | 4.0(4f)C |

## Resolved Caveats in Release 4.0(4e)

The following caveats are resolved in Release 4.0(4e):

| Defect ID | Symptom | First Bundle Affected | Resolved in Release |
|---|---|---|---|
| CSCvh87378 | Servers in the community VLAN were not able to communicate with the primary VLAN after upgrade to Cisco UCS Manager Release 3.2.(2b) or later releases when the server on the primary VLAN is in the UCS Domain.<br>This issue is resolved. | 3.2(2b)A | 4.0(4e)A |
| CSCvr08327 | PSUs on blade chassis that were using UCS 2204 or UCS 2208 Fabric Extenders were shut down by thermal faults during Fabric Extender firmware upgrade. The PSUs could not be powered on afterwards until they were reseated.<br>This issue is resolved. | 4.0(1d)B | 4.0(4e)B |
| CSCvq43680 | The Fabric Interconnect randomly rebooted due to FCPC High Availability Policy (HAP) reset.<br>This issue is resolved. | 4.0(2b)A | 4.0(4e)A |

| Defect ID | Symptom | First Bundle Affected | Resolved in Release |
|---|---|---|---|
| CSCvq71404 | Access of direct KVM IP for blade and rack servers with 6400 Series Fabric Interconnects were redirecting to the Cisco UCS Manager Domain.<br>This issue is resolved. | 4.0(2d)A | 4.0(4e)A |
| CSCvp45607 | When a Cisco UCS Manager user selected **Show Current User's Activities** and then **Acknowledge All** they could reboot all servers with a pending reboot from all users without understanding the full impact.<br>Selecting **Acknowledge All** now automatically deactivates **Show Current User's Activities** to ensure full visibility of the reboot impacts. | 3.2(3e)A | 4.0(4e)A |
| CSCvr11045 | TCP ports 81 and 743 were accessible on UCS 6454 Fabric Interconnects when Cisco IMC Web service was disabled.<br>This issue is resolved. | 4.0(4b)A | 4.0(4e)A |
| CSCvr07248 | In the Cisco UCS Manager GUI, navigating to **Equipment** > **Policies** > **Power Groups** showed information only on the **General** tab. The tabs for **Chassis**, **Rack Unit**, **FEX**, **FI**, **Faults**, and **Events** did not display information.<br>This issue is resolved. | 4.0(4a)A | 4.0(4e)A |
| CSCvq82024 | When the BIOS menu setup item "AEP Error Injection" was enabled, an error was injected to the Persistent Memory device, causing an erroneous purple screen of death (PSOD) generation. The Operating System was not notified and hence, the machine check exception (MCE) was not properly handled.<br>This issue is resolved. | 4.0(4b)B | 4.0(4e)B |

| Defect ID | Symptom | First Bundle Affected | Resolved in Release |
|---|---|---|---|
| CSCvr04369 | Under rare and specific conditions, the link status of the Ethernet port of a Cisco UCS 14xx adapter card, and of the attached switch port, failed to come up multiple times. This was due to due to poor quality of the analog electrical signal received by Ethernet SERDES component of the VIC adapter, in the configurations which do not use the Ethernet Link-Training protocol. This issue occurred when the following conditions were present:<br>• Cisco VIC 14xx adapter card instance and port instance:<br>• Cisco UCS VIC 1455<br>• Cisco UCS VIC 1457<br>• Cisco UCS VIC 1495<br>• Cisco UCS VIC 1497<br>• Transceiver module instances that do not use the Ethernet Auto-Negotiation protocol:<br>• 10G CU<br>• 10G Optical<br>• 25G CU<br>• 25G Optical<br>• 40G Optical<br>• 100G Optical<br>• Other possible environmental conditions.<br>This issue is resolved. | 4.0(4a)C | 4.0(4e)C |
| CSCvn77341 | Namespaces created under Red Hat Enterprise Linux 7.6 by using the in-box ndctl tool, were showing "Critical" health state when examined in the BIOS Setup or the UEFI IPMCTL tool, even though the namespaces were healthy.<br>This issue is resolved. | 4.0(4a)B and C | 4.0(4e)B and C |

| Defect ID | Symptom | First Bundle Affected | Resolved in Release |
|---|---|---|---|
| CSCvn81521 | On systems with Intel[®] Optane[™] Data Center persistent memory modules in 2LM (memory mode), uncorrectable errors were logged on the persistent memory modules when errors occurred on DDR4 DIMMs (configured as near memory) on the same channel.<br>This issue is resolved. | 4.0(4a)B and C | 4.0(4e)B and C |

## Resolved Caveats in Release 4.0(4d)

The following caveats are resolved in Release 4.0(4d):

| Defect ID | Symptom | First Bundle Affected | Resolved in Release |
|---|---|---|---|
| CSCvq26156 | Upgrade of UCS C-Series servers to 4.0(4c) C-Bundle caused the Cisco 12G Modular SAS HBA to stop discovering/communicating with some Intel S4500 disk drives. This could result in failure of the software upgrade of these drives.<br>This issue has been resolved.<br>**Note** Cisco HyperFlex does not support UCS Manager 4.0(4a), 4.0(4b) or 4.0(4c). | 4.0(4a)C | 4.0(4d)A |
| CSCvq38756 | In rare cases, with NIC teaming configuration on a UCS Cluster, transient traffic loss occurred when the Fabric Interconnect reloaded.<br>This issue has been resolved. | 4.0(4b) A | 4.0(4d)A |
| CSCvq84120 | After Fabric Interconnect reboot, vNICs sometimes failed over prematurely, resulting in intermittant traffic loss.<br>This issue has been resolved. | 4.0(4b) A | 4.0(4d)A |

## Resolved Caveats in Release 4.0(4c)

The following caveats are resolved in Release 4.0(4c):

| Defect ID | Symptom | First Bundle Affected | Resolved in Release |
|---|---|---|---|
| CSCvp31766 | When upgrading blade servers, the VMs that were using VM-FEX interfaces lost connectivity.<br>This issue has been resolved. | 4.0(4a)B | 4.0(4c)B |

| Defect ID | Symptom | First Bundle Affected | Resolved in Release |
|---|---|---|---|
| CSCvo99427 | When upgrading Cisco UCS Central to Release 2.0(1h), visibility to some UCS domains was lost. When running a connectivity test from Cisco UCS Central to the Cisco UCS Manager domains that lost visibility, the connection was successful but showed a warning message.<br>This issue has been resolved. | 4.0(4a) C | 4.0(4c)A |
| CSCvp89594 | One side of the UCS 6454 Fabric Interconnect became unresponsive while connecting and was unable to connect to NX-OS while in an ssh session.<br>This issue has been resolved. | 3.2(1d)A | 4.0(4c)A |
| CSCvo06391 | UCS C125 M5 and C480 M5 server discovery failed at "Discover Bmc Preconfig Pnu OS Peer".<br>The Ethernet interfaces of the UCS VIC adapter showed physical link status as down or Ethernet PCS protocol errors.<br>This issue has been resolved. | 4.0(4a)A | 4.0(4c)A |
| CSCvo18110 | Fibre Channel NVMe interface paths to namespaces that undergo link flaps were lost.<br>This issue has been resolved. | 4.0(4a)A | 4.0(4c)A |
| CSCvq28261 | PSUs on blade chassis that were using UCS 2304 Fabric Extender with UCS 6324 Fabric Interconnect were shut down by thermal faults during Fabric Extender firmware upgrade. The PSUs could not be powered on afterwards until they were reseated.<br>This issue has been resolved. | 4.0(1d)B | 4.0(4c)B |
| CSCvo48003 | On M4 servers, an uncorrectable ECC error was detected during Patrol Scrub. When the CPU IMC (Integrated Memory Controller) Patrol Scrubber detects an uncorrectable ECC error, it logs a truncated DIMM address (4KB page boundary) to the Machine Check Banks<br>This issue has been resolved. | 4.0(4a) B | 4.0(4c) B |
| CSCvp31749 | BMC CPU temperatures thresholds (IPMI) will now adjust when Intel Speed Select configurations are changed. | 4.0(4a)B | 4.0(4c)B |

| Defect ID | Symptom | First Bundle Affected | Resolved in Release |
|---|---|---|---|
| CSCvo32597 | Cisco UCS Manager was not receiving correct sensor readings from the IOM for the Platinum II AC Power Supply for the UCS 5108 chassis.<br>This issue has been resolved. | 4.0(4b)B | 4.0(4c)B |
| CSCvq17624 | The old power supply unit (PSU) data was not cleared from Cisco UCS Manager when a PSU was removed from a UCS 5108 chassis with UCS IOM 2408.<br>This issue has been resolved. | 4.0(4b)A | 4.0(4c)A |
| CSCvq29766 | On UCS Manager managed systems with 6400 Series Fabric Interconnect, Cisco UCS Central is now able to launch the KVM console. | 4.0(4b)A | 4.0(4c)A |
| CSCvq49222 | When a UCS C220 M5 server with VIC 1455 or 1457 interface cards that was directly connected to a UCS 6454 Fabric Interconnect by two 25 GE interfaces was rebooted, the Operating System detected the status as down.<br>This issue has been resolved. | 4.0(4b)A | 4.0(4c)A |
| CSCvo78920 | When a system with Intel® Optane™ Data Center persistent memory modules installed booted, in some instances, a persistent memory module entered a "Non-Functional" health state.<br>Resolved through the updated Intel firmware in Release 4.0(4c) | 4.0(4a)B, C | 4.0(4c)B, C |
| CSCvp38545 | Intel® Optane™ Data Center persistent memory module went into a "Non-Functional" health state when tested in a chamber with HiBit DIMMs. An AC power cycle caused the failed persistent memory module to go into a "Fatal Failure" state.<br>Resolved through the updated Intel firmware in Release 4.0(4c) | 4.0(4a)B, C | 4.0(4c)B, C |
| CSCvp38555 | On first power-up, Intel® Optane™ Data Center persistent memory modules went into a "Non-Functional" health state.<br>Resolved through the updated Intel firmware in Release 4.0(4c) | 4.0(4a)B, C | 4.0(4c)B, C |

## Resolved Caveats in Release 4.0(4b)

The following caveats are resolved in Release 4.0(4b):

| Defect ID | Symptom | First Bundle Affected | Resolved in Release |
|---|---|---|---|
| CSCvp40415 | After upgrading to Cisco UCS Manager 4.0(4a), a "Persistent Memory configuration not matching" warning is seen on M5 servers during service profile association.<br>There was no functional impact from this issue. Association would still complete without any issues, and the server would successfully boot to the host OS, if installed.<br>This issue has been resolved. The warning does not appear. | 4.0(4a)A | 4.0(4b)A |
| CSCvp68182 | Upgrading from a Cisco UCS Manager Release earlier than Release 3.2(3j) to Cisco UCS Manager Release 4.0(4a), or upgrading from Cisco UCS Manager Release 4.0(1a), 4.0(1b), or 4.0(1c) to Cisco UCS Manager Release 4.0(4a), causes a small subset of Cisco UCS B200 M5, B480 M5, and S3260 M5 servers to not activate or lose IOM connectivity to the BMC<br>This issue has been resolved. | 4.0(4a) B and C | 4.0(4b) B and C |
| CSCvn64815 | In a setup with Cisco UCS C-Series servers integrated with Cisco UCS Manager and having more than 4 PCI adapters (including mLOM), Cisco UCS Manager was showing only 4 adapters in the inventory. This issue is resolved, and Cisco UCS Manager now shows all the adapters in the inventory. | 3.2(1d)A | 4.0(4b)A |
| CSCvp23760 | After upgrading to Cisco UCS Manager release 4.0(4a) on a setup with Cisco UCS C-series servers, one port of the Qlogic adapter showed as disconnected. This issue is resolved, and both the ports are connected. | 4.0(4a)C | 4.0(4b)C |

## Resolved Caveats in Release 4.0(4a)

The following caveats are resolved in Release 4.0(4a):

| Defect ID | Symptom | First Bundle Affected | Resolved in Release |
|---|---|---|---|
| CSCvm66006 | After reconfiguring and reassociating service profiles, traffic hashed to one of the hif-pc members gets dropped. This happened when DCBX did not converge properly on the impacted interface of the blade server.<br>This issue has been resolved. Now, the Fabric Interconnect checks the correct DCBX Peer ACK. | 4.0(1a)A | 4.0(4a)A |
| CSCvn66725 | Service Profile association failed with "Failed to create session-requested operation timed out" error message when trying to enable drive security for Self Encrypted Drives (SEDs) using remote Key Management Interoperability Protocol (KMIP) server on a UCS M4 server connected to a UCS 6454 Fabric Interconnect.<br>This issue has now been resolved. | 4.0(1c)B | 4.0(4a)B |
| CSCvn57345 | After restoring the Cisco UCS Manager full state backup file of a UCS device which was configured, registered, claimed and connected with Cisco Intersight, the device shows up as disconnected in Cisco Intersight.<br>This issue has been resolved. Cisco UCS Manager full state backup will not have Device Connector information. The device must be reclaimed after performing erase configuration and restore from full state backup. | 4.0(2a)A | 4.0(4a)A |

| Defect ID | Symptom | First Bundle Affected | Resolved in Release |
|---|---|---|---|
| CSCvo58393 | After upgrading to Cisco UCS Manager Release 4.0, FCoE port channels did not come up, and member links showed admin as down. The following errors were seen:<br>`Severity: Critical`<br>`Code: F999676`<br>`Last Transition Time: 2019-02-26T03:19:45.668`<br>`ID: 23387272`<br>`Status: None`<br>`Description: [FSM:FAILED]: Uplink fc port configuration on B(FSM:sam:dme:SwFcSanBorderDeploy). Remote-Invocation-Error: [FSM:STAGE:REMOTE-ERROR]: Result: service-unavailable Code: unspecified Message:`<br>`(sam:dme:SwFcSanBorderDeploy:UpdateConnectivity)`<br>`Affected Object: sys/switch-B/border-fc`<br>`Name: Fsm Sam Dme Sw Fc San Border Deploy Fsm Fail`<br>`Cause: Fsm Failed`<br>This issue is now resolved. | 4.0(2a)A | 4.0(4a)A |
| CSCvo64592 | When attempting to integrate a UCS C-Series server with Cisco UCS Manager Release 4.0 on UCS 6454 Fabric Interconnects, server discovery failed. This issue is now resolved, and the rack server discovery succeeds. | 4.0(1a)A | 4.0(4a)A |
| CSCvo66721 | After a VM changes pinning as a result of power-up/power-down, port group change, or VMotion, the MAC address of that VM now gets removed immediately from the MAC address table of the FI to which it is no longer pinned. | 4.0(2a)A | 4.0(4a)A |
| CSCvn82697 | Despite the locale being defined on a sub-organization, remotely authenticated users could see all the organizations. This issue is now resolved. | 3.2(3g)A | 4.0(4a)A |
| CSCvo91744 | After upgrading to Cisco UCS Manager Release 4.0(2), if the Network Control Policy was configured with **MAC Security** set to **Deny**, some servers showed VIF down on the upgraded Fabric Interconnect.<br>This issue is resolved. | 4.0(2a)A | 4.0(4a)A |

## Resolved Caveats in Release 4.0(2e)

The following caveats are resolved in Release 4.0(2e):

| Defect ID | Symptom | First Bundle Affected | Resolved in Release |
|---|---|---|---|
| CSCvn82697 | Despite the locale being defined on a sub-organization, remotely authenticated users could see all the organizations. This issue is now resolved. | 3.2(3g)A | 4.0(2e)A<br>4.0(4a)A |
| CSCvo19661 | Instead of broadcasting Fabric Interconnect Management IP addresses, UCS 6454 Fabric Interconnects were broadcasting KVM out-of-band IP addresses through LLDP upstream ACI leafs and downstream to ESXi hosts through CDP. This issue is fixed, and the Fabric Interconnect now broadcasts the correct IP address. | 4.0(1c)A | 4.0(2e)A |
| CSCvo64592 | When attempting to integrate a UCS C-Series server with Cisco UCS Manager Release 4.0 on UCS 6454 Fabric Interconnects, server discovery failed. This issue is now resolved, and the rack server discovery succeeds. | 4.0(1a)A | 4.0(2e)A<br>4.0(4a)A |
| CSCvn77413 | Ethernet ports on a 6332 or 6332-16 UP Fabric Interconnect showed high input discard counts, but with no appreciable performance impact.<br>This issue is now resolved. | 3.2(3h)A | 4.0(2e)A |

## Resolved Caveats in Release 4.0(2d)

The following caveats are resolved in Release 4.0(2d):

| Defect ID | Symptom | First Bundle Affected | Resolved in Release |
|---|---|---|---|
| CSCvn22595 | When using Cisco UCS B200 M5 servers with VIC 1340 and VIC 1380 adapters on a system running Cisco UCS Manager 3.2(3d) firmware and Red Hat Linux as the OS, vNICs that share the same bus ID but have different function numbers are no longer assigned to the same Input-Output Memory Management Unit (IOMMU) group. | 3.2(3d)B | 4.0(2d)B |
| CSCvn60002 | Cisco VNICs and VHBAs no longer experience degraded response time in accessing physical links after power-on or link-flap. Servers configured for sanboot now boot correctly. | 4.0(2b)A | 4.0(2d)A |
| CSCvo13678 | Cisco UCS M5 rack servers with multiple NVIDIA GPUs no longer fail discovery and produce a core file during firmware install of Cisco UCS Manager Release 4.0(2a) on the rack server. | 4.0(2a)A | 4.0(2d)A |

| Defect ID | Symptom | First Bundle Affected | Resolved in Release |
|---|---|---|---|
| CSCvn81327 | The Cisco UCS-IOM-2304 IO Module no longer crashes and produces a kernel core dump pointing to `pick_next_task_rt` in certain situations. Traffic forwarding is no longer affected. | 3.2(2d)A | 4.0(2d)A |
| CSCvm66499 | The launch KVM feature is now functional when inband KVM VLAN is configured, and the server management is connected through FEX. | 4.0(1a)C | 4.0(2d)C |
| CSCvh18287 | Cisco UCS C240 M5 servers no longer display error code F0776 and a fault message stating that non-existent disks are inoperable. | 3.2(1d)C | 4.0(2d)C |
| CSCvm66118 | When a PSU with serial number LITxxxxxx is inserted or reseated in a chassis connected to a Cisco UCS Manager managed 6300 Series Fabric Interconnect, it no longer causes the Fabric Interconnect to report PSU fan faults. | 3.2(2f)B | 4.0(2d)B<br>3.2(3j)B |
| CSCvm89871 | Cisco UCS Manager managed C240 M4 rack servers no longer fail discovery on UCS 6332 and 6332-16UP Fabric Interconnects after the following configuration sequence:<br>**1.** Disable the port that is part of the uplink Ethernet port-channel.<br>**2.** Delete the interface from the port-channel.<br>**3.** Re-configure the port type as **Server** .<br>**4.** Connect the server to the re-configured port. | 3.1(2c)C | 4.0(2d)C |
| CSCvo22832 | Cisco UCS Manager C-Series servers direct-attached to UCS 6454 Fabric Interconnects using VIC 14xx Series adapters now capture CDP/LLDP packets correctly. | 4.0(2a)A | 4.0(2d)A |
| CSCvo04128 | Fibre Channel ports configured in E mode and supported on the UCS 6454 Fabric Interconnect no longer experience delays in coming online after boot or link-flap. | 4.0(2a)A | 4.0(2d)A |

## Resolved Caveats in Release 4.0(2b)

The following caveats are resolved in Release 4.0(2b):

| Defect ID | Symptom | First Bundle Affected | Resolved in Release |
|---|---|---|---|
| CSCvk63036 | Unable to form a SAN port-channel between a Cisco UCS Fabric Interconnect pair and a Cisco Fibre Channel switch, where the Organizationally Unique ID (OUI) of the switch is one of the following:<br>• 003a9c<br>• 000831<br>• d0a5a6<br>This issue has been resolved. | 4.0(2a)A | 4.0(2b)A |
| CSCvn91826 | In a setup with Cisco VIC 14xx adapters, server discovery no longer fails due to server ID range limitation. The server ID range is now 1 to 254. | 4.0(2a)A | 4.0(2b)A |
| CSCvk26441 | When running Cisco UCS Manager Release 4.0(2a) on UCS 6454 Fabric Interconnects, LDAP user login no longer fails if the group map rule has a role other than **aaa** and **read-only**. | 4.0(2a)A | 4.0(2b)A |
| CSCvk53356 | When running Cisco UCS Manager Release 4.0(2a) on UCS 6454 Fabric Interconnects, an admin password could not be recovered using the password recovery procedure.<br>This issue has been resolved. | 4.0(2a)A | 4.0(2b)A |

## Resolved Caveats in Release 4.0(2a)

The following caveats are resolved in Release 4.0(2a):

| Defect ID | Symptom | First Bundle Affected | Resolved in Release |
|---|---|---|---|
| CSCvk62258<br>CSCvm04161 | Making LLDP configuration changes on one node of a UCS S3260 server was causing the second server node to crash. This issue was observed predominantly on Windows Operating Systems.<br>This issue has been resolved. | 3.1(3a)C | 4.0(2a)C |
| CSCvn10940 | VLAN 4093 has been removed from the list of reserved VLANs and is available for configuration. | 4.0(1a)A | 4.0(2a)A |
| CSCvh97755 | Cisco UCS 6200 Series Fabric Interconnect does not pass EAPOL-Start frames from the vEthernet interface to the upstream uplink port in the switch.<br>This issue is now resolved. | 3.1(2c)A | 4.0(2a)A |

| Defect ID | Symptom | First Bundle Affected | Resolved in Release |
|---|---|---|---|
| CSCvm08604 | During chassis firmware upgrade on Cisco S3260 chassis, the security keys for the Self-Encrypting Drives (SEDs) were mismatched between the controller and the drives.<br>This issue is resolved. | 3.2(3b)A | 3.2(3i)A<br>4.0(2a)A |
| CSCvk38240 | When using UCS VIC 1340 with adapter firmware version 4.2(3b), which is contained in the 3.2(3d) blade server firmware bundle, UEFI Boot from SAN would fail.<br>This failure no longer occurs. | 3.2(3d)B | 4.0(2a)B |
| CSCvj78742 | The active IOM no longer reboots unexpectedly due to satsyslog hap reset while failing over from the peer IOM that was rebooted. | 3.2(3d)A | 3.2(3h)A<br>4.0(2a)A |
| CSCvi66859 | In a system configured with VLAN groups and mapped with FI uplink interfaces, an unexpected outage was experienced when a VLAN is removed from a vNIC template or from a VLAN group.<br>This issue has been resolved. | 3.2(2b)A | 4.0(2a)A |
| CSCvm23975 | In a system with a Cisco UCS Manager-managed C-Series rack server and any V-Series GPU adapter, the GPU mode can be changed through the Graphics Policy in Cisco UCS Manager even if the C-Series rack server has one or more of the following GPU adapters:<br>• UCSC-GPU-V100-16G<br>• UCSC-GPU-V100-32G | 4.0(1a)A | 4.0(2a)A |

## Resolved Caveats in Release 4.0(1d)

The following caveats are resolved in Release 4.0(1d):

| Defect ID | Symptom | First Bundle Affected | Resolved in Release |
|---|---|---|---|
| CSCvm57553 | On a very small number of UCS-IOM-2304, the boot and run time may become degraded due to JFFS2 Clearmarker filesystem errors. This is caused by a limitation in a vendor-specific kernel filesystem patch, and affects IOMs that are built with 16-3743-01 NOR flash chips.<br>This issue is resolved, and no longer affects any UCS IOM. | 4.0(1a)A | 4.0(1d)A and 3.2(3i)A |

| Defect ID | Symptom | First Bundle Affected | Resolved in Release |
|---|---|---|---|
| CSCvm08604 | During chassis firmware upgrade on Cisco S3260 chassis, the security keys for the Self-Encrypting Drives (SEDs) are no longer mismatched between the controller and the drives. | 3.2(3b)A | 4.0(1d)A and 3.2(3i)A |
| CSCvj98360 | BMC did not detect the DIMM, and blade server discovery was stuck with the following message:<br>`Mismatched DIMM configuration`<br>This issue has been resolved. | 4.0(1a)B | 4.0(1d)B |
| CSCvm09239 | In a setup where a UCS 2304 IOM is connected to a UCS 6300 Series FI through a single link with a 40G QSFP cable, the IOMs no longer disconnect and reconnect while gathering chassis log files from UCS Central. | 3.2(3d)A | 4.0(1d)A and 3.2(3i)A |
| CSCvk36317 | After upgrading Cisco UCS Manager from Release 3.1(1l) to 3.2(3b), the existing PVLAN configuration no longer fails. The upstream server in the primary VLAN is now able to reach the VM/Host in the isolated VLAN in the UCS domain. | 3.2(3a)A | 4.0(1d)A and 3.2(3h)A |
| CSCvm50159 | In UCS-FI-6248UP, fans do not get detected by the switch. As a result, the switches shut down with a series of error messages:<br>`System minor alarm on fans: One fan missing or failed`<br>`Fan module 1 xxxx-FAN removed`<br>`System shutdown in 60 seconds due to fan removal`<br>`System major alarm on fans: Multiple fans missing or failed`<br>`System shutdown in 55 seconds due to fan removal`<br>`System shutdown in 50 seconds due to fan removal`<br>This issue is resolved. | 2.2(8l)A | 4.0(1d)A and 3.2(3i)A |
| CSCvk63025 | UCS 6332-16UP port 33/34 no longer has connectivity issues with C93180YC-FX port 49/50 when using a CU1M passive cable. | 3.2(3b)A | 4.0(1d)A and 3.2(3i)A |
| CSCvm44391 | The vNIC template lists duplicate vLAN entries from **LAN Cloud** and **Appliance** options.<br>This issue is resolved. The vNIC template now filters vLAN entries and lists only unique vLAN names. | 3.2(3g)A | 4.0(1d)A and 3.2(3i)A |

| Defect ID | Symptom | First Bundle Affected | Resolved in Release |
|---|---|---|---|
| CSCvm91294 | In a UCS FI setup connected to S3260 chassis with the following conditions, the DME process crashes after upgrading the chassis firmware:<br>• servers having UCS-C3K-M4 RAID storage controllers and rear boot SSDs<br>• disk zoned to both the controllers, and VDs created on top loading disks and rear boot SSDs<br>This issue is resolved. | 3.2(3g)A | 4.0(1d)A and 3.2(3i)A |
| CSCvm68038 | After the tech support logs are downloaded, samdme user sessions do not get cleared from the subordinate FI. This leads to multiple unresponsive sessions, and after the session count on the subordinate FI reaches 64 (maximum allowed), remote access to the FI is lost.<br>This issue has been resolved. The samdme user sessions are automatically cleared from the subordinate FI after the techsuport logs are downloaded. | 3.2(2d)A | 4.0(1d)A and 3.2(3i)A |
| CSCvm21299 | Primary FI upgrade no longer becomes unresponsive when logs are continuously written to the pa_setup.log file. | 3.2(3a)A | 4.0(1d)A and 3.2(3i)A |
| CSCvm54628 | On UCS 6200 Series, FI management IP address changes do not get updated in the IOM or FEX. Hence, the devices connected to the host interfaces continue to receive the old management IP address through the CDP process.<br>This issue is resolved. The devices connected to the host interfaces now receive the updated management IP address through the CDP process. | 3.2(3b)A | 4.0(1d)A and 3.2(3i)A |
| CSCvm95801<br>CSCvn01215 | On UCS 6300 Series and UCS 6324, FI management IP address changes do not get updated in the IOM or FEX. Hence, the devices connected to the host interfaces continue to receive the old management IP address through the CDP process.<br>This issue is resolved. The devices connected to the host interfaces now receive the updated management IP address through the CDP process. | 3.2(3b)A | 4.0(1d)A and 3.2(3j)A |
| CSCvn10940 | VLAN 4093 has been removed from the list of reserved VLANs and is available for configuration. | 4.0(1a)A | 4.0(1d)A and 4.0(2a)A |

| Defect ID | Symptom | First Bundle Affected | Resolved in Release |
|---|---|---|---|
| CSCvn09080 | On UCS 6454, FI management IP address changes do not get updated in the IOM or FEX. Hence, the devices connected to the host interfaces continue to receive the old management IP address through the CDP process.<br>This issue is resolved. The devices connected to the host interfaces now receive the updated management IP address through the CDP process. | 4.0(1a)A | 4.0(1d)A |
| CSCvn25087 | In scenarios with very specific write/read patterns, there could be potential data loss for 3.8 TB and 7.6 TB Micron 5100 SSD SATA drives. UECC read errors and reallocated sector counts are displayed in SMART log.<br>This issue is now resolved. | 4.0(1c)B and 4.0(1c)C | 4.0(1d)B and 4.0(1d)C |

## Resolved Caveats in Release 4.0(1c)

The following caveats are resolved in Release 4.0(1c):

| Defect ID | Symptom | First Bundle Affected | Resolved in Release |
|---|---|---|---|
| CSCvh04307 | On Cisco HyperFlex nodes with SED drives, installing software packages on the storage controller VM failed with the following error:<br>`There are locked drives on the system, unlock them and retry deployment.`<br>The drives could become locked on hosts that were rebooted. The fix for this issue was integrated in Release 4.0(1a).<br>Additionally, there was a scenario in which the drives could become locked on hosts that were cold powered down for a prolonged period and then rebooted. The fix for this scenario was integrated in Release 4.0(1c). | 3.1(3c)C | 4.0(1c)C |

| Defect ID | Symptom | First Bundle Affected | Resolved in Release |
|---|---|---|---|
| CSCvm14726 | Cisco UCS 6324 Fabric Interconnects with the new SPI Flash device cannot boot with previous software releases. This is because the original SPI Flash device used on the UCS 6324 Fabric Interconnect is no longer being produced. Hence, a pin-compatible replacement part is being used going forward. However, due to the vendor and part ID changing, the UCS 6324 Fabric Interconnect equipped with the new part can only operate with OS versions that have support for the new part built in.<br>This issue is now resolved. | 4.0(1a)A | 4.0(1c)A |
| CSCvk30528 | In UEFI boot mode, Cisco UCS Managed C-Series servers failed to boot to the RHEL or ESXi OS installed on an iSCSI LUN configured on an EMC storage device. Instead, the server entered into the UEFI shell prompt after every reboot.<br>This issue has been resolved. The server now boots to the OS correctly. | 4.0(1a)C | 4.0(1c)C |

## Resolved Caveats in Release 4.0(1b)

The following caveats are resolved in Release 4.0(1b):

| Defect ID | Symptom | First Bundle Affected | Resolved in Release |
|---|---|---|---|
| CSCvm17259 | In a system with a Cisco UCS Manager-managed C-Series rack server, the firmware for the UCSC-GPU-V100-32G GPU was not seen in the Host Firmware Pack (HFP) of the Firmware Policy after configuring the service profile for the server. This issue is now resolved, and the firmware is visible in the HFP. | 4.0(1a)A | 4.0(1b)A |
| CSCvm10391 | The Cisco UCS 6454 Fabric Interconnect was not sending any Call Home messages to the configured SMTP server.<br>This issue has now been resolved. Call Home messages are now being sent by the Cisco UCS 6454 Fabric Interconnect and received as emails at the configured SMTP server. | 4.0(1a)A | 4.0(1b)A |

## Resolved Caveats in Release 4.0(1a)

The following caveats are resolved in Release 4.0(1a):

| Defect ID | Symptom | First Bundle Affected | Resolved in Release |
|---|---|---|---|
| CSCvh04307 | On Cisco HyperFlex nodes with SED drives, installing software packages on the storage controller VM failed with the following error:<br>`There are locked drives on the system, unlock them and retry deployment.`<br>Additionally, the drives could become locked on hosts that were rebooted.<br>This issue is now resolved. | 3.1(3c)C | 4.0(1a)C |
| CSCva17452 | Packets are no longer dropped at the UP ports of the Cisco UCS 6332-16IUP Fabric Interconnect Series when two no-drop classes (one Ethernet and one FCoE) are configured on the system. | 3.1(1e)A | 4.0(1a)A |
| CSCve53858 | After enabling/disabling breakout ports and creating/deleting port channels, FI QoS queues are no longer stuck. | 3.2(2b)A | 4.0(1a)A |
| CSCvh79589 | The timer group library no longer causes the bcm_usd process to crash and reboot UCS 6332 Series Fabric Interconnects during normal operational state. | 3.2(2b)A | 4.0(1a)A |
| CSCvi16121 | The server reboots unexpectedly and the service profile is re-associated when there is a configuration change for a service profile bound to an updating service profile template with a server pool assigned. This happens when the server assigned to the service profile is not part of the server pool.<br>This issue is now resolved. Unexpected server reboots and service profile re-association no longer happen after the configuration change. | 3.2(1d)A | 4.0(1a)A |

## Open Caveats

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

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

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

## Open Caveats for Release 4.0(4m)

The following caveats are open in Release 4.0(4m):

| Defect ID | Symptom | Workaround | First Bundle Affected |
|---|---|---|---|
| CSCvx99711 | The **`show version`** command on NXOS prompt does not show SSD model info. The two fields below show empty strings:<br>`SSD model:`<br>`SSD firmware version:` | Use the command **`show system internal file /proc/scsi/scsi`** to obtain the information. | 4.0(1a)A |

## Open Caveats for Release 4.0(4l)

The following caveats are open in Release 4.0(4l):

| Defect ID | Symptom | Workaround | First Bundle Affected |
|---|---|---|---|
| CSCvx72997 | Under certain rare conditions, when booting from Golden FPGA, a 6400 Series Fabric Interconnect might get stuck on Loader during reload. Check the syslog on boot-up to verify whether system is booting from Primary FPGA or Golden FPGA. | Run the **reboot** command on loader or power-cycle the system. | 4.0(4)A |

## Open Caveats for Release 4.0(4i)

The following caveats are open in Release 4.0(4i):

| Defect ID | Symptom | Workaround | First Bundle Affected |
|---|---|---|---|
| CSCvt60312 | During upgrade of UCS C-Series servers, service profile association took 1 to 2 hours to perform the "Perform Inventory of Server - PNUOS Inventory". | In Cisco UCS Manager, navigate to the **Installed Firmware** tab and check if **Activate Status** of all drives is **Ready**. If the activate status of all the drives is ready, reset the server through KVM or Cisco UCS Manager to progress the upgrade. | 4.0(4g)B |

| Defect ID | Symptom | Workaround | First Bundle Affected |
|---|---|---|---|
| CSCvs93286 | After performing server Firmware upgrade with Host Firmware Pack (auto-install servers) on an adapter, the adapter activation gets stuck at the pending-next-boot state. This condition occurs when the adapter activation is triggered immediately after BIOS update followed by host power ON when both the server BIOS and adapter are updated. | Log into Cisco UCS Manager and reset the adapter. | 4.0(4g)A, 4.0(4h)A and C |
| CSCvv80576 | On a UCS Managed B or C Series server or UCS Mini connected to either 6200 Series or 6300 Series Fabric Interconnects, after a vNIC fail-over, traffic does not switch to the second Fabric Interconnect, resulting in dropped traffic. Servers with 6400 Series Fabric Interconnects are not affected. | Make sure traffic is continuous from the vNIC source during fail-over. | 3.2(3o)A<br>Resolved in 4.0(4k)A |
| CSCvs06864 | During installation of Windows 2016 or Windows 2019 on SAN LUN, blue screen of death (BSoD) is observed. This condition is observed when service profile configured with 2 or more vHBAs is associated on a Cisco UCS VIC 14xx series adapter bundled with UCS versions 4.0(4a) or later versions. | On each Cisco UCS VIC 14xx series adapter, limit the number of vHBAs to one per adapter during Windows 2016 or Windows 2019 installation on SAN LUN. Add the remaining vHBAs after installation. | 4.0(4a) |

## Open Caveats for Release 4.0(4h)

The following caveats are open in Release 4.0(4h):

| Defect ID | Symptom | Workaround | First Bundle Affected |
|---|---|---|---|
| CSCvt64871 | In rare situations, Cisco UCS C480 M5 servers and Cisco UCS 480 M5 ML servers stop responding and reboot after ADDDC virtual lockstep is activated. This results in #IERR and M2M timeout in the memory system.<br>For more information, see:<br>• Intel® Xeon® Processor Scalable FamilySpecification Update (Errata > SKX108)<br>• Second Generation Intel® Xeon® Scalable Processors Specification Update(Errata > CLX37) | If the server crashes many times after activating ADDDC virtual lockstep, disable ADDDC.<br>For more information, see the Cisco Software Advisory at https://www.cisco.com/c/en/us/support/docs/field-notices/704/fn70432.html | 4.0(4c)B |

| Defect ID | Symptom | Workaround | First Bundle Affected |
|---|---|---|---|
| CSCvt55829 | SanDisk Lightning II Solid State Drives (SSDs) LT0400MO and LT1600MO with respect to PIDS listed below, report 0 GB of available storage space remaining under normal operation at 40,000 power on hours. SSDs go offline and become unusable after power cycle event resulting in data loss, potentially on multiple drives if they are placed in service at the same time.<br>The PIDs of affected SSDs are:<br>• (400GB) UCS-SD400G1KHY-EP, UCS-SD400G12S4-EP, UCS-C3X60-12G240<br>• (1.6TB) UCS-SD16TG1KHY-EP, UCS-SD16TB12S4-EP, UCS-C3X60-12G2160<br>This issue is resolved. | Install firmware version C405 to resolve the issue. | 4.0(4h)C<br>Resolved in 4.0(4i)C |
| CSCvt46877<br>CSCvt46838 | A 6400 Series Fabric Interconnect experiences an unexpected reset when the number of peers is high. | Disable fabric services. | 4.0(4h)A<br>Resolved in 4.0(4i)A |

| Defect ID | Symptom | Workaround | First Bundle Affected |
|---|---|---|---|
| CSCvn74327 | After a firmware upgrade on a Series 1400 adapter, the virtual ports are unavailable and the system log displayed the following messages:<br>`191024-05:13:13.410919 laser.i2c ERROR: i2c1: stuck bus - failed to clear`<br>`191024-05:13:18.529477 laser.i2c ERROR: i2c1: stuck bus - failed to clear`<br>`191024-05:13:18.530797 kernel: paloi2c c8004400.i2c1: target 0x20: timeout error`<br>`191024-05:13:23.579591 kernel: paloi2c c8004400.i2c1: target 0x20: timeout error`<br>`191024-05:13:23.579895 laser.i2c ERROR: i2c1: stuck bus - failed to clear`<br>`191024-05:13:28.695617 kernel: paloi2c c8004400.i2c1: target 0x20: timeout error`<br>`191024-05:13:28.695951 laser.i2c ERROR: i2c1: stuck bus - failed to clear`<br>`191024-05:13:33.747636 kernel: paloi2c c8004400.i2c1: target 0x20: timeout error`<br>`191024-05:13:33.747969 laser.i2c ERROR: i2c1: stuck bus - failed to clear` | Power-cycle the system. | 4.0(4h)A<br>Resolved in 4.0(4i)A |

| Defect ID | Symptom | Workaround | First Bundle Affected |
|---|---|---|---|
| CSCvu14656 | On upgrade of BIOS to one of the following versions, the booting of M5 servers get stuck at the memory testing step:<br>• C240M5.4.0.4r.0.0305200743<br>• C220M5.4.0.4p.0.0224200755<br>• B200M5.4.0.4l.0.0305202307<br>• B480M5.4.0.4m.0.0305202307<br>• S3X60M5.4.0.4o.0.0224200755 | To boot the server, perform the following:<br>**1.** Revert BIOS to prior working version and boot the system to OS.<br>**2.** Review logs to determine DIMMs with correctable or uncorrectable ECC errors and replace or remove faulty DIMMs.<br>**3.** Upgrade to BIOS version included in 4.0(4h) bundle and make sure that the system boots as expected. | 4.0(4h)C<br>Resolved in 4.0(4i)C |
| CSCvu11155 | On upgrade of BIOS to one of the following versions, you might experience performance degradation on Cisco UCS B-Series, C-series, and S- series M5 servers running with second Generation Intel® Xeon® Scalable Processors:<br>• C240M5.4.0.4r.0.0305200743<br>• C220M5.4.0.4p.0.0224200755<br>• B200M5.4.0.4l.0.0305202307<br>• B480M5.4.0.4m.0.0305202307<br>• S3X60M5.4.0.4o.0.0224200755 | There is no known workaround. | 4.0(4h)B and C |

## Open Caveats for Release 4.0(4e)

The following caveats are open in Release 4.0(4e):

| Defect ID | Symptom | Workaround | First Bundle Affected |
|---|---|---|---|
| CSCvr01259 | With UCS 6400 Series Fabric Interconnects connected to UCS 2408 IOMs, the HIF port interface counters are not updated on the Fabric Interconnect. However, the virtual Ethernet will show the correct packet count. | Use the virtual Ethernet counters. | 4.0(4e)A |
| CSCvr67352 | On blade servers connected to 6454 Fabric Interconnects, the management instance loses access to the OOB KVM connection under the following conditions:<br>• The IOM is rebooted<br>• One of the Fabric Interconnects becomes inoperable<br>On rack servers connected to 6454 Fabric Interconnects, the management instance loses access to the KVM connection under the following conditions:<br>• The FEX is rebooted<br>• The FEX is inoperable on one Fabric Interconnect<br>• One of the Fabric Interconnects is not reachable.<br>This issue is applicable only for service profile management IP addresses. | Reboot the Fabric Interconnect that has the stale OOB KVM IP address configured on mgmt0 interface. | 4.0(4e)A<br>Resolved in 4.0(4f)A |

| Defect ID | Symptom | Workaround | First Bundle Affected |
|---|---|---|---|
| CSCvr68316 | In a standalone C-Series server, when a UCS VIC 1455/1457 adapter is connected to a switch with port-channel enabled on both the VIC and switch side, the Ethernet and Fibre Channel data paths do not work.<br>The issue is specific to standalone C-Series servers, and is not applicable to UCS Manager managed C-Series servers. However, the issue may manifest during the integration of a C-Series server with a UCS Manager system, where the Cisco IMC or VIC adapter "reset to factory-default" is a pre-requisite step of the server integration workflow. | Disable the VIC 1455/1457 "Portchannel" configuration from Cisco IMC and re-enable it. | 4.0(4e)C<br>Resolved in 4.0(4f)C |
| CSCvr79388 | Under certain rare conditions on M5 B Series servers, the server reboots after activation of ADDDC virtual lockstep, resulting in a CATERR and an M2M timeout in the Memory system. | Contact TAC. | 4.0(4e)<br>Resolved in 4.0(4h)C |
| CSCvr79396 | On M5 B Series servers, the Virtual lock step (VLS) sparing copy finishes early, leading to incorrect values in the lock step region . | Contact TAC. | 4.0(4e)C<br>Resolved in 4.0(4h)C |

| Defect ID | Symptom | Workaround | First Bundle Affected |
|---|---|---|---|
| CSCvt38091 | After upgrading to UCS Manager release 4.0(4e), a B200-M5 blade server displayed messages similar to the following:<br>`Model UCS-FI-6332-16UP with Host Name (host name) reported following Diagnostics test failure:`<br>`'Recovered : Server 1/6 (service profile: (profile name) inaccessible'` | The message will eventually clear itself. | 4.0(4e)B |

## Open Caveats for Release 4.0(4d)

The following caveats are open in Release 4.0(4d):

| Defect ID | Symptom | Workaround | First Bundle Affected |
|---|---|---|---|
| CSCvr23703 | Server Boot Time may increase.<br>Under certain circumstances, such as using Intel® Optane™ Data Center persistent memory module in App Direct Mode, while using a large number of Name Spaces, the boot time can increase by up to 9%. | None | 4.0(4d)B |
| CSCvr47266 | During migration from a Model 6248 Fabric Interconnect to Model 6454 Fabric Interconnect, UCS 2208 IOMs silently failed. Any actions that require portAG fail. All versions of Cisco UCS Manager allow for burst size 0 to apply, but only 6454 Fabric Interconnects fail as a result (after migration). | Configure a burst size in range of 512-268435456, even in a failed state. | 4.0(4d)A<br>Resolved in 4.0(4f)A<br>. |

| Defect ID | Symptom | Workaround | First Bundle Affected |
|---|---|---|---|
| CSCvr23703 | Under specific conditions on a B480 M5 server, such as using Intel® Optane™ Data Center persistent memory module in App Direct Mode, and using large number of Name Spaces, the server boot time noticably increased. | None | 4.0(4d)B |
| CSCvr40744 | Port 5661 on a 6400 Series Fabric Interconnect is open for `httpd` and `tcpwrapped`. | No known workaround. | 4.0(4d)A and B<br>Resolved in 4.0(4f)A |
| CSCvr46327 | When replacing a UCS 2208 IOM with a UCS 2408 IOM, virtual ethernet interfaces become unavailable. Virtual Ethernet interfaces are not available in the output of the **show interface virtual status** command, but are available in the output of the **show interface brief** command in NXOS. | Reload the Fabric Interconnects after one of them completes the migration, then execute a Fabric Interconnect reload in Cisco UCS Manager to bring up the virtual Ethernet interfaces. | 4.0(4d)A |

## Open Caveats for Release 4.0(4c)

The following caveats are open in Release 4.0(4c):

| Defect ID | Symptom | Workaround | First Bundle Affected |
|---|---|---|---|
| CSCvq74492 | System becomes unresponsive during BIOS post when the Intel X520 PCIe adapter is present on the system and iSCSI mode is enabled for Intel X550 LOMs. This happens only when boot mode is set to legacy. | If this issue occurs, do one of the following:<br>• Switch to UEFI boot mode.<br>Or<br>1. When system is hung, set the LOM Option to disable using the CIMC feature to set the BIOS tokens.<br>2. Reboot the server to the UEFI shell.<br>3. Use the Intel bootutil and enable iSCSI for X520 adapter and reboot the server (Intel bootutil along with its userguide is part of the driver iso).<br>4. On next boot, during BIOS post enter into Intel OPROM Utility(Ctrl +D), enable the ISCSI mode for X550 LOM. Save and restart.<br>5. LOM ISCSI LUN will boot without any issue. | 4.0(4c)C |

| Defect ID | Symptom | Workaround | First Bundle Affected |
|---|---|---|---|
| CSCvq26156 | | 1. Before upgrading to 4.0(4a) release, upgrade only the firmware of the drives to SCV1CS07, which is part of Release 4.0(4a) or later release packages.<br>2. Now proceed with full upgrade of 4.0(4a) or later release package.<br>If already impacted by this issue, do the following to recover:<br>1. Downgrade Cisco 12G Modular SAS HBA to a previous working version (00.00.00.50 or 00.00.00.58 available in 4.0(1) and 4.0(2) release packages respectively).<br>2. Upgrade the firmware of the impacted drives to SCV1CS07, which is part of Release 4.0(4a) or later release packages.<br>3. After drive firmware is updated, proceed with upgrade of Cisco 12G Modular SAS HBA firmware to 09.00.00.06, which is part of Release 4.0(4a) or later release packages. | 4.0(1a)C<br>4.0(2a)C<br>4.0(4c)C<br>Resolved in 4.0(4d)C |

| Defect ID | Symptom | Workaround | First Bundle Affected |
|---|---|---|---|
| | Upgrade of UCS C-Series Server firmware to 4.0(4a) or later releases can cause the Cisco 12G Modular SAS HBA to stop discovering the following Intel S4500 drive models and results in disk firmware upgrade failure.<br>• SSDSC2KB480G7K - 480GB 2.5-inch Enterprise Value 6G SATA SSD<br>• SSDSC2KB960G7K - 960GB 2.5-inch Enterprise Value 6G SATA SSD<br>• SSDSC2KG019T7K - 1.9TB 2.5-inch Enterprise performance 6G SATA SSD<br>• SSDSC2KG480G7K - 480GB 2.5-inch Enterprise performance 6GSATA SSD<br>• SSDSC2KG960G7K - 960GB 2.5-inch Enterprise performance 6G SATA SSD<br>• SSDSC2KB038T7K - 3.8TB 2.5-inch Enterprise Value 6G SATA SSD<br>This issue occurs only when the drive firmware version before the upgrade is SCV1CS05. Other drive firmware versions are not affected.<br>**Note** Cisco HyperFlex | | |

| Defect ID | Symptom | Workaround | First Bundle Affected |
|---|---|---|---|
| | does not support UCS Manager 4.0(4a), 4.0(4b) or 4.0(4c). | | |
| CSCvq64055 | A physical link on a UCS C-Series server with a VIC 1455/1457 interface connected with its peer using 25G Copper passive 5M cable (SFP-H25G-CU5M does not link up or is not discovered by the UCS.<br>This issue occurs either in a Cisco UCS Manager managed environment or in standalone environments where the VIC 1455/1457 interface is connected to Cisco Nexus switches or to a server configured with SAN boot. It can also occur when a network boot does not boot or load the OS.<br>The issue happens primarily because of delays in the VIC 1455/1457 interface detecting the physical link up with 5M long 25G copper passive cables (SFP-H25G-CU5M).<br>This issue affects all M5 models | **1.** Use shorter copper passive cables (SFP-25G-CU1M. SFP-25G-CU2M, SFP-25G-CU3M).<br>**2.** Use optical cables. | 4.0(1a)C<br>4.0(2a)C<br>4.0(4a)C |

| Defect ID | Symptom | Workaround | First Bundle Affected |
|---|---|---|---|
| CSCvq38756 | Intermittant traffic loss sometimes occurs on a UCS Cluster with NIC teaming when the Fabric Interconnect reloads. | In the Cisco UCS Manager Ethernet adapter policy, configure a larger failback timeout value. After the vNIC accesses its secondary interface, this setting controls how long the primary interface must be available before the system resumes using the primary vNIC interface.<br>Enter a number of seconds between 0 and 600. | 4.0(4b)A<br>Resolved in 4.0(4d)A |
| CSCvp49398 | On any C/HX-series M5 server deployment with a VIC 1455/1457 interface directly connected (through either single or dual link connections) to a 6454 Fabric Interconnect using 10/25GE passive cables on each fabric, traffic drops for over 75 seconds after a Fabric Interconnect reboot. | None | 4.0(2d)C |
| CSCvq09345 | Cisco UCS M5 blade servers associated with service profiles that have a persistent memory policy may display the following configuration error message:<br>`Persistent Memory Policy configured on a server not having persistent memory DIMMS.`<br>This happens in some rare scenarios, such as during multiple cycles of server reboot, discovery, and association. | Decommission and then recommission the server. | 4.0(4b)B |

| Defect ID | Symptom | Workaround | First Bundle Affected |
|---|---|---|---|
| CSCvq90219 | Cisco UCS Manager activation failed on a Blade server with 6200 Series Fabric Interconnect during manual upgrade from UCS Manager 3.2(3k) to UCS Manager 4.0.4. | None | 4.0(4c)A<br>Resolved in 4.0(4f)A |

## Open Caveats for Release 4.0(4b)

The following caveats are open in Release 4.0(4b):

| Defect ID | Symptom | Workaround | First Bundle Affected |
|---|---|---|---|
| CSCvp31766 | When upgrading blade servers, the VMs using VM-FEX interfaces lose connectivity. | Upgrade to Cisco UCS Manager Release 4.0(4c) or a later release. | 4.0(4b)B<br>Resolved in 4.0(4c)B |
| CSCvq17624 | The old power supply unit (PSU) data is not cleared from Cisco UCS Manager when a PSU is removed from a UCS 5108 chassis with UCS IOM 2408. | None | 4.0(4b)A<br>Resolved in 4.0(4c)A |
| CSCvq29766 | After upgrading a UCS-managed blade server to UCS Manager version 4.0(4b), UCS Central was unable to launch the KVM console. | Launch KVM from UCS Manager domain. | 4.0(4b)A<br>Resolved in 4.0(4c)A |
| CSCvq49222 | When a UCS C220 M5 server with VIC 1455 or 1457 interface cards directly connected to a 6454 Fabric Interconnect by 2-25GE interfaces is rebooted, the Operating System detects the status as down for an interval ranging from few seconds to two minutes. | Deploy active optical transceivers, such as<br>`SFP-10G-AOC1M/2M/3M/5M/7M/10M.` | 4.0(4b)B |

| Defect ID | Symptom | Workaround | First Bundle Affected |
|---|---|---|---|
| CSCvq26156 | Upgrade of UCS C-Series servers to 4.0(4c) C-Bundle causes the Cisco 12G Modular SAS HBA to stop discovering/communicating with some Intel S4500 disk drives. This could result in failure of the software upgrade of these drives.<br>This issue only occurres with Controller firmware version 09.00.00.06. | Pre-Upgrade - in host firmware package omit the Raid Controller upgrade.<br>Post-Upgrade - Roll back the Raid Controller firmware to version 00.00.00.58. | 4.0(4a)C<br>Resolved in 4.0(4d)A |
| CSCvq84120 | After Fabric Interconnect reboot, vNICs sometimes fail over prematurely due to the timing of policy association, causing intermittant traffic loss. The system displays the message: `Cannot apply non-existing policy to interface`. | None. | 4.0(4b)A<br>Resolved in 4.0(4d)A |
| CSCvr11045 | Ports 81 and 743 are accessible on UCS 6454 Fabric Interconnects even though CIMC web service was disabled. | None. | 4.0(4b)A<br>Resolved in 4.0(4d)A |

| Defect ID | Symptom | Workaround | First Bundle Affected |
|---|---|---|---|
| CSCvq09345 | Cisco UCS M5 blade servers associated with service profiles that have a persistent memory policy may display the following configuration error message:<br>“Persistent Memory Policy configured on a server not having persistent memory DIMMS.”<br>This happens in some rare scenarios, such as multiple cycles of server reboot and discovery and association. | Decommission and then recommission the server. | 4.0(4b)A |
| CSCvq82024 | When BIOS menu setup item "AEP Error Injection" is enabled, an error is injected to the Intel® Optane™ Data Center persistent memory module, causing an erroneous PSOD generation.The operating system is not notified and hence, the MCE was is properly handled. | None | 4.0(4b)B<br>Resolved in4.0(4e)B |
| CSCvq57262 | During an upgrade of the infrastructure bundle of a UCS 6400 Series Fabric Interconnect with RDMA, one of the rack servers shows a pending reboot acknowledgement. | None | 4.0(4b)A<br>Resolved in4.0(4f)A |
| CSCvp52336 | UCS 6454 Fabric Interconnect is unable to receive the DHCP IP address during initial setup. | Use static IP for the initial setup | 4.0(4b)A<br>Resolved in4.0(4f)A |

| Defect ID | Symptom | Workaround | First Bundle Affected |
|---|---|---|---|
| CSCvq51008 | UCS B460 M4 blade servers on a single adapter cannot find an adaptor to associate at placement of the vCon. The error message `configuration failed due to insufficient-resources,connection-placement` is displayed. | Swap the master and slave blades, which makes the server adaptor number 3. In this configuration, the server will associate without error. | 4.0(4b)A and B<br>Resolved in4.0(4f)A and B |
| CSCvr35735 | UCS 6454 Fabric Interconnects cannot switch traffic between a pair of UCS rack-servers when vNICs are pinned to the Fabric Interconnect. | Pin vNICs of affected pairs on different Fabric Interconnects, if the Fabric Interconnects are in a cluster.<br>If a Fabric Interconnect is running in standalone, discover the server on a different port. | 4.0(4b)A<br>Resolved in4.0(4f)A |
| CSCvq98090 | SAN paths on UCS 6454 Fabric Interconnects go offline when the Fabric Interconnect is power-cycled. | Restart the member links. | 4.0(4b)A<br>Resolved in4.0(4f)A |
| CSCvr76930 | Ports could fail to link on UCS Managed servers with 2408 Fabric Extenders attached through SFP-H25G-CU5M cables. | Do not use model SFP-H25G-CU5M cables. Use another model of cable, such as SFP-H25G-CU3M or SFP-H25G-AOC5M. | 4.0(4b)B and C |
| CSCvr34407 | UCS M4 and M5 rack servers connected to UCS 6300 Series Fabric Interconnects lost their VLAN configuration after an enable or disable operation from Cisco UCS Manager. | Re-acknowlege the server. | 4.0(4b)A<br>Resolved in4.0(4f)A |

| Defect ID | Symptom | Workaround | First Bundle Affected |
|---|---|---|---|
| CSCvr47266 | During migration from UCS 6200 Series Fabric Interconnects to UCS 6454 Fabric Interconnects, PortAG will continually bootstrap if incorrect burst size is set in the Quality of Service policy. Failure is silent: no alerts or core files are created. | Configure burst size in a range between 512 and 268435456. Cisco UCS Manager will apply this workaround even in a failed state. | 4.0(4b)A<br>Resolved in4.0(4f)A |
| CSCvr43466 | Cisco UCS Manager integrated Cisco UCS B-Series and C-Series M5 servers report the following hardware inventory mismatch fault even though the hardware has not changed: `hardware inventory mismatch` | Decommission and re-acknowledge the server. | 4.0(4b)B<br>Resolved in4.0(4g)B |
| CSCvr95365 | After firmware upgrade from Cisco UCS Manager Release 4.0(1a) to Release 4.0(4b), discovery of a Cisco UCS C240 M5 server that is equipped with a Cisco 12G Modular SAS HBA controller, fails with the following error:<br>`mc_attrib_set_suboem_id failed to set the SubOEM ID` | Replace the affected HBA controller. | 4.0(4b)C |
| CSCvr98210 | When upgrading UCS Manager 3.2.x to UCS Manager 4.0.x on a system with appliance ports or FCoE storage ports, LLDP becomes disabled by default and any service requiring LLDP stops working. | To recover connectivity, disable and then re-enable LLDP in the network control policy after upgrading to Cisco UCS Manager Release 4.0. | 4.0(4b)A<br>Resolved in 4.0(4h)A |

| Defect ID | Symptom | Workaround | First Bundle Affected |
|---|---|---|---|
| CSCvs25524 | On 6300 Series Fabric Interconnects, messages like the following appear in the console logs:<br>`FI6332-DC3-A %SYSMGR-2-TMP_DIR_FULL: System temporary directory usage is unexpectedly high at 80%.` | Open a TAC case; TAC can go in and empty unneeded logs from the /tmp directory. Rebooting the Fabric Interconnect can also solve this problem, as the temp directory is held in RAM. | 4.0(4b)A<br>Resolved in 4.0(4h)A |
| CSCvt08435 | On the 6300 Series Fabric Interconnect, while monitoring SNMP on IOM 2304, HIF ports counts intermittently drop to zero, causing high traffic indications on the third party monitoring applications. | None | 4.0(4b)A<br>Resolved in 4.0(4i)A |
| CSCvu07675 | Auto-install of firmware on a UCS-Managed integrated C-Series rack server fails to activate the SAS Controller. | Decommission and re-acknowledge the affected rack servers. | 4.0(4b)C<br>Resolved in 4.0(4i)C |

## Open Caveats for Release 4.0(4a)

The following caveats are open in Release 4.0(4a):

*Table 22: Intel® Optane™ Data Center Persistent Memory Modules - Intel Open Caveats*

| Defect ID | Symptom | Workaround | First Bundle Affected |
|---|---|---|---|
| CSCvn77341 | Namespaces created under Red Hat Enterprise Linux 7.6 by using the in-box ndctl tool, may be seen in "Critical" health state when examined in the BIOS Setup or the UEFI IPMCTL tool. However, the namespaces are healthy, and their functionality is not affected.<br>This is an issue with the Intel® Optane™ Data Center persistent memory module HII and UEFI IPMCTL tool.<br>Intel IPS case filed. | Use RHEL 7.6 version 4.20.13-200.fc29 or later kernel . The namespaces are healthy, and their functionality is not affected. | 4.0(4a)B and C<br>Resolved in4.0(4e)B and C |
| CSCvn81521 | On systems with Intel® Optane™ Data Center persistent memory modules in 2LM (memory mode), uncorrectable errors get logged on the persistent memory modules when errors occur on DDR4 DIMMs (configured as near memory) on the same channel.<br>Intel IPS case filed. | Examine the MCAOut files to identify the actual failed DIMM location. | 4.0(4a)B and C<br>Resolved in4.0(4e)B and C |
| CSCvp08356 | When Intel® Optane™ Data Center persistent memory modules are populated in the system, and the system is operational, occasionally false uncorrectable errors are reported on DIMM A1. This has no functional impact.<br>Intel IPS case filed. | Clear errors by using **Reset all Memory errors** in Cisco UCS Manager. | 4.0(4a)B and C |

| Defect ID | Symptom | Workaround | First Bundle Affected |
|---|---|---|---|
| CSCvo78920 | When a system with Intel® Optane™ Data Center persistent memory modules installed boots, in some instances, a persistent memory module health state may enter a "Non-Functional" state. In some instances, the persistent memory module will recover ("Healthy" health state) after an AC power cycle. If a persistent memory module becomes "Non-Functional" and does not recover, it should be replaced.<br>Intel IPS case filed. | No known workaround. | 4.0(4a)B and C<br>Resolved through the updated Intel firmware in Release 4.0(4c) |
| CSCvp38545 | Intel® Optane™ Data Center persistent memory module goes into a "Non-Functional" health state when tested in a chamber with HiBit DIMMs. AC power cycle causes the failed persistent memory module to go into a "Fatal Failure" state.<br>Intel IPS case filed. | No known workaround | 4.0(4a)B and C<br>Resolved through the updated Intel firmware in Release 4.0(4c) |
| CSCvp38555 | Intel® Optane™ Data Center persistent memory modules go into a "Non-Functional" health state when it is first powered up.<br>Intel IPS case filed. | No known workaround | 4.0(4a)B and C<br>Resolved through the updated Intel firmware in Release 4.0(4c) |
| CSCvp38564 | Intel® Intelligent Power Technology Node Manager (NM) PTU does not work with Intel® Optane™ DC persistent memory modules in App Direct mode. Hence, the power characterization accuracy is reduced.<br>Intel IPS case filed. | If persistent memory modules are detected in a system, the BIOS will not load NMPTU to prevent unresponsiveness or an infinite loop. | 4.0(4a)B and C |

| Defect ID | Symptom | Workaround | First Bundle Affected |
|---|---|---|---|
| CSCvp37389 | In some specific situations, in-flight write traffic can hit a small probability of a DDRT surprise clock stop, which may cause the Intel® Optane™ Data Center persistent memory module to go into a "Fatal Failure" state and result in a persistent memory module Media Disable. | No known workaround. | 4.0(4a)B and C |

*Table 23: Intel® Optane™ Data Center Persistent Memory Modules - Cisco Open Caveats*

| Defect ID | Symptom | Workaround | First Bundle Affected |
|---|---|---|---|
| CSCvp30026 | Intel® Optane™ Data Center persistent memory modules were managed by Cisco UCS Manager with secure passphrase enabled. Subsequently, the persistent memory policy was removed to transition the server into the host-managed mode. When this happened, regions and namespaces were reported as "Unmanageable" in Cisco UCS Manager although the regions and namespaces are actually "Healthy". It is a reporting issue. There is no functional impact. | Use host-based tools and disable persistent memory module security. Then reacknowledge the server. | 4.0(4a)B |
| CSCvo52036 | Adding additional namespaces along with the existing namespaces that are mounted in Red Hat Enterprise Linux 7.6 with Intel® Optane™ Data Center persistent memory modules in App Direct mode may cause Red Hat boot failure. | Ensure that the required namespaces are created and applied as mount points only once. After this, more namespaces should not be added. | 4.0(4a)B |
| CSCvn64709 | For Intel® Optane™ Data Center persistent memory modules in host-managed mode, security cannot be enabled by setting the passphrase in the BIOS setup. Use Intel UEFI or OS tools to enable the security. | Use host-based tools IPMCTL tool to set the passphrase. | 4.0(4a)B |

| Defect ID | Symptom | Workaround | First Bundle Affected |
|---|---|---|---|
| CSCvp36938 | After the **Reset to Factory Default** operation is performed, under **Inventory**, the persistent memory module Config Status will appear as "Host Managed". This happens when a persistent memory policy is attached to a service profile (UCS-managed persistent memory modules). It is a reporting issue. Any subsequent persistent memory policy changes will restore the config to the UCS-managed mode. | If there is space on any region, adding a namespace with the minimum size will clear this condition, and the persistent memory module Config Status will appear as "Configured" | 4.0(4a)B |
| CSCvp31928 | For Intel® Optane™ Data Center persistent memory modules in UCS-managed mode, after local security is configured on a server, it can be deleted. This will disable security. | Use host-based tools to configure persistent memory module security. | 4.0(4a)B and C |
| CSCvp40415 | After upgrading to Cisco UCS Manager 4.0(4a), a "Persistent Memory configuration not matching" warning is seen on C-Series and B-Series M5 servers during service profile association.<br>There is no functional impact. Association will still complete without any issues, and the server will successfully boot to the host OS, if installed. | No known workaround. | 4.0(4a)A |
| CSCvo84482 | For Intel® Optane™ Data Center persistent memory modules, the **Health** tab in Cisco UCS Manager displays only the latest health message, regardless of the severity of the message. Thus, lower severity messages can overwrite higher severity messages. | See the CIMC logs for the complete list of health messages. | 4.0(4a)B |

*Table 24: Fabric Interconnect*

| Defect ID | Symptom | Workaround | First Bundle Affected |
|---|---|---|---|
| CSCvp23834 | FTP from the UCS 6454 FI local-mgmt prompt does not work. The terminal is stuck in a loop. | Use SCP to copy the files or logs from the FI. | 4.0(4a)A |
| CSCvo06391 | UCS C125 M5 and C480 M5 server discovery failed at "Discover Bmc Preconfig Pnu OS Peer".<br>On the Ethernet interfaces of the UCS VIC adapter, one of the following symptoms are seen:<br>• Ethernet physical link status shows as down<br>• Ethernet PCS protocol errors<br>On the FEX server interfaces, the Ethernet physical link status shows as "Up".<br>This happens when certain specific models of UCS VIC adapter cards are connected to specific models of Nexus FEXes with specific transceiver/cable-assembly models. These models are:<br>Transceiver media type: 10G-CU<br>UCS VIC adapters models:<br>• VIC 1457<br>• VIC 1455<br>Nexus FEX models:<br>• N2K-C2348UPQ-10GE<br>FEX NX-OS version: 4.0(1d), 4.0(2c), 4.0(3a)<br>Cisco UCS Manager infra bundle versions: 4.0(1d), 4.0(2d), 4.0(3a)<br>One of the following triggering events:<br>• FEX server interface (HIF) physical link flap<br>• Server reboot | Replace the copper transceiver/cable-assembly with an optical transceiver and fiber cable. | 4.0(4a)A<br>Fixed in 4.0(4c). |

| Defect ID | Symptom | Workaround | First Bundle Affected |
|---|---|---|---|
| CSCvp31766 | After upgrading blade servers to Cisco UCS Manager release 4.0(4a), the VMs using VM-FEX interfaces lost connectivity. | Upgrade the firmware to 4.0(4c) or downgrade the firmware to a previously working release. | 4.0(4a) C<br>Resolved in 4.0(4c)C |
| CSCvp89594 | When upgrading to Cisco UCS Manager 4.0(4a), NX-OS hangs on one side of the 6454 Fabric Interconnect while connecting, the command prompt disappears, and the server is unable to connect to NX-OS while in an ssh session. | Reboot the Fabric Interconnect. | 4.0(4a) A<br>Resolved in 4.0(4c)A |
| CSCvo18110 | Fibre Channel-to-NVMe paths to the name spaces that undergo link flaps are lost. | Reboot the host. | 4.0(4a) A<br>Resolved in 4.0(4c)A |
| CSCvp49398 | On a UCS C220 M5 Server using neNIC driver version 1.0.27.0 with VIC 1457 directly connected to the 6454 Fabric Interconnect , using 2-25GE interfaces on each fabric, if a fabric interconnect is rebooted, traffic will drop for over 75 seconds. This issue was also seen with RHEL with a vNIC on a single fabric with fabric failover. | None | 4.0(2b)A<br>4.0(4a) A |
| CSCvq26156 | Upgrade of UCS C-Series servers to 4.0(4c) C-Bundle causes the Cisco 12G Modular SAS HBA to stop discovering/communicating with some Intel S4500 disk drives. This could result in failure of the software upgrade of these drives.<br>This issue only occurres with Controller firmware version 09.00.00.06. | Pre-Upgrade - in host firmware package omit the Raid Controller upgrade.<br>Post-Upgrade - Roll back the Raid Controller firmware to version 00.00.00.58. | 4.0(4a)C<br>Resolved in 4.0(4d)A |

Table 25: BIOS

| Defect ID | Symptom | Workaround | First Bundle Affected |
|---|---|---|---|
| CSCvn73435 | When the system is under reboot stress or any other stress, the Cisco IMC System Event Log (SEL) reports "UPI Correctable errors" for each Second Generation Intel® Xeon® Scalable processor present on the system. | Keep processor C states at BIOS default. | 4.0(4a)B |

Table 26: BMC

| Defect ID | Symptom | Workaround | First Bundle Affected |
|---|---|---|---|
| CSCvp68182 | Upgrading from a Cisco UCS Manager Release earlier than Release 3.2(3j) to Cisco UCS Manager Release 4.0(4a), or upgrading from Cisco UCS Manager Release 4.0(1a), 4.0(1b), or 4.0(1c) to Cisco UCS Manager Release 4.0(4a), causes a small subset of Cisco UCS B200 M5, B480 M5, and S3260 M5 servers to not activate or lose IOM connectivity to the BMC. | If servers have already been upgraded to Cisco UCS Manager Release 4.0(4a) without any issues, continue to use Release 4.0(4a).<br>For servers running a Cisco UCS Manager Release earlier than 3.2(3j), 4.0(1a), 4.0(1b), or 4.0(1c), upgrade to Cisco UCS Manager Release 4.0(2), 4.0(4b) or later.<br>For more information, see the Cisco Software Deferral Notice at https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/sw/SA/SW_Deferral_Notice_CSCvp68182.html | 4.0(4a)B,<br>4.0(4a)C |

Table 27: External Controllers

| Defect ID | Symptom | Workaround | First Bundle Affected |
|---|---|---|---|
| CSCvm15304 | On the UCS C480 M5 servers with two Intel ColdStream drives on PCI Switch1 and PCISwitch Rear, the Intel ColdStream Next 750GB drive link goes to degraded state after a few reboots. | No known workaround. | 4.0(4a)C |

| Defect ID | Symptom | Workaround | First Bundle Affected |
|---|---|---|---|
| CSCvo39645<br>CSCvo89921 | CATERR/IERR occurs on multiple reboots and the system becomes unresponsive during POST. This issue occurs on servers with NVMe drives on mSwitch connected configuration. | When this issue occurs, perform a warm reboot. | 4.0(4a)C |
| CSCvo31178 | Local disk firmware activation fails for a specific drive model of HGST HUS726020ALS210 on S-Series servers. | No known workarounds. If there is a need for the drive firmware to be updated, contact TAC. | 4.0(4a)C |
| CSCvp23760 | After upgrading to Cisco UCS Manager release 4.0(4a) in a setup with Cisco UCS C-series servers, one port of the Qlogic adapter shows as disconnected. | Downgrade the firmware to a previously working release. | 4.0(4a)C<br>Resolved in 4.0(4b)C |
| CSCvo99427 | UCS Central visibility to some UCS Domains is lost. UCSM DME logs will say certificate expired for Central. | If using the self-signed keyring, regenerate the default keyring in UCS Central:<br>`UCSC # connect policy-mgr`<br>`UCSC(policy-mgr)# scope org`<br>`UCSC(policy-mgr) /org# scope device-profile`<br>`UCSC(policy-mgr) /org/device-profile # scope security`<br>`UCSC(policy-mgr) /org/device-profile/security # scope keyring default`<br>`UCSC(policy-mgr) /org/device-profile/security/keyring* # set regenerate yes`<br>`UCSC(policy-mgr) /org/device-profile/security/keyring* #commit-buffer`<br>If using a third-party certificate, regenerate the default keyring, switch to the default keyring, then switch back to the 3rd party certificate keyring. | 4.0(4a) C<br>Resolved in 4.0(4c)C |

| Defect ID | Symptom | Workaround | First Bundle Affected |
|---|---|---|---|
| CSCvo48003 | On UCS M4 servers, an uncorrectable ECC error is detected during Patrol Scrub. When the CPU IMC (Integrated Memory Controller) Patrol Scrubber detects an uncorrectable ECC error, it logs a truncated DIMM address (4KB page boundary) to the Machine Check Banks. | Before replacing it, review the system logs to confirm if the Uncorrectable ECC error was logged for the correct DIMM. | 4.0(4a) B<br>Resolved in 4.0(4c)B |
| CSCvr07248 | Under the Equipment category on the UCS Management GUI, the Policy page for the Power Group shows only information on the General Tab. The tabs for Chassis, Rack Unit, FEX, FI, Faults, and Events do not display information. | Use the CLI for obtaining Power Group information. | 4.0(4a)A<br>Resolved in 4.0(4e)B |

## Open Caveats for Release 4.0(2a)

The following caveats are open in Release 4.0(2a):

| Defect ID | Symptom | Workaround | First Bundle Affected |
|---|---|---|---|
| CSCvo13678 | UCS M5 rack servers with NVIDIA GPUs fail discovery during Cisco UCS Manager Release 4.0(2) rack server firmware install. This is caused by the svc_sam_bladeAG process crashing and producing a core file. | If this issue occurs, downgrade to a release earlier than Cisco UCS Manager Release 4.0(2). | 4.0(2a)A<br>Resolved in 4.0(2d)A |
| CSCvh18287 | Cisco C240 M5 servers are displaying error code F0776 and a fault message stating that non-existent disks are inoperable. | Not an issue, as the fault message is only displayed for non-existent disks. | 4.0(1a)C<br>4.0(2a)C |

| Defect ID | Symptom | Workaround | First Bundle Affected |
|---|---|---|---|
| CSCvk63036 | Unable to form a SAN port-channel or trunking between a Cisco UCS Fabric Interconnect pair and a Cisco Fibre Channel switch when the Organizationally Unique ID (OUI) of the switch is one of the following:<br>• 003a9c<br>• 000831<br>• d0a5a6 | Use single F-Port links without a port-channel. Trunk mode should be OFF for UCS FI and MDS. | 4.0(2a)A<br>Resolved in 4.0(2b)A |
| CSCvn38097 | When a cable is pulled and plugged back in, or when other similar operations that result in link down and link up are performed, an SLES 12 SP3 host with FC-NVMe storage may crash with the following stack trace:<br>`[  809.738358] Call Trace:`<br>`[  809.739728]`<br>`[<ffffffff81302b58>]`<br>`blk_mq_run_hw_queues+0x48/0x90`<br>`[  809.741102]`<br>`[<ffffffff8130441c>]`<br>`blk_mq_requeue_work+0x10c/0x120`<br>`[  809.742454]`<br>`[<ffffffff810989e4>]`<br>`process_one_work+0x154/0x410`<br>`[  809.743803]`<br>`[<ffffffff810995c6>]`<br>`worker_thread+0x116/0x4a0`<br>`[  809.745145]`<br>`[<ffffffff8109ead9>]`<br>`kthread+0xc9/0xe0`<br>`[  809.746463]`<br>`[<ffffffff81616505>]`<br>`ret_from_fork+0x55/0x80`<br>`[  809.752620] DWARF2 unwinder`<br>` stuck at`<br>`ret_from_fork+0x55/0x80`<br>`[  809.753954]` | There is no known workaround. To resolve this issue, an NVMe core with the fix is required. | 4.0(2a)B and C |
| CSCvn50292 | UCS 6454 Fabric Interconnect reboots with IGMP hap reset in slab allocations without any triggers. This issue was observed on a Cisco UCS Manager container restart, but was never observed again with the same or different triggers. | There are no known workarounds.The Fabric Interconnect will reboot in these conditions. | 4.0(2a)A |

| Defect ID | Symptom | Workaround | First Bundle Affected |
|---|---|---|---|
| CSCvn66725 | Service Profile association fails with "Failed to create session-requested operation timed out" error message when trying to enable drive security for Self Encrypted Drives (SEDs) using remote Key Management Interoperability Protocol (KMIP) server on a UCS M4 server connected to a UCS 6454 Fabric Interconnect. | There is no known workaround. | 4.0(1c)B<br>Resolved in 4.0(4a)B |
| CSCvn57345 | After restoring the Cisco UCS Manager full state backup file of a UCS device which was configured, registered, claimed and connected with Cisco Intersight, the device shows up as disconnected in Cisco Intersight. | If this issue occurs, do the following:<br>**1.** Reconfigure the device connector and register it to the cloud.<br>**2.** Delete the device from the cloud inventory.<br>**3.** Claim the device again with Device ID and new claim code (Device MO ID will be new). | 4.0(2a)A<br>Resolved in 4.0(4a)A |
| CSCvo58393 | After upgrading to Cisco UCS Manager Release 4.0, FCoE port channels do not come up, and member links show admin as down. The following errors are seen:<br>`Severity: Critical`<br>`Code: F999676`<br>`Last Transition Time:`<br>`2019-02-26T03:19:45.668`<br>`ID: 23387272`<br>`Status: None`<br>`Description: [FSM:FAILED]:`<br>`Uplink fc port configuration`<br>`on`<br>`B(FSM:sam:dme:SwFcSanBorderDeploy).`<br>`Remote-Invocation-Error:`<br>`[FSM:STAGE:REMOTE-ERROR]:`<br>`Result: service-unavailable`<br>`Code:`<br>`unspecified Message:`<br>`(sam:dme:SwFcSanBorderDeploy:UpdateConnectivity)`<br>`Affected Object:`<br>`sys/switch-B/border-fc`<br>`Name: Fsm Sam Dme Sw Fc San`<br>`Border Deploy Fsm Fail`<br>`Cause: Fsm Failed` | If this issue occurs, do one of the following:<br>• Perform Shut/No shut on the Ethernet/FCoE ports.<br>• Un-configure and re-configure the FCoE port role.<br>• Change the speed of the FCoE uplink port role to any speed (by using the Cisco UCS Manager CLI). | 4.0(2a)A<br>Resolved in 4.0(4a)A |

| Defect ID | Symptom | Workaround | First Bundle Affected |
|---|---|---|---|
| CSCvo66721 | After a VM changes pinning as a result of power-up/power-down, port group change, or VMotion, the MAC address of that VM does not get removed immediately from the MAC address table of the FI to which it is no longer pinned. | If this issue occurs, modify info_ifacl_label= 0x00000021 by using the info_ifacl_label command.<br>As a workaround for this issue, set the 5th bit in existing value of info_ifacl_label.<br>Apply his workaround whenever port shut/no shut happens. | 4.0(2a)A<br>Resolved in 4.0(4a)A |
| CSCvn91826 | In a setup with Cisco VIC 14xx adapters, server discovery may fail when the rack server IDs have exceeded the rack server ID range, which is 1 to 99.<br>The following error message may appear:<br>`ID: 101`<br>`Server: sys/rack-unit-101`<br>`    FSM 1:`<br>`        Remote Result: Service`<br>` Unavailable`<br>`        Remote Error Code:`<br>`1002`<br>`        Remote Error`<br>`Description: command chassis`<br>`associate 101 chassis-serial`<br>`xxxxx`<br>`module-serial xxxxx`<br>`port-profile`<br>`ucsm_internal_rackserver_portprofile`<br>` module-side left`<br>`may need to break down at 8`<br>`        Status: Discover Sw`<br>`Configure Port Channel Local`<br>`        Previous Status:`<br>`Discover Sw Configure Port`<br>`Channel Local`<br>`        Timestamp:`<br>`2019-01-12T23:00:39.348`<br>`        Try: 2`<br>`        Flags: 0`<br>`        Progress (%): 3`<br>`        Current Task:`<br>`Configuring port channel for`<br>`server 101(FSM-STAGE:sam:dme:` | Decommission the affected server and recommission the same server with a server ID less than 99. | 4.0(2a)A<br>Resolved in 4.0(2b)A |

| Defect ID | Symptom | Workaround | First Bundle Affected |
|---|---|---|---|
| CSCvk26441 | When running Cisco UCS Manager Release 4.0(2a) on UCS 6454 Fabric Interconnects, LDAP user login fails if the group map rule has a role other than **aaa** and **read-only**. | There is no known workaround.<br>If this issue occurs, upgrade Cisco UCS Manager to Release 4.0(2b) or later releases. | 4.0(2a)A<br>Resolved in 4.0(2b)A |
| CSCvk53356 | When running Cisco UCS Manager Release 4.0(2a) on UCS 6454 Fabric Interconnects, an admin password cannot be recovered using the password recovery procedure. | There is no known workaround.<br>If this issue occurs, upgrade Cisco UCS Manager to Release 4.0(2b) or later releases. | 4.0(2a)A<br>Resolved in 4.0(2b)A |
| CSCvn60002 | VNICs and VHBAs experience degraded response time in bringing up physical links after power-on or link-flap. Servers configured for `sanboot` sometime fail to boot. This can occur on initial server bringup, on physical link-flap, or on IOM reboot. | If `sanboot` fails, reboot the server. | 4.0(2a)A<br>Resolved in 4.0(2d)A |
| CSCvo04128 | Fibre Channel ports configured in E mode and supported on the UCS 6454 Fabric Interconnect can take an arbitrary amount of time to come online after boot or link-flap. | No workaround. | 4.0(2a)A<br>Resolved in 4.0(2d)A |
| CSCvo22832 | Cisco UCS Manager integrate C-Series servers direct-attached to UCS 6454 Fabric Interconnects using VIC 14xx Series adapters cannot capture CDP/LLDP packets. This is caused by the Fabric Interconnect incorrectly creating the platform header,so that it does not populate the physical interface for transmitting the packets. | No workaround. | 4.0(2a)A<br>Resolved in 4.0(2d)A |

| Defect ID | Symptom | Workaround | First Bundle Affected |
|---|---|---|---|
| CSCvo91744 | After upgrading to Cisco UCS Manager Release 4.0(2), if the Network Control Policy is configured with **MAC Security** set to **Deny**, some servers show VIF down on the upgraded Fabric Interconnect. Cisco UCS Manager displays the following fault on the affected servers:<br>`Severity: Warning`<br>`Code: F78413`<br>`Status: None`<br>`Description:`<br>`[FSM:STAGE:REMOTE-ERROR]:`<br>`Result: service-unavailable`<br>`Code: unspecified Message:`<br>`ERROR: Failed to update`<br>`maximum`<br>`value#(sam:dme:ComputePhysicalAssociate:SwConfigHostOsLocal)`<br>`Affected Object:`<br>`sys/chassis-1/blade-4`<br>`Name: Fsm Sam Dme Compute`<br>`Physical Associate Remote Inv`<br>`Cause: Sw Config Hostoslocal`<br>`Failed`<br>`Type: Fsm`<br>`Acknowledged: No`<br>`Occurrences: 5`<br>`Creation Time:`<br>`Original Severity: Warning`<br>`Previous Severity: Warning`<br>`Highest Severity: Warning`<br>The following is observed in svc_sam_portAG logs:<br>`[MAJOR][][][app_sam_portAG:config]`<br>` Error enabling the port`<br>`security for the ethernet VIF,`<br>`details: ERROR: Failed to`<br>`update maximum value` | Delete the Network Control Policy before the upgrade. | 4.0(2a)A<br>Resolved in 4.0(4a)A |

## Open Caveats for Release 4.0(1d)

The following caveats are open in Release 4.0(1d):

| Defect ID | Symptom | Workaround | First Bundle Affected |
|---|---|---|---|
| CSCvq28261 | Power Supply Units on blade chassis that were using UCS 2304 Fabric Extender with UCS 6324 Fabric Interconnect are shut down by thermal faults during Fabric Extender firmware upgrade. The PSUs can't be powered on afterwards until they are reseated. Re-seating the Power Supply Units could require a complete chassis outage. | Do not upgrade the Fabric Extender firmware if thermal faults are present. Clear the thermal faults before upgrading. | 4.0(1d)B<br>Resolved in 4.0(4c)B |
| CSCvr08327 | Power Supply Units on blade chassis that are using UCS 2204 or UCS 2208 Fabric Extenders were shut down by thermal faults during Fabric Extender firmware upgrade. The PSUs can't be powered on afterwards until they are reseated. Re-seating the Power Supply Units could require a complete chassis outage. | Do not upgrade the Fabric Extender firmware if thermal faults are present. Clear the thermal faults before upgrading. | 4.0(1d)B<br>Resolved in4.0(4e)B |

## Open Caveats for Release 4.0(1c)

The following caveats are open in Release 4.0(1c):

| Defect ID | Symptom | Workaround | First Bundle Affected |
|---|---|---|---|
| CSCvo19661 | Instead of broadcasting Fabric Interconnect Management IP addresses, UCS 6454 Fabric Interconnects are broadcasting KVM out-of-band IP addresses through LLDP upstream ACI leafs and downstream to ESXi hosts through CDP. | This issue can impact ACI VMM provisioning of EPGs, which rely on correct CDP or LLDP information being sent.<br>When using ACI VMM, changing the policy to pre-provision can avoid unexpected issues. | 4.0(1c)A<br>Resolved in 4.0(2e)A |

## Open Caveats for Release 4.0(1a)

The following caveats are open in Release 4.0(1a):

| Defect ID | Symptom | Workaround | First Bundle Affected |
|---|---|---|---|
| CSCvm66006 | After reconfiguring and reassociating service profiles, traffic hashed to one of the hif-pc members gets dropped. This happens when DCBX has not converged properly on the impacted interface of the blade server. | Re-acknowledge the server to recover from this issue.<br>To avoid this issue, do not perform continuous or simultaneous association and reassociation of blade servers. | 4.0(1a)A<br>Resolved in 4.0(4a)A |
| CSCvr98210 | When upgrading from Cisco UCS Manager Release 3.2 to Release 4.0 on a system with appliance ports or FCoE storage ports, LLDP becomes disabled by default. FCoE or any connectivity that requires LLDP may stop working. | To recover connectivity, disable and then re-enable LLDP in the network control policy after upgrading to Cisco UCS Manager Release 4.0. | 4.0(1a)A |
| CSCvo64592 | When attempting to integrate a UCS C-Series server with Cisco UCS Manager Release 4.0 on UCS 6454 Fabric Interconnects, server discovery fails. | If this occurs, reboot the Cisco UCS Manager container or the FI. | 4.0(1a)A<br>Resolved in 4.0(4a)A and 4.0(2e)A |
| CSCvm23975 | In a system with a Cisco UCS Manager-managed C-Series rack server and any V-Series GPU adapter, the GPU mode cannot be changed through the Graphics Policy in Cisco UCS Manager.<br>This happens when the C-Series rack server has one or more of the following GPU adapters:<br>• UCSC-GPU-V100-16G<br>• UCSC-GPU-V100-32G | If this occurs, configure the graphics mode by using the native NVIDIA 'nvidia-smi' utility tool on any supported OS. | 4.0(1a)A<br>Resolved in 4.0(2a)A |

| Defect ID | Symptom | Workaround | First Bundle Affected |
|---|---|---|---|
| CSCvm14726 | Cisco UCS 6324 Fabric Interconnects with the new SPI Flash device cannot boot with previous software releases. This is because the original SPI Flash device used on the 6324 Fabric Interconnect is no longer being produced; hence a pin-compatible replacement part is being used going forward. However, due to the vendor and part ID changing, the 6324 Fabric Interconnect equipped with the new part can only operate with OS versions that have support for the new part built in. | When using Cisco UCS 6324 Fabric Interconnects with the new SPI Flash device, use only those releases that came out after the hardware change on the 6324 Fabric Interconnect was introduced. | 4.0(1a)A<br>Resolved in 4.0(1c)A |
| CSCvk30528 | In UEFI boot mode, Cisco UCS Managed C-Series servers fail to boot to the RHEL or ESXi OS installed on an iSCSI LUN configured on an EMC storage device. Instead, the server enters into the UEFI shell prompt after every reboot.<br>The server boots to the OS as expected if the LUN is from any other storage device than EMC. | After the server enters into UEFI shell prompt, exiting the shell prompt boots the server to the OS. | 4.0(1a)C<br>Resolved in 4.0(1c)C |
| CSCvm17259 | In a system with a Cisco UCS Manager integrated C-Series rack server, the firmware for the UCSC-GPU-V100-32G GPU is not seen in the Host Firmware Pack (HFP) of the firmware policy after configuring the service profile for the server. | If this issue occurs, do the following:<br>• Move the server to Standalone mode from Cisco UCS Manager-managed mode.<br>• Update the server through the Host Update Utility (HUU) iso.<br>• After the update is complete, bring the server back up in Cisco UCS Manager-managed mode. | 4.0(1a)A<br>Resolved in 4.0(1b)A |
| CSCvm10391 | The Cisco UCS 6454 Fabric Interconnect does not send any Call Home messages to the configured SMTP server. | No known workaround. | 4.0(1a)A<br>Resolved in 4.0(1b)A |

| Defect ID | Symptom | Workaround | First Bundle Affected |
|---|---|---|---|
| CSCvm03356 | Cisco UCS B-Series M3 servers and C-Series M3 servers are based on Intel® processors that are vulnerable to exploits that use CPU speculative processing and data cache timing to potentially identify privileged information. These exploits are collectively known as L1 Terminal Fault (L1TF).<br>- CVE-2018-3615 (affecting SGX), also known as Foreshadow, is not known to affect any existing Cisco UCS servers because Cisco UCS M5 and earlier generation servers, and HyperFlex M5 and earlier generation servers do not use Intel® SGX technology.<br>- CVE-2018-3620 (affecting OS/System Management Mode) and CVE-2018-3646 (affecting Virtual Machine Monitors) are referred to as L1 Terminal Fault attacks by Intel®. These vulnerabilities are mitigated by applying the updated processor microcode from Intel included in the server firmware bundle, and the relevant Operating System and Hypervisor patches from the appropriate vendors. | The fix for CVE-2018-3620 (OS/SMM) and CVE-2018-3646 (VMM) requires applying the updated processor microcode from Intel® as well as the relevant Operating System and Hypervisor patches from the appropriate vendors.<br>For more information, please see the Cisco Security Advisory available here:<br>CPU Side-Channel Information Disclosure Vulnerabilities: August 2018 | 4.0(1a)B, 4.0(1a)C<br>3.2(1d)B, 3.2(1d)C<br>3.1(1e)B, 3.1(1e)C<br>2.2(1b)B, 2.2(1b)C<br>CSCvm03356 is resolved in 4.0(1a)B, 4.0(1a)C |

| Defect ID | Symptom | Workaround | First Bundle Affected |
|---|---|---|---|
| CSCvm03351 | Cisco UCS B-Series M4 servers, C-Series M4 servers, S3260 M4 storage servers, and HyperFlex M4 servers are vulnerable to exploits that use CPU speculative processing and data cache timing to potentially identify privileged information. These exploits are collectively known as L1 Terminal Fault (L1TF).<br>• CVE-2018-3615 (affecting SGX), also known as Foreshadow, is not known to affect any existing Cisco UCS servers because Cisco UCS M5 and earlier generation servers, and HyperFlex M5 and earlier generation servers do not use Intel® SGX technology.<br>• CVE-2018-3620 (affecting OS/System Management Mode) and CVE-2018-3646 (affecting Virtual Machine Monitors) are referred to as L1 Terminal Fault attacks by Intel®. These vulnerabilities are mitigated by applying the updated processor microcode from Intel included in the server firmware bundle, and the relevant Operating System and Hypervisor patches from the appropriate vendors. | The fix for CVE-2018-3620 (OS/SMM) and CVE-2018-3646 (VMM) requires applying the updated processor microcode from Intel® as well as the relevant Operating System and Hypervisor patches from the appropriate vendors.<br>For more information, please see the Cisco Security Advisory available here:<br>CPU Side-Channel Information Disclosure Vulnerabilities: August 2018 | 4.0(1a)B, 4.0(1a)C<br>3.2(1d)B, 3.2(1d)C<br>3.1(1e)B, 3.1(1e)C<br>2.2(1b)B, 2.2(1b)C<br>CSCvm03351 is resolved in 4.0(1a)B, 4.0(1a)C |

| Defect ID | Symptom | Workaround | First Bundle Affected |
|---|---|---|---|
| CSCvm03339 | Cisco UCS B-Series M5 servers, C-Series M5 servers, and HyperFlex M5 servers are based on Intel® processors that are vulnerable to exploits that use CPU speculative processing and data cache timing to potentially identify privileged information. These exploits are collectively known as L1 Terminal Fault (L1TF).<br>• CVE-2018-3615 (affecting SGX), also known as Foreshadow, is not known to affect any existing Cisco UCS servers because Cisco UCS M5 and earlier generation servers, and HyperFlex M5 and earlier generation servers do not use Intel® SGX technology.<br>• CVE-2018-3620 (affecting OS/System Management Mode) and CVE-2018-3646 (affecting Virtual Machine Monitors) are referred to as L1 Terminal Fault attacks by Intel®. These vulnerabilities are mitigated by applying the updated processor microcode from Intel included in the server firmware bundle, and the relevant Operating System and Hypervisor patches from the appropriate vendors. | The fix for CVE-2018-3620 (OS/SMM) and CVE-2018-3646 (VMM) requires applying the updated processor microcode from Intel® as well as the relevant Operating System and Hypervisor patches from the appropriate vendors.<br>For more information, please see the Cisco Security Advisory available here:<br>CPU Side-Channel Information Disclosure Vulnerabilities: August 2018 | 4.0(1a)B, 4.0(1a)C<br>3.2(1d)B, 3.2(1d)C<br>3.1(1e)B, 3.1(1e)C<br>2.2(1b)B, 2.2(1b)C<br>CSCvm03339 is resolved in 4.0(1a)B, 4.0(1a)C |
| CSCvh06851 | When an adaptor that is sending both Drop and No-Drop QoS class traffic encounters conjestion, the IOM sends the incomplete value of the user-configured PFC priority map to the adaptor. Because of this, all QoS classes are treated as No-Drop, and the adaptor slows down both Drop and No-Drop traffic to the IOM. | There is no known workaround. | 3.2 (2b)A |

| Defect ID | Symptom | Workaround | First Bundle Affected |
|---|---|---|---|
| CSCvi66859 | In a system configured with VLAN groups and mapped with FI uplink interfaces, an unexpected outage is experienced when a VLAN is removed from a vNIC template or from a VLAN group. | When a VLAN group is used by both uplinks and vNICs, do the following before a VLAN is removed from the VLAN group:<br>**1.** Add the VLAN to the uplink explicitly.<br>**2.** Remove the VLAN from the VLAN group.<br>**3.** Wait until the VLAN is removed from all vNICs and then remove the VLAN from the uplink. | 3.2(2b)A<br>Resolved in 4.0(2a)A |
| CSCvj17303 | A httpd core is observed during upgrade and downgrade of Cisco UCS Manager between Releases 3.2(3a) and 4.0(1a). | There is no known workaround. httpd restarts automatically. | 4.0(1a)A |
| CSCux48594 | When upgrading Cisco UCS Manager from Release 2.5(2a) to Release 3.1 and later releases, a DME core occurs. | Do not take any action when the DME core occurs. The upgrade process will continue and complete successfully. | 3.1(1e)A |
| CSCvh69831 | In a setup with Cisco UCS B260 or B460 M4 servers with eight vNICs, after installing ESXi 6.0/6.5, the second half of the vNICs on host port 2 are ordered first in ESXi. Thus, the vNICs are out of order during initial install. | Manually configure the NIC placement policy so that the second half of the vNICs are ordered first.<br>OR<br>Manually assign the second half of the vNICs to host port 1. | 3.1(3b)B |
| CSCvj98360 | BMC does not detect the DIMM and blade server discovery is stuck with the following message:<br>`Mismatched DIMM configuration` | Power down the host and reboot the BMC to recover from this state. | 4.0(1a)B<br>Resolved in 4.0(1d)B |

| Defect ID | Symptom | Workaround | First Bundle Affected |
|---|---|---|---|
| CSCvn49417 | While setting up a new UCS 6454 Fabric Interconnect, when you boot to the initial configuration, the network uplinks come online before the Fabric Interconnect is configured. Network links come online prematurely and may cause a broadcast storm in rare instances.<br>Further, CDP neighbor information is displayed and MAC addresses of UCS 6454 Fabric Interconnects from earlier deployments are being learnt at this stage. | To avoid this scenario, ensure that your network uplinks are down until initial configuration of the Fabric Interconnect is complete.<br>If this issue occurs, shut down upstream switch connections. | 4.0(1a)A |
| CSCvn22595 | When using UCS B200 M5 servers with VIC 1340 and VIC 1380 adapters on a system running Cisco UCS Manager 3.2(3d) firmware and Red Hat Linux as the OS, vNICs that share the same bus ID are assigned to the same Input-Output Memory Management Unit (IOMMU) group, despite having different function numbers. | No workaround. | 3.2(3d)B<br>Resolved in 4.0(2d)B |
| CSCvn81327 | The Cisco 2304 IOM crashes and produces a kernel core dump that points to `pick_next_task_rt`. If this condition is encountered, traffic forwarding ceases until a watchdog timer triggers a reboot. However, prior to the reboot, ports still appear as up even though the traffic to the affected module is lost. | No workaround. | 3.2(2d)C<br>Resolved in 4.0(2d)C |
| CSCvm66499 | The launch KVM feature is not functional after Fabric Interconnect cluster failover when in-band KVM VLAN is configured and the server management is connected through FEX. | Perform a re-acknowledge to the server. | 4.0(1a)C<br>Resolved in 4.0(2d)C |
| CSCvh18287 | Cisco UCS C240 M5 servers display error code F0776 and a fault message stating that non-existent disks are inoperable. | N/A. Message is for drives that do not exist. | 4.0(1a)A<br>3.2(1d)A<br>Resolved in 4.0(2d)A |

| Defect ID | Symptom | Workaround | First Bundle Affected |
|---|---|---|---|
| CSCvm66118 | When a PSU with serial number LITxxxxxx is inserted or reseated in a chassis connected to a UCS 6300 Series Fabric Interconnect, it may cause the Fabric Interconnect to report PSU fan faults. However, the PSU LED remains green and the PSU and the fans continue to work. | Do not reseat the PSU if it is not necessary.<br>If reseating or moving this PSU is required, reboot the Fabric Interconnect after the PSU is inserted. | 3.2(2f)B<br>Resolved in 4.0(2d)A |
| CSCvm89871 | Cisco UCS Manager integrated C-Series rack servers on UCS 6332 or 6332-16UP Fabric Interconnects fail discovery when the following sequence of actions occurs:<br>**1.** Disable the port that is part of the uplink Ethernet port-channel.<br>**2.** 2. Delete the interface from the port-channel.<br>**3.** Re-configure the port type as **Server** .<br>**4.** Connect the server to the re-configured port. | **1.** With the Fabric Interconnect and rack server powered on, connect the cables between them.<br>**2.** Configure the FI port type as **Uplink**.<br>**3.** Configure the port type as **Server**. | 3.1(2c)A<br>Resolved in 4.0(2d)A |
| CSCvn82697 | Despite the locale being defined on a sub-organization, remotely authenticated users can see all the organizations. | None | 3.2(3g)A<br>Resolved in 4.0(2e)A |
| CSCvn77413 | Ethernet ports on a 6332 or 6332-16 UP Fabric Interconnect showed high input discard counts, but with no appreciable performance impact. | Match upstream VLANs to VLANs created on the Fabric Interconnect. | 3.2(3h)A<br>Resolved in 4.0(2e)A |

| Defect ID | Symptom | Workaround | First Bundle Affected |
|---|---|---|---|
| CSCvr04369 | | Use a transceiver type that uses the Ethernet Auto-Negotiation protocol. These transceivers are:<br>• 40G CR<br>• 100G CR | 4.0(4d)B<br>Resolved in4.0(4e)B |

| Defect ID | Symptom | Workaround | First Bundle Affected |
|---|---|---|---|
| | The link status of the Ethernet port of a Cisco UCS 14xx adapter card, and of the attached switch port, fails to come up multiple times. In typical cases, the following symptoms further characterize this issue:<br>- Ethernet physical link status keeps flapping (CSCvr09649).<br>- The following counters have a positive value and increment:<br>`dbgcli:2> bod-serdes_error`<br>`  uif  lane   nif`<br>`------------------`<br>`   0    0    0`<br>`...`<br>`linkup_failure = 1275`<br>`...`<br>`LINKUP_FAILED = 1275`<br>- The following counters have a positive value and increment:<br>`dbgcli:2> bod-pcs_err 0 0`<br>`0-0: linkdown with pcs`<br>`error happened 311 times`<br>These counters have been available since the following releases: Cisco UCS Manager (C-Bundle) 4.0(4c), CIMC/HUU 4.0(4e), VIC Firmware 5.0(3c)).<br>This issue has been observed in practice on a limited number of instances of the Cisco UCS VIC 1457 adapter card model, on physical Ethernet port 1, when equipped with a limited set of 25G optical transceiver modules.<br>Manifestations of the issue are extremely rare and highly specific to the following elements of a deployment environment:<br>- Cisco VIC 14xx adapter card | | |

| Defect ID | Symptom | Workaround | First Bundle Affected |
|---|---|---|---|
| | instance and port instance:<br>• Cisco UCS VIC 1455<br>• Cisco UCS VIC 1457<br>• Cisco UCS VIC 1495<br>• Cisco UCS VIC 1497<br>• Transceiver module instances that do not use the Ethernet Auto-Negotiation protocol:<br>• 10G CU<br>• 10G Optical<br>• 25G CU<br>• 25G Optical<br>• 40G Optical<br>• 100G Optical<br>• Other possible environmental conditions. | | |
| CSCvr95393 | A TACACS user is able to login to the Fabric Interconnect even when the NOLOGIN policy has been set. | | 4.0(1a)A<br>Resolved in 4.0(4k)A |
| CSCvr83759 | After upgrading from UCS Manager 3.2(3c) to 4.0(4c), blade server access to UCS Manager Fabric Interconnects fails when using openSSH or SecureCRT with "password" authentication. | None | 3.2(3e)A<br>Resolved in 4.0(4h)A |
| CSCvj70519 | Port 7162, used for UCS communications, is open on the 6400 Series Fabric Interconnects. | None | 4.0(1a)A<br>Resolved in 4.0(4g)A |

| Defect ID | Symptom | Workaround | First Bundle Affected |
|---|---|---|---|
| CSCvr06387 | The SNMP process on the UCS 6324 Fabric Interconnect crashes repeatedly. Messages similar to the following are displayed:<br>`TIMESTAMP HOSTNAME %CALLHOME-2-EVENT: SAM_ALERT_DIAGNOSTIC_MINOR`<br>`TIMESTAMP HOSTNAME` plus last message repeated 2 times<br>`TIMESTAMP HOSTNAME` plus last message repeated 1 time<br>`TIMESTAMP HOSTNAME %SYSMGR-2-SERVICE_CRASHED: Service "snmpd" (PID XX) hasn't caught signal 6 (core will be saved).`<br>`TIMESTAMP HOSTNAME %CALLHOME-2-EVENT: SW_CRASH snmpd in slot 1 crashed with crash type : stateful crash` | N/A | 4.0(1a)A<br>Resolved in 4.0(4g)A |
| CSCvq37888 | On UCS M4 Servers, connectivity between UCS Manager and the Cisco IMC is lost due to the Cisco IMC running out of memory. Connectivity could not be restored until the blade was re-seated. | Reset the blade from UCS Manager.<br>Re-seat the blade.<br>Stop running port scanners on the KVM port of Cisco IMC IP addresses; the default KVM port number is 2068. | 4.0(1a)A<br>Resolved in 4.0(4g)A |
| CSCvq77449 | Restarting CMC2 on UCS S3260 M5 servers causes all virtual drives configured in both dual RAID controllers to go offline. All other physical drives, except the boot drives, display **Foreign Configuration** status. | Reboot the server to auto-import the drive configurations displaying **Foreign Configuration** status.<br>If auto-import during reboot fails, contact TAC to import the configuration. | 4.0(1a)C |
| CSCvr15733 | Under load, a vNIC becomex permanently nonfunctional due to rate limit shutoff issues. | None | 4.0(1a)A<br>Resolved in 4.0(4h)A |
| CSCvs61735 | UCS Manager doesn't provide correct overall status for the IOM on a Cisco 6400 Series Fabric Interconnect. | None | 4.0(1a)A<br>Resolved in 4.0(4i)C |

| Defect ID | Symptom | Workaround | First Bundle Affected |
|---|---|---|---|
| CSCvt27869 | A 6200 series Fabric Interconnect encounters an OOB memory access, causing the Fabric Interconnect to reboot. | None | 4.0(1a)A<br>Resolved in 4.0(4i)C |
| CSCvr04665 | When SFP-H25G-CU5M cable is used between VIC 1455/1457 adaptors with a VIC firmware version lower than 5.1(2a) and 6400 series fabric interconnects, the link between the adaptor and the 6400 Series fabric interconnect sometimes fails to link up. | Use any of the following cables as workaround:<br>• 25G AOC cables or 25G optical transceivers<br>• SFP-H25G-CU3M or shorter cables | 4.0(1a)<br>Resolved in 4.0(4k) |

## Behavior Changes and Known Limitations

### Fibre Channel Ports Experiencing txmit Credit Loss Are Now Disabled

CSCvq76790—As of the 4.0(4h) release, UCS Fabric Interconnect fibre channel links disable ports experiencing txmit credit loss. By default, the UCS Fabric Interconnect now error-disable the FC port whenever the port monitor feature detects a threshold of 30 credit loss over 2 minutes period on the FC port. The message `error disable fc port, if_index: <if_index_value>` is logged in the fcpc trace log

This change affects all Fibre Channel type ports, uplinks, and storage appliance ports.

### Cannot Create Virtual Drives with Cached IO Policy Enabled

CSCvn72355—Beginning with Cisco UCS Manager Release 4.0(4), you cannot create a virtual drive (VD) on systems with the **IO Policy** set to **Cached**. While creating a VD, Cached IO policy is disabled on Cisco UCS Manager GUI and CLI, Cisco IMC and LSI Storage Authority (LSA). By default, new VDs will now be created with Direct IO policy. Any existing VD that is configured with Cached IO policy will automatically be modified to Direct IO policy.

Systems with Cisco UCS Manager Release 4.0(4) and later releases, will not have the **IO Policy** set to **Cached** while creating the VD. After upgrading to Release 4.0(4), ensure that you modify the **IO Policy** to **Direct** for storage profiles.

### FSM Discovery Takes Longer to Complete for UCS 6454 Fabric Interconnects

Under certain conditions, FSM discovery after a Fabric Interconnect failover takes longer to complete on UCS 6454 Fabric Interconnects than it takes on UCS 6200 Series and 6300 Series Fabric Interconnects. This is because of the discovery algorithm being used for UCS 6454 Fabric Interconnects.

### Cisco UCS Manager Version No Longer Displayed on the UI Login Screen

Beginning with Cisco UCS Manager Release 4.0(4a), the Cisco UCS Manager release version is no longer displayed on the UI login screen.

### Allowed WWPN and WWNN Ranges for a WWN Pool

Beginning with Cisco UCS Manager Release 4.0(1a), the allowed WWPN and WWNN ranges for a WWN pool in Cisco UCS 6454 FIs are changed from:

20:00:00:00:00:00:00:00 to 20:FF:FF:FF:FF:FF:FF:FF or 50:00:00:00:00:00:00:00to 5F:FF:FF:FF:FF:FF:FF:FF

to

20:00:00:00:00:00:00:00 to 20:FF:**00**:FF:FF:FF:FF:FF or from 50:00:00:00:00:00:00:00 to 5F:FF:**00**:FF:FF:FF:FF:FF

The third octet of the WWPN must remain **00**.

When Fibre Channel traffic is sent through the Cisco UCS infrastructure, the source WWPN is converted to a MAC address. The WWPN pool range changes are implemented to avoid values that can translate to a source multicast MAC address.

### Compatibility Between Infrastructure and Host Firmware Versions on a C480 M5 Servers with an MSwitch

CSCvp13552—For a C480 M5 server, beginning with Cisco UCS Manager Release 4.0(4a), the compatibility between A and C bundles for the MSwitch firmware upgrade has changed to the following:

| | Host Firmware Versions (C Bundle) Earlier Than 4.0(4a) | Host Firmware Versions (C Bundle) 4.0(4a) and Later |
|---|---|---|
| **Infrastructure Versions (A Bundle) Earlier Than 4.0(4a)** | Compatible | Incompatible |
| **Infrastructure Versions (A Bundle) 4.0(4a) and Later** | Incompatible | Compatible |

On C480 M5 servers with an MSwitch, to upgrade the MSwitch firmware from a release earlier than 4.0(4) to Release 4.0(4), do the following in order:

1. Upgrade the Infrastructure A bundle to Release 4.0(4).
2. Perform decommission/recommission or re-acknowledgement of the C480 M5 server to update the invTag and model name for the front MSwitches.
3. Upgrade the C bundle to Release 4.0(4).

### Compatibility Between Infrastructure and Host Firmware Versions for NVIDIA V100 Series GPUs

CSCvp05259—Beginning with Cisco UCS Manager Release 4.0(4a), when upgrading firmware for NVIDIA SXM2 V100 32GB and NVIDIA V100 PCIe 32GB GPUs, the compatibility between A and C bundles has changed to the following:

| | Host Firmware Versions (C Bundle) Earlier Than 4.0(4a) | Host Firmware Versions (C Bundle) 4.0(4a) and Later |
|---|---|---|
| **Infrastructure Versions (A Bundle) Earlier Than 4.0(4a)** | Compatible | Incompatible |
| **Infrastructure Versions (A Bundle) 4.0(4a) and Later** | Compatible | Compatible |

### UCS 6300 Series Fabric Interconnect ASIC Limitation with Passive Cables

UCS 6300 Series FIs support passive cables, except on the uplink ports. The ASIC on the FI does not support auto-negotiation (CSCvc98464), which is why only active cables are recommended for use on uplink ports.

This limitation also applies when connecting non-uplink ports to upstream switch ports that do not support auto-negotiation. When using passive cables, the link may not work because the 6300 Series FI uses auto-negotiation, and the peer switch port does not support it. You cannot disable auto-negotiation on the 6300 Series FI, which is why Cisco recommends that you use active cables in such a scenario.

### Booting Becomes Unresponsive on RHEL 7.5 or 7.6, and the usNIC Functionality is Affected

Booting becomes unresponsive on Red Hat Enterprise Linux version 7.5 or 7.6 when both usNIC devices are provisioned on the VIC through Cisco UCS Manager or Cisco IMC, and the Intel or AMD Input Output Memory Management Unit (IOMMU) is enabled.

This is because Linux API signatures in RHEL v7.5 and v7.6 exposed a race condition in the inbox usnic_verbs.ko drivers, causing the boot to hang.

When this happens, do the following:

1. Boot the device with the Intel or AMD IOMMU disabled.
2. Download the enic_verbs or usnic_verbs drivers from Cisco.com and install. Unlike the inbox usnic_verbs driver, these drivers do not hang on boot.
3. Re-enable the Intel or AMD IOMMU.

Boot should proceed normally and usNIC functionality will be restored.

### Algorithm Support in OpenSSH to Log into Servers through the SSH

Starting with Cisco UCS Manager Release 4.0, certain insecure ciphers are blocked by UCS Fabric Interconnects. To log into servers through the SSH protocol, you must use a version of OpenSSH that supports at least one algorithm in the following categories:

- Key exchange algorithms supported from Cisco UCS Manager Release 4.0(2a)
  - For Cisco Fabric Interconnect 6454
    - ecdh-sha2-nistp256
    - ecdh-sha2-nistp384
    - ecdh-sha2-nistp521
    - diffie-hellman-group-exchange-sha256
    - diffie-hellman-group16-sha512
    - diffie-hellman-group18-sha512
    - diffie-hellman-group-exchange-sha1
    - diffie-hellman-group14-sha1
  - For Cisco Fabric Interconnect 6248, 6324 and 63xx
    - diffie-hellman-group-exchange-sha256

        - diffie-hellman-group16-sha512
        - diffie-hellman-group18-sha512

- Key exchange algorithms supported from Cisco UCS Manager Release 4.0(4a)
    - For Cisco Fabric Interconnect 6454
        - ecdh-sha2-nistp256
        - ecdh-sha2-nistp384
        - ecdh-sha2-nistp521
        - diffie-hellman-group16-sha512
        - diffie-hellman-group14-sha1
    - For Cisco Fabric Interconnect 6248, 6324 and 63xx
        - diffie-hellman-group-exchange-sha256
        - diffie-hellman-group16-sha512
- Encryption algorithms
    - aes128-ctr
    - aes192-ctr
    - aes256-ctr
- MAC algorithms
    - hmac-sha2-256
    - hmac-sha2-512

### Priority Flow Control and Link-Level Flow Control on UCS 6454 Fabric Interconnects

When an interface on a UCS 6454 Fabric Interconnect has Priority Flow Control (PFC) admin configured as **auto** and Link-Level Flow Control (LLFC) admin configured as **on**, the PFC operation mode will be **off** and the LLFC operation mode will be **on**.

On UCS 6300 Series and earlier Fabric Interconnects, the same configuration will result in the PFC operation mode being **on** and the LLFC operation mode being **off**.

### UCS M5 BIOS Tokens for Fast Boot

Cisco UCS Manager Release 4.0(2) introduces the following BIOS tokens to improve boot time for UCS M5 servers:

- Adaptive Memory Training Control
- OptionROM Launch Optimization Control
- BIOS Tech Message Level Control

The default value for all three tokens is **Enabled**.

When the server bundle is upgraded to Cisco UCS Manager Release 4.0(2), but the infrastructure bundle is not upgraded to Release 4.0(2), the servers will use these tokens with their default value, which is **Enabled**. In this scenario, these tokens cannot be managed through Cisco UCS Manager.

To obtain policy level control for these tokens, while continuing with an older Infrastructure bundle, upgrade the Cisco UCS Manager catalog to Release 4.0(2).

### Board Controller Activation for UCS C240 M5 Servers with LITE-ON 1050W PSU May Fail During Downgrade from Cisco UCS Manager Release 4.0(2)

CSCvm08504—Board controller activation for UCS C240 M5 servers with LITE-ON 1050W PSU may fail during the discovery process when it is downgraded from Cisco UCS Manager Release 4.0(2). The following error message is displayed:

```
Error: PSU2 update failed
```

If this error occurs, retry downgrade.

To avoid this error, do not downgrade systems equipped with LITE-ON 1050W PSUs.

### Physical Displays for Servers Introduced in Cisco UCS Manager Release 3.2(3) and Later Releases Appear Incorrectly in the Java KVM Console

CSCvk24995—In the Java KVM console, the physical displays for Cisco UCS Manager-managed UCS servers introduced in Cisco UCS Manager Release 3.2(3) and later releases appear incorrectly. For example, the C125 M5 Server appears incorrectly as C240-M4L.

In the HTML KVM console, the physical displays appear correctly for all Cisco UCS Manager-managed UCS servers.

### System Restore with Unsupported Features

CSCvk21286—In Cisco UCS Manager Release 4.0(1), if a full state backup is collected on a UCS 6200 Series Fabric Interconnect with the following unsupported features, then full state restore cannot be used to restore this file on a UCS 6454 Fabric Interconnect:

- Chassis Discovery Policy and Chassis Connectivity Policy are in non port channel mode
- Switching mode is either Ethernet or FC
- Virtual Machine Management is enabled - VMware, Linux KVM, or Microsoft Hypervisor

### Port Auto-Discovery Policy with 25G Cables and UCS 6454 Fabric Interconnects

CSCvk00796—Port Auto-Discovery policy does not work when a rack server with UCS VIC 1455 is connected to a UCS 6454 Fabric Interconnect through a 25G cable. In such scenarios, manually configure the server port.

### Single Link Port Channel for FC/FCoE between VIC 1455 or VIC 1457 Adapters and UCS 6300 Fabric Interconnects

Cisco UCS Manager Release 4.0(1) supports only single link port channel for FC/FCoE between VIC 1455 or 1457 adapters that are on direct-connect rack-servers, and UCS 6300 Series Fabric Interconnects.

**Note** Do not add a second port channel link between VIC 1455 or 1457 adapters that are on direct-connect rack-servers, and UCS 6300 Series Fabric Interconnects.

### Exceeding Maximum CQ Value Results in Configuration Failure

Modifying the VMMQ adapter policy through the VMQ connection policy results in exceeding the maximum Completion Queue (CQ) value. Each VIC 1400 Series adapter supports a maximum of 1984 user-configurable hardware CQ resources. If this number is exceeded, the `Out of CQ Resources` error appears in the Cisco UCS Manager GUI, and vNIC creation fails with a configuration failure at service profile association.

### FC Uplink Port at 8 Gbps Must Use IDLE as Fill Pattern

CSCvj31676—For Cisco UCS 6454 fabric interconnect, if the FC uplink speed is 8 Gbps, set the fill pattern as IDLE on the uplink switch. If the fill pattern is not set as IDLE, FC uplinks operating at 8 Gbps might go to an errDisabled state, lose SYNC intermittently, or notice errors or bad packets.

### FI Port Does Not Auto-Detect Change in Port Speed

CSCvi45111—On a UCS rack-mount server with a UCS 14xx VIC ASIC, when you replace a 25G cable with a 10G cable, the corresponding FI port goes down and stays in a suspended state. Ports do not auto-detect the change in port speed from 25G to 10G. To recover from this state, decommission and then recommission the rack-mount server.

### C125 M5 Server Boot Mode

CSCvj41626—C125 M5 Server supports only UEFI boot mode.

### Cisco VIC 1455 and 1457 Connectivity

The FEX to FI uplink should be configured in port channel.

### vNIC MTU configuration

For VIC 14xx adapters:

- The vNIC's MTU size can be changed from the host interface settings. The value must be equal to or less than the MTU specified in the associated QoS system class. If this MTU value exceeds the MTU value in the QoS system class, packets may be dropped during data transmission.
- When the Overlay network is configured, the overall MTU size must not exceed the MTU value in the QoS system class.

### Microsoft Standalone NIC Teaming and Virtual Machine Queue Support for VIC14xx Adapters

Microsoft standalone NIC teaming works only with Virtual Machine Queue (VMQ). For VIC 14xx adapters, VMQ is VMMQ with single queue. In order to support this, you must create a new VMMQ adapter policy with 1 TQ, 1 RQ and 2 CQ combination and assign it to the VMQ Connection Policy.

### Chassis Discovery Policy and Chassis Connection Policy

Chassis Discovery Policy and Chassis Connection Policy are not supported for new generation SIOC for M5 servers. Cisco UCS Manager shows an error if you try to configure a chassis discovery policy or chassis connection policy.

## Known Limitations in Release 4.0(4)

The following caveat is the known limitations in Release 4.0(4):

| Defect ID | Symptom | Workaround | First Affected Release |
|---|---|---|---|
| CSCvr67677 | Cisco UCS C220 M4 and C240 M4 servers with specific on-board NAND flash, which run Cisco IMC release 3.0(4d) or earlier, fail to upgrade to any new Cisco IMC release due to bad blocks on NAND flash.<br>This issue does not impact server operation, only the ability to upgrade Cisco IMC.<br>Following error is seen while upgrading HUU:<br>`ERROR: CIMC Update failed (Error Code 1902)`<br>Following FSM state of the server is seen in Cisco UCSM integrated servers:<br>`wait-foribmcfw_update-failed` | Cisco recommends that you contact TAC to check for the number of bad blocks in the NAND flash before attempting firmware upgrade. It is recommended to fix the condition before attempting the upgrade rather than fixing it after a failed Cisco IMC firmware upgrade.<br>Debug plug-in is loaded to inspect the bad block and fix the condition if the system is determined to have too many bad blocks on the NAND flash.<br>If you are already facing this issue, contact TAC to verify the bad blocks and recover them. | 4.0(4b) |

| Defect ID | Symptom | Workaround | First Affected Release |
|---|---|---|---|
| CSCvr42736 | When the Fabric link connected between a 6300 Series Fabric Interconnect and IOM is 40GBASE-CR4 QSFP type copper cable, auto infrastructure upgrade fails with the error`IOM activation stuck at "Pending Next Boot"`.<br>This issue is NOT observed on other cable types. | Use the following procedure:<br>**1.** Log in to the UCS Manager GUI.<br>**2.** Select either the A (primary) or B (subordinate) Fabric Interconnect Ethernet ports as follows:<br>• **Equipment** > **Fabric Interconnects** > **Fabric Interconnect A (primary)** > **Physical ports** > **Ethernet ports**<br>• **Equipment** > **Fabric Interconnects** > **Fabric Interconnect B (subordinate)** > **Physical ports** > **Ethernet ports**<br>**3.** Select the Fabric ports that are connected to the IOM and unconfigure them.<br>**4.** Reconfigure the Fabric ports as server ports. | 4.0(4e)A |

## 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