Release Notes for Cisco UCS Manager, Release 4.1

First Published: 2020-02-20

Last Modified: 2023-11-27

Cisco UCS Manager

Cisco UCS™ Manager, Release 4.1 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 4.1. 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 4.1(x) is supported from Release 3.1(3), Release 3.2(3), and later releases. For UCS Mini and UCS-FI-63xx series Fabric Interconnects, upgrading directly to Cisco UCS Manager Release 4.1(x) is supported from Release 3.1(3), and Release 3.2(3) and later releases. See *Cisco UCS Manager Firmware Management Guide, Release 4.1* for details.

Deprecation Notice

Deprecated Release 4.1(3a)

Release 4.1(3a) is deprecated and firmware files are no longer available.

Cisco recommends that you upgrade to release 4.1(3b) or later. For more information, refer to the Deferral Notice: https://www.cisco.com/web/software/DefTracker/downloads/1311/CSCvx11527.html.

Deprecated Release 4.1(1c)

Release 4.1(1c) is deprecated and firmware files are no longer available. For more information, refer Field Notice: FN - 70595.

Cisco recommends that you upgrade to release 4.1(1d) or later.

Deprecation of Older Release Bundles

As of release 4.1(3d), the following bundles are deprecated and no longer available.

- ucs-c-fusion-io-pfio365m.7.1.17.gbin
- ucs-c-fusion-io-pfio785m.7.1.17.gbin
- ucs-c-fusion-io-pfio1205m.7.1.17.gbin
- ucs-c-fusion-io-pfio3000m.7.1.17.gbin

Deprecation of DES Privacy Protocol

For the SNMP security encryption, 128-bit AES encryption is the default privacy password option. Starting with Cisco UCS Manager Release 4.2. DES functionality will be completely deprecated. While still configurable, use of DES will result in the fault message: `ERROR: AES is not enabled`. As DES is a weak encryption algorithm, Cisco strongly recommends using the AES encryption default for security purposes.

Revision History

Release	Date	Description
4.1(3m)	November 27, 2023	Created release notes for Cisco UCS Manager Release 4.1(3m).
4.1(3l)	August 03, 2023	Created release notes for Cisco UCS Manager Release 4.1(3l).
4.1(3j)	May 24, 2023	Added Security Fixes for release 4.1(3j).
4.1(3k)	January 17, 2023	Created release notes for Cisco UCS Manager Release 4.1(3k).
4.1(3j)	August 16, 2022	Created release notes for Cisco UCS Manager Release 4.1(3j).
4.1(3i)	June 27, 2022	Created release notes for Cisco UCS Manager Release 4.1(3i).
4.1(3h)	January 31, 2022	Created release notes for Cisco UCS Manager Release 4.1(3h).
4.1(3f)	August 31, 2021	Created release notes for Cisco UCS Manager Release 4.1(3f).
4.1(3e)	July 29, 2021	Created release notes for Cisco UCS Manager Release 4.1(3e).
4.1(3d)	May 31, 2021	Created release notes for Cisco UCS Manager Release 4.1(3d).
4.1(3c)	April 05, 2021	Created release notes for Cisco UCS Manager Release 4.1(3c).

Release	Date	Description
4.1(3b)	January 26, 2021	Created release notes for Cisco UCS Manager Release 4.1(3b).
	March 31, 2021	Added CSCvw49192 to the list of Resolved Caveats.
4.1(3a)	January 13, 2021	Created release notes for Cisco UCS Manager Release 4.1(3a).
	January 25, 2021	Added CSCvx11527 to the list of Open Caveats.
	February 10, 2021	Added CSCvw47746 to the list of Resolved Caveats.
	April 07, 2021	Added CSCvw45654, CSCvw38983, CSCvv96107, and CSCvw38995 to the list of Security Fixes.
	June 1, 2021	Added CSCvy46626 to the liest of Open Caveats.
4.1(2c)	February 17, 2021	Created release notes for Cisco UCS Manager Release 4.1(2c).
	March 31, 2021	Added CSCvw49192 to the list of Resolved Caveats.
4.1(2b)	October 20, 2020	Created release notes for Cisco UCS Manager Release 4.1(2b).
	December 9, 2020	Added CSCvw49192 to the list of Open Caveats.
4.1(2a)	July 30, 2020	Created release notes for Cisco UCS Manager Release 4.1(2a).
	August 10, 2020	Added CSCvt35661 to the list of Resolved Caveats.
	December 22, 2020	Added CSCvq17291 to the list of Resolved Caveats.
4.1(1e)	September 02, 2020	Created release notes for Cisco UCS Manager Release 4.1(1e).
4.1(1d)	July 10, 2020	Created release notes for Cisco UCS Manager Release 4.1(1d).
	July 23, 2020	Added CSCvu11155 to the list of Resolved Caveats.

Release	Date	Description
4.1(1c)	April 20, 2020	Created release notes for Cisco UCS Manager Release 4.1(1c).
	May 27, 2020	Added CSCvu14656 to the list of Open Caveats.
	June 12, 2020	Added CSCvu11155 to the list of Open Caveats.
4.1(1b)	March 12, 2020	Created release notes for Cisco UCS Manager Release 4.1(1b).
4.1(1a)	February 20, 2020	Created release notes for Cisco UCS Manager Release 4.1(1a).
	March 04, 2020	Added CSCvt23481 to the list of Open Caveats.
	July 07, 2020	Added CSCvs73313 to the list of Resolved Caveats.

Top Reasons to Move to Cisco UCS Manager Release 4.1

Here are the top reasons to move to Cisco UCS Manager Release 4.1:

- Support for UCS 64108 Fabric Interconnects.
- Improved memory RAS features on M5 servers.
- RDMA Over Converged Ethernet (RoCE) Version 2 Support for UCS VIC 1400 Series Adapters.

Note In Cisco UCS Manager Release 4.1(1a), Windows RDMA support is being enabled as a Tech Preview feature and is disabled by default.

From Cisco UCS Manager Release 4.1(2a), RoCEv2 protocol for Windows 2019 NDKPI mode 1 and mode 2, is supported with both IPV4 and IPV6.

- Support for NVMe over Fabrics (NVMeoF) using RDMA for Converged Ethernet version 2 (RoCEv2) on Redhat Enterprise Linux 7.6 and 7.7 with Linux Z-Kernel 3.10.0-957.27.2, for Cisco UCS 14xx Series adapters.
- Support for NVMe over Fibre Channel (FC-NVMe) on SLES 12 SP4, SLES 12 SP5, SLES 15, SLES 15 SP1 and RHEL 7.6.
- Support for Intel® Virtual RAID on CPU (VRoC), which allows you to create and manage RAID volumes within the BIOS of VMD-enabled NVMe SSD drives.
- Support for new peripherals and optics.

New Features in Release 4.1

Cisco UCS Manager, Release 4.1 is a unified software release for all supported UCS hardware platforms.

New Hardware Features

- New Hardware in Release 4.1(3m) — None
- New Hardware in Release 4.1(3l) — None
- New Hardware in Release 4.1(3k) — None
- New Hardware in Release 4.1(3j) — None
- New Hardware in Release 4.1(3i) — None
- New Hardware in Release 4.1(3h) — None
- New Hardware in Release 4.1(3f) — None
- New Hardware in Release 4.1(3e), on page 6
- New Hardware in Release 4.1(3d) — None
- New Hardware in Release 4.1(3c) — None
- New Hardware in Release 4.1(3b) — None
- New Hardware in Release 4.1(3a), on page 6
- New Hardware in Release 4.1(2b), on page 7
- New Hardware in Release 4.1(2a), on page 7
- New Hardware in Release 4.1(1e) — None
- New Hardware in Release 4.1(1d) — None
- New Hardware in Release 4.1(1c) — None
- New Hardware in Release 4.1(1b) — None
- New Hardware in Release 4.1(1a), on page 8

New Software Features

- New Software in Release 4.1(3m) — None
- New Software in Release 4.1(3l) — None
- New Software in Release 4.1(3k) — None
- New Software in Release 4.1(3j) — None
- New Software in Release 4.1(3i) — None
- New Software Features in Release 4.1(3h), on page 9
- New Software in Release 4.1(3f) — None
- New Software Features in Release 4.1(3e), on page 9

- New Software in Release 4.1(3d) — None
- New Software in Release 4.1(3c) — None
- New Software in Release 4.1(3b) — None
- New Software Features in Release 4.1(3a), on page 9
- New Software Features in Release 4.1(2b), on page 11
- New Software Features in Release 4.1(2a), on page 11
- New Software in Release 4.1(1e) — None
- New Software in Release 4.1(1d) — None
- New Software in Release 4.1(1c) — None
- New Software in Release 4.1(1b) — None
- New Software Features in Release 4.1(1a), on page 12

New Hardware in Release 4.1(3e)

Peripherals

- Support for NVIDIA A40 GPU in Cisco UCS C480 M5 rack servers.

New Hardware in Release 4.1(3a)

Peripherals

- Support for NVIDIA A-100 GPU cards (UCSC-GPU-A100) on UCS C240 M5 servers and UCS C480 M5 servers.
- Support for NVIDIA GPU Cloud (NGC) on NVIDIA v100 on Cisco UCS C240 M5 servers and HyperFlex HX240C M5 servers.
- Support for AMD platform secure boot is enabled in Cisco UCS C125 M5 server.
- Support for FPGA upgrade in Cisco UCS 6454 Fabric Interconnect and Cisco UCS 64108 Fabric Interconnect:
  - On upgrading Infrastructure to Cisco UCS Manager release 4.1(3a) or later releases, the version of IOFPGA gets upgraded to v22 on Cisco UCS 6454 Fabric Interconnect.
  - Starting with Cisco UCS Manager release 4.1(3a), the secure FPGA upgrade feature is enabled for Cisco UCS 64108 Fabric Interconnect, by default. The FPGA will get upgraded when Infrastructure is upgraded from 4.1(3) to later releases.

  Post the IOFPGA version upgrade, upgrade golden regions of FPGA on Fabric Interconnect to address Secure Boot vulnerability. To upgrade golden regions of FPGA, install secure FPGA in fabric interconnect. For more information on secure FPGA installation procedure, see Cisco UCS Manager Network Management Guide and Cisco UCS Manager Network Management Guide using the CLI.
- Support for QSFP-40/100-SRBD at 40G with Cisco UCS 6300 and 6400 Series Fabric Interconnects on uplink port connection, and Cisco UCS-IOM-2304 and Cisco UCS-IOM-2304V2 I/O modules.

- Support for SFP-25G-AOC4M 4 meter AOC cable connection from VIC 1455/57 adapters at 25G to 6454/64108 Fabric Interconnects with Nexus N9K-C93240YC-FX2 switch in Standalone mode.
- Support for UCS-S3260-NVMW19T 1.9TB 2.5in U.2 WD SN640 NVMe Medium Performance Value Endurance drive and UCS-S3260-NVMW64T 6.4TB 2.5in U.2 WD SN640 NVMe Medium Performance High Endurance drive on Cisco UCS S3260 servers.

New Hardware in Release 4.1(2b)

Peripherals

- Support for RAID controller on Cisco UCS C240 SD M5 Server.

New Hardware in Release 4.1(2a)

Server

- Support for Cisco UCS C240 SD M5 Server.
- Support for Cisco UCS C125 M5 Rack Server Node based on AMD EPYC 2 7002 (ROME) Processors.

Peripherals

- Support for Broadcom HBA 9400-8I HBA Storage Adapter (UCSC-SAS9400-8i) on C125 M5 servers.
- Support for PCI Express passthrough with ESX 6.5 on LSI 9400-8i storage controller.
- Support for Broadcom HBA 9400-8I Tri-Mode Storage Adapter to enable design flexibility to operate NVMe, SAS, or SATA storage devices in a single drive bay.
- Support for usNIC on UCS C125 M5 servers.
- Support for IOM 2408 with VIC 1440 adapters with PE with 25G and 40G Ethernet connections.
- Support for Mellanox ConnectX-5 MCX516A-CDAT dual port 100GbE QSFP28 NIC (UCSC-P-M5D100GF) on Cisco UCS C220 M5, C240 M5 and S3260 Storage servers.
- Support for UCSC-GPU-RTX6000 and UCSC-GPU-RTX8000 on Cisco UCS C240 M5 servers.
- Support for the following NVMe drives on Cisco UCS S3260 Storage servers:

NVMe Drive	PID for UCS S3260	Product Description
SN640 1.9TB	UCS-S3260-NVMW19T	1.9TB 2.5 in U.2 WD SN640 NVMe Med. Perf. Value Endurance
SN640 6.4TB	UCS-S3260-NVMW64T	6.4TB 2.5 in U.2 WD SN640 NVMe Med. Perf. ValueEndurance

New Hardware in Release 4.1(1a)

High-Density Fourth Generation Fabric Interconnect

The Cisco UCS 64108 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 64108 offers line-rate, low-latency, lossless 10/25/40/100 Gigabit Ethernet, Fibre Channel over Ethernet (FCoE), and Fibre Channel functions.

The high-density Cisco UCS 64108 108-Port Fabric Interconnect is a two-rack-unit (2RU) 10/25/40/100 Gigabit Ethernet, FCoE and Fibre Channel switch. The switch has 96 10/25-Gbps fixed Ethernet (16 unified ports) and 12 40/100-Gbps Ethernet uplink ports. The 16 unified ports can support 10/25-Gbps Ethernet or 8/16/32G Fibre Channel ports. All Ethernet ports are capable of supporting FCoE.

Fabric Interconnect Migration

You can migrate from a UCS 6200 Series Fabric Interconnect to the following UCS 6400 Series Fabric Interconnects:

- UCS 64108 Fabric Interconnect
- UCS 6454 Fabric Interconnect

However, you cannot migrate back to a UCS 6200 Series Fabric Interconnect after you have migrated to a UCS 6400 Series Fabric Interconnect.

You can migrate from a UCS 6454 Fabric Interconnect to a UCS 64108 Fabric Interconnect. However, you cannot migrate back to a UCS 6454 Fabric Interconnect after you have migrated to a UCS 64108 Fabric Interconnect.

Peripherals

- Support for the UCSC-PCIE-IQ10GF 4 Port 10Gb Network Interface Card on UCS C125 M5 servers
- Support for the Intel XXV710-DA2OCP1 2 Port x 10/25Gb OCP 2.0 Network Interface Card on UCS C125 M5 servers
- Support for the Intel X710-DA2 2 x 10GbE SFP+ PCIe Network Interface Card on UCS C125 M5 servers
- Support for the Mellanox ConnectX-5 MCXM516A-CDAT 2 x 100GbE QSFP PCI Network Interface Card on C220 M5, C240 M5, C480 M5, C480 M5 ML servers
- Support for the Mellanox ConnectX-5 MCX515A-CCAT 1 x 100GbE QSFP PCI Network Interface Card on C220 M5, C240 M5, C480 M5 servers
- Support for the Mellanox ConnectX-5 MCX512A-ACAT 2 x 25Gb/10GbE SFP PCI Network Interface Card on C220 M5, C240 M5, C480 M5 servers
- Support for the following NVME drives on UCS C125 M5 servers:

NVMe Drive	PID for UCS C125 M5
Intel P4510 1TB (SSDPE2KX010T8K)	UCSC-NVME2H-I1000
Intel P4510 4TB (SSDPE2KX040T8K)	UCSC-NVME2H-I4000
Intel P4610 1.6TB (SSDPE2KE016T8K)	UCSC-NVME2H-I1600

NVMe Drive	PID for UCS C125 M5
Intel P4610 3.2TB (SSDPE2KE032T8K)	UCSC-NVME2H-I3200

- Support for NVIDIA T4 16GB GPU cards (UCSC-GPU-T4-16) on UCS C125 M5 servers and in the IO Expander on UCS S3260 M5 servers
- Support for QLogic QLE 2692 - 2 x 16Gb Gen 6 Fibre Channel HBA on UCS C125 M5 servers

New Software Features in Release 4.1(3h)

Feature Enhancements

- M5 Server BIOS updates for Windows 2022.
- Update for Intel IPU 2021.2 for Xeon® Scalable Processors (Cascade Lake).
- New BIOS settings to allow enabling and disabling of Trusted Platform Module security.

New Software Features in Release 4.1(3e)

Feature Enhancements

- New property added to create and modify the Internet Group Management Protocol (IGMP) Source IP Proxy State in Multicast Policy.
- Added an option to disable the Lewisburg SATA AHCI controller on Cisco UCS M5 servers.
- Support to display the DIMM manufacturing date/country information in dmidecode's (SMBIOS) Asset Tag field.
- Support mechanism for 6400 series Fabric Interconnets to send the Registered State Change Notification (RSCN) when the Cisco UCS IOM port-channel membership changes.

Note ESX NFNIC driver version 5.0.0.37 and later or 4.0.0.87 and later process this RSCN.

Linux FNIC driver version 2.0.0.85 and later process this RSCN.

New Software Features in Release 4.1(3a)

Feature Enhancements

- Support for Enhanced Data Path (ENS) with Geneve Offload on Cisco UCS VIC 1400 Series adapters.

  N-VDS contains two network stacks: standard stack and ENS stack. NSX-T manager selects the stack based on the user setting. By default, N-VDS runs in the standard mode. It uses the standard stack and utilizes the standard network driver for its uplink ports. For the VIC adapter, the standard driver is neNIC driver. The ENS driver is supported on on ESX 6.7U3, ESX 7.0, and ESX 7.0U1.

- Self-Monitoring, Analysis and Reporting Technology (SMART) attributes for Power-On Hours are now available for SAS SSDs, and are populated in the same manner as SATA drives.
- A new adapter policy, Power Save Mode, allows global management of the chassis toward maximizing energy efficiency or availability. The policy is global and is inherited by all chassis managed by Cisco UCS Manager. It is disabled by default.
- Cisco UCS Manager Release 4.1(3a) introduces the following BIOS tokens to improve RAS memory setting for UCS M5 servers:
  - Memory Thermal Throttling Mode
  - Advanced Memory Test
  - Transparent Secure Memory Encryption (TSME)
  - Auto Secure Encrypted Virtualization (SEV)
  - DRAM SW Thermal Throttling

  For more information on memory BIOS tokens, see the RAS Memory BIOS Settings section in Cisco UCS Manager Server Management Guide.
- Ability to install secure FPGA in fabric interconnect. For more information, see Cisco UCS Manager Network Management Guide and Cisco UCS Manager Network Management Guide using the CLI.
- Introduced the `Create oui [oui-id]` command to manually add OUIs into the databases which is necessary to establish FC port-channels with new Cisco FC devices or devices with newly assigned OUI ranges.

  For more information, see Cisco UCS Manager Storage Management Guide using the CLI.
- Provision to configure Priority Flow Control (PFC) watchdog interval to detect whether packets in a no-drop queue are being drained within a specified time period.

  For more information, see Cisco UCS Manager Network Management Guide using the CLI.
- Starting with Cisco UCS Manager Release 4.1(3a), you can connect Cisco UCS Rack servers with VIC 1455 and 1457 adapters, to the uplink ports 49-54 on Cisco UCS 6454 Fabric Interconnects and 97 to 108 in Cisco UCS 64108 Fabric Interconnects.
- Generic Network Virtualization Encapsulation (GENEVE Offload) is now supported on ESX 7.0U1 Operating system.
- Support for NVMe over Fibre Channel (FC-NVMe) on UCS 6300 series Fabric Interconnects, UCS 6454, and UCS 64108 Fabric Interconnects with Cisco UCS VIC 13xx series adapters on RHEL 7.8, RHEL 7.9, and RHEL 8.2. This support is also available on Cisco C220 and C240 M5 Standalone rack servers with Cisco UCS 13xx series adapters.
- Support for NVMe over Fibre Channel (FC-NVMe) on UCS 6300 series Fabric Interconnects, UCS 6454, and UCS 64108 Fabric Interconnects with Cisco UCS VIC 14xx series adapters on ESX 7.0, ESX 7.0 U1 and ESX 7.0u2.

  This support is also available on Cisco Standalone rack servers with Cisco UCS 14xx series adapters.
- Support for NVMe over Fibre Channel with Cisco UCS 1400 series adapters on RHEL 7.8, RHEL 7.9, RHEL 8.2.

- Support for NVMe over Fabrics (NVMeoF) using IPv4 or IPv6 RDMA over Converged Ethernet version 2 (RoCEv2) on Red Hat Enterprise Linux 7.8 and 8.2.
- Support for fNIC Multi-Queue on RHEL 7.6, RHEL 7.7, RHEL 7.9, RHEL 8.0, RHEL 8.1, RHEL 8.2, RHEL 8.3, SLES 12 SP5, and SLES15 SP2.
- FDMI support on Red Hat Enterprise Linux 7.9/8.2 and SLES 15 SP 2.
- 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 4.1(2b)

Feature Enhancements

- Cisco UCS Manager Release 4.1(2b) introduces the following BIOS tokens to improve RAS memory setting for UCS M5 servers:
  - Memory Refresh Rate
  - Panic and High Watermark

  For more information on memory BIOS tokens, see the RAS Memory BIOS Settings section in Cisco UCS Manager Server Management Guide.

New Software Features in Release 4.1(2a)

Feature Enhancements

- Support for Redfish on all Cisco UCS C-series and Cisco UCS B-series servers to enable Intersight with feature coverage of all endpoints.
- Support for NVMe over Fabrics (NVMeoF) using IPv4 or IPv6 RDMA over Converged Ethernet version 2 (RoCEv2) is supported on Red Hat Enterprise Linux 7.7 with Linux Z-Kernel-3.10.0-1062.9.1.el7.x86_64.
- Support for RoCEv2 protocol for Windows 2019 NDKPI mode 1 and mode 2, with both IPV4 and IPV6.
- A new fan policy option, Acoustic Mode, for reducing noise levels in acoustic-sensitive environments, is now available on Cisco UCS C220 M5, C240 M5, and C240 SD M5 Rack Servers.
- Support for Generic Network Virtualization Encapsulation (GENEVE) Offload on ESX 6.7U3 and ESX 7.0. GENEVE offload is present in all Ethernet adapter policies and is disabled by default.
- Support for NVMe over Fibre Channel on Red Hat Enterprise Linux 7.7, 8.0 and 8.1.
- Support for Red Hat Enterprise Linux 8.2 multi-queue on Unified fNIC drivers.
- Support for VIC adapters on Redhat Enterprise Linux 7.8 and 8.2 and ESX 7.0.

Intersight Management Mode

Intersight Managed Mode (IMM) is a new set of features introduced in Cisco Intersight to configure, deploy, and manage a Server Profile for B-Series, FI-managed C-Series servers. IMM introduces a new implementation

of concepts first introduced with Cisco UCS Manager and moves ownership of the policy model into Cisco Intersight. Hence, policies, VLANs, and VSANs are created in advance and built into a Server Profile. Then, the Server Profile is assigned and deployed to a Cisco Intersight discovered B-Series or managed C-Series servers.

Note Cisco UCS Infrastructure and Server FW version 4.1(2) enables an opt-in for IMM; a policy driven configuration platform for FIs and attached servers. When IMM is enabled, the entire UCS domain is reset to factory defaults and this will cause a disruption for workloads running on servers in the domain.

For more information, see https://intersight.com/help/resources#intersight_managed_mode.

New Software Features in Release 4.1(1a)

Cisco UCS 64108 Fabric Interconnect

This release introduces Cisco UCS 64108 Fabric Interconnects that support 96 10/25-Gbps ports (16 unified ports) and 12 40/100-Gbps uplink ports. The 16 unified ports can support 10/25-Gbps Ethernet or 8/16/32G Fibre Channel ports. The *Cisco UCS Manager Getting Started Guide, Release 4.1* provides details about the specific ports.

Cisco UCS Manager Release 4.0(1) and 4.0(2) introduced support for various software features on Cisco UCS 6454 Fabric Interconnects. Cisco UCS Manager Release 4.1 extends support for these features on Cisco UCS 64108 Fabric Interconnects. These software features are:

- 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

Legacy Features Not Supported

The following features are not supported on Cisco UCS 64108 Fabric Interconnects:

- Chassis Discovery Policy in Non-Port Channel Mode
- Chassis Connectivity Policy in Non-Port Channel Mode
- Service profiles with dynamic vNICs
- Multicast Optimize for QoS
- Netflow
- Port profiles and distributed virtual switches

RDMA Over Converged Ethernet Version 2 Support for UCS VIC Adapters

RDMA over Converged Ethernet (RoCE) v2 for Microsoft SMB Direct

RDMA over Converged Ethernet version 2 (RoCEv2) is an *internet layer* protocol, which means that RoCEv2 packets can be routed. RoCEv2 allows direct memory access over the network by encapsulating an Infiniband (IB) transport packet over Ethernet.

This release introduces support for RoCEv2 with Cisco UCS VIC 1400 Series adapters. It also adds support for Microsoft SMB Direct with RoCEv2 on Microsoft Windows 2019. Refer UCS Hardware and Software Compatibility for more details about support of Microsoft SMB Direct with RoCEv2 on Microsoft Windows 2019. RoCEv2 support is being enabled as a **Tech Preview** feature. Refer Cisco UCS Manager Configuration Guide for RDMA over Converged Ethernet (RoCE) v2 for more details on RoCEv2.

Note RoCEv1 is not supported on Cisco UCS VIC 1400 Series adapters. RoCEv2 is not supported on UCS VIC 12xx Series and 13xx Series adapters.

NVMe over Fabric via Ethernet (NVMeoF) with Support for RDMA

NVMe over Fabric via Ethernet (NVMeoF) support on Redhat Enterprise Linux 7.6 z-kernels with version 3.10.0-957.27.2.el7 or later is added for Cisco UCS 14xx Series adapters. RDMA also supports NVMeoF.

Support for Fibre Channel and NVMe over Fibre Channel (FC-NVME)

Support for NVMe over Fibre Channel (FC-NVMe) on SLES 12 SP4, SLES 12 SP5, SLES 15, SLES 15 SP1 and RHEL 7.6. Unified driver support for Fibre Channel and NVMe over Fibre Channel (FC-NVME) on SLES 12 SP4, SLES 15, and RHEL 7.6. This support is available on UCS 6300 Series Fabric Interconnects and UCS 6454 Fabric Interconnects with Cisco UCS 14xx Series adapters. NVMe over Fibre Channel now supports up to 16 interfaces.

Memory RAS Enhancements

This release introduces the following Memory RAS enhancements:

Intel Post Package Repair (PPR) uses additional spare capacity within the DDR4 DRAM to remap and replace faulty cell areas detected during system boot time. Remapping is permanent and persists through power-down and reboot.

Partial DIMM Mirroring enables better Virtualization Host Resiliance by creating a mirror copy of specific regions of memory cells, instead of keeping the complete half of the mirror copy. Memory mirrors, using up to 50% of capacity, can be specified in gigabytes or percentage of total capacity, across up to 4 mirrors, and can be configured across multiple IMCs or sockets. Partial mirroring cannot be used in connection with standard mirroring or ADDDC sparing.

Address Range allows the memory presented to the user to be limited to a specified subset of actual memory.

Intel® VMD and Intel® Virtual RAID on CPU (VRoC)

Intel® Volume Management Device (VMD) provides storage management options for NVMe drives, including surprise hot-plug and LED status management. Virtual RAID on CPU (VRoC) enables creating and managing RAID volumes within the BIOS of VMD-enabled NVMe SSD drives by using hardware logic inside the Intel Xeon processor. The Cisco implementation of VRoC, supported only on Intel NVMe drives, supports RAID 0 (striping), RAID 1 (mirroring), RAID 5 (striping with parity) and RAID 10 (combined mirroring and striping).

Feature Enhancements

- A per-chassis fan control policy for B-Series servers allows a single policy to control the speed of all server fans in an enclosure.
- Support for configuring vMedia mount as writable when both the following conditions are met:

- Device Type is HDD
- Protocol is NFS or CIFS

- Intel® Optane™ Data Center persistent memory module support is extended to C480 M5ML servers.

Deprecated Hardware and Software in Cisco UCS Manager Release 4.1

Beginning with Cisco UCS Manager Release 4.1(1), the KVM Console GUI is available only as an HTML5-based application. It is no longer available as a Java-based application.

Beginning with Cisco UCS Manager Release 4.1(1), VM-FEX is only supported with Red Hat Enterprise Linux (RHEL) on KVM.VMware VM-FEX on ESX, Windows VM-FEX, and Hyper-V VM-FEX are no longer supported.

Beginning with Cisco UCS Manager Release 4.1(1), FDMI on Unified Linux fNIC drivers is no longer supported.

Beginning with Cisco UCS Manager Release 4.1(3d), the following drives are no longer supported:

UCSC-F-FIO-1205M	Cisco UCS 1.2TB MLC Fusion ioDrive2
UCSC-F-FIO-3000M	Cisco UCS 3TB MLC Fusion ioDrive2
UCSC-F-FIO-365M	Cisco UCS 365GB MLC Fusion-io ioDrive2
UCSC-F-FIO-785M	Cisco UCS 785GB MLC Fusion-io ioDrive2
UCSB-F-FIO-785M	Cisco UCS 785GB MLC Fusion-io ioDrive2
UCSB-F-FIO-365M	Cisco UCS 365GB MLC Fusion-io ioDrive2

Deprecation in Future Releases

The following adapters are approaching end-of-life (EOL) and will not be supported in future releases of Cisco UCS Manager:

- Emulex LPe12002 8G FC adapter (N2XX-AEPCI05)
- Emulex LPe16002-M6 16G FC rack HBA (UCSC-PCIE-E16002)
- AMD Firepro 7150 x2 PCIe x16 Graphics Card (UCSC-GPU-7150X2)
- Cisco UCS Fusion ioDrive2 Adapter

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 4.1(1) is integrated with C-Series Standalone Release 4.1(1) for the M5 servers, Release 4.0(2) for all the M4 servers, and Release

3.0(4) for all M3 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 1: 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
4.1(3)	4.1(3)	S3260 M4, All M5
	4.1(2)	C220 M4, C240 M4, C460 M4
	3.0(4)	All M3
4.1(2)	4.1(2)	C220 M5, C240 M5, C240 SD M5, C480 M5, S3260 M5, C480 M5 ML, C125 M5, C220 M4, C240 M4, C460 M4, S3260 M4
	3.0(4)	All M3
4.1(1)	4.1(1)	C220 M5, C240 M5, C480 M5, S3260 M5, C125 M5, C480 M5 ML only
	4.0(2)	C220 M4, C240 M4, C460 M4, S3260 M4, C125 M5 only
	3.0(4)	All M3
4.0(4)	4.0(4)	C220 M5, C240 M5, C480 M5, S3260 M5, C480 M5 ML only
	4.0(2)	C220 M4, C240 M4, C460 M4, S3260 M4, C125 M5 only
	3.0(4)	All M3
4.0(2)	4.0(2)	C220 M4, C240 M4, C460 M4, C220 M5, C240 M5, C480 M5, S3260 M4, S3260 M5, C125 M5, C480 M5 ML only
	3.0(4)	All M3
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

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

System Requirements

Cisco UCS Central Integration

The following table provides the release version with which Cisco UCS Manager can be registered with Cisco UCS Central.

Cisco UCS Manager	Cisco UCS Central
4.1(3)	2.0(1m) or later releases
4.1(2)	2.0(1l) or later releases
4.1(1)	2.0(1k) or later releases

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

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 Mozilla Firefox 45 or higher Google Chrome 45 or higher Apple Safari version 9 or higher 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 4.1* 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 6400 Series Fabric Interconnects:

Table 2: Mixed Cisco UCS Releases Supported on Cisco UCS 6200, 6300, 6400 Series Fabric Interconnects

	Infrastructure Versions (A Bundles)								
Host FW Versions (B or C Bundles)	2.2(8)	3.1(3)	3.2(3)	4.0(1)	4.0(2)	4.0(4)	4.1(1)	4.1(2)	4.1(3)
2.2(8)	6200	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	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	6200,6332, 6332-16UP
4.0(1)	—	—	—	6200,6332, 6332-16UP, 6454	6200,6332, 6332-16UP, 6454	6200,6332, 6332-16UP, 6454	6200,6332, 6332-16UP, 6454	6200,6332, 6332-16UP, 6454	6200,6332, 6332-16UP, 6454

	Infrastructure Versions (A Bundles)								
4.0(2)	—	—	—	6200,6332, 6332-16UP, 6454	6200,6332, 6332-16UP, 6454	6200,6332, 6332-16UP, 6454	6200,6332, 6332-16UP, 6454	6200,6332, 6332-16UP, 6454	6200,6332, 6332-16UP, 6454
4.0(4)	—	—	—	6200,6332, 6332-16UP, 6454	6200,6332, 6332-16UP, 6454	6200,6332, 6332-16UP, 6454	6200,6332, 6332-16UP, 6454	6200,6332, 6332-16UP, 6454	6200,6332, 6332-16UP, 6454
4.1(1)	—	—	—	—	—	—	6200,6332, 6332-16UP, 6454, 64108	6200,6332, 6332-16UP, 6454, 64108	6200,6332, 6332-16UP, 6454, 64108
4.1(2)	—	—	—	—	—	—	6200,6332, 6332-16UP, 6454, 64108	6200,6332, 6332-16UP, 6454, 64108	6200,6332, 6332-16UP, 6454, 64108
4.1(3)	—	—	—	—	—	—	6200,6332, 6332-16UP, 6454, 64108	6200,6332, 6332-16UP, 6454, 64108	6200,6332, 6332-16UP, 6454, 64108

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

Table 3: 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(3)	4.0(1)	4.0(2)	4.0(4)	4.1(1)	4.1(2)	4.1(3)
3.1(3)	6324	6324	6324	6324	6324	6324	6324	6324
3.2(3)	—	6324	6324	6324	6324	6324	6324	6324
4.0(1)	—	—	6324	6324	6324	6324	6324	6324
4.0(2)	—	—	6324	6324	6324	6324	6324	6324
4.0(4)	—	—	6324	6324	6324	6324	6324	6324
4.1(1)	—	—	—	—	—	6324	6324	6324
4.1(2)	—	—	—	—	—	6324	6324	6324
4.1(3)	—	—	—	—	—	6324	6324	6324

The following table lists the mixed B, C bundles that are supported on all platforms with the 4.1(x)A bundle:

Table 4: Mixed B, C Bundles Supported on All Platforms with the 4.1(x)A Bundle

	Infrastructure Versions (A Bundles)			
Host FW Versions (B, C Bundles)	4.1(x)			
	6200	6300	6324	6400
	ucs-k9-bundle-infra.4.1.x.xxx.A.bin	ucs-6300-k9-bundle-infra.4.1.x.xxx.A.bin	ucs-mini-k9-bundle-infra.4.1.x.xxx.A.bin	ucs-6400-k9-bundle-infra.4.1.x.xxx.A.bin
2.2(8) (B, C Bundles)	Yes	—	—	—
3.1(3) (B, C Bundles)	Yes	Yes	Yes	—
3.2(3) (B, C Bundles)	Yes	Yes	Yes	—
4.0(1), 4.0(2), 4.0(4) (B, C Bundles)	Yes	Yes	Yes	Yes
4.1(1)	Yes	Yes	Yes	Yes
4.1(2)	Yes	Yes	Yes	Yes
4.1(3)	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 6400 Series Fabric Interconnects and Components

Blade Servers

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

Table 5: Minimum Host Firmware Versions for Blade Servers

Servers	Minimum Software Version UCS 6200 Series FI	Minimum Software Version UCS 6332, 6332-16UP FI	Minimum Software Version UCS 6332, 6332-16UP FI		Minimum Software Version UCS 6454 FI	Minimum Software Version UCS 64108 FI	Suggested Software Version UCS 6200 Series FI UCS 6332, 6332-16UP FI UCS 6400 Series FI
	UCS-IOM- 2204 UCS-IOM- 2208	UCS-IOM- 2204 UCS-IOM- 2208	UCS-IOM- 2304	UCS-IOM- 2304V2	UCS-IOM- 2204 UCS-IOM- 2208 UCS-IOM- 2408*	UCS-IOM- 2204 UCS-IOM- 2208 UCS-IOM- 2408*	UCS-IOM-2204 UCS-IOM-2208 UCS-IOM-2408*
					* UCS-IOM-2408 supported on M4 and M5 only with UCS 6400 Series FI & VIC 1300/1400		
B22 M3 E5-2400 B22 M3 E5-2400 v2 **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) 2.2(8a)	3.1(3a) 3.1(3a)	3.1(3a)	4.0(4o)	4.0(1a)	4.1(1a)	4.1(3m)
B200 M3 E5-2600 B200 M3 E5-2600 v2 **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) 2.2(8a)	3.1(3a) 3.1(3a)	3.1(3a)	4.0(4o)	4.0(1a)	4.1(1a)	4.1(3m)
B200 M4	2.2(8a)	3.1(3a)	3.1(3a)	4.0(4o)	4.0(1a)	4.1(1a)	4.1(3m)
B200 M5	3.2(1d)	3.2(1d)	3.2(1d)	4.0(4o)	4.0(1a)	4.1(1a)	4.1(3m)
B260 M4 E7-2800 v2 B260 M4 E7-4800 v2 B260 M4 E7-8800 v2 B260 M4 E7-4800 v3 B260 M4 E7-8800 v3	2.2(8a) 2.2(8a) 2.2(8a) 2.2(8a) 2.2(8a)	3.1(3a) 3.1(3a) 3.1(3a) 3.1(3a) 3.1(3a)	3.1(3a)	4.0(4o)	4.0(1a)	4.1(1a)	4.1(3m)
B260 M4 E7-4800 v4 B260 M4 E7-8800 v4	2.2(8b) 2.2(8b)	3.1(3a) 3.1(3a)	3.1(3a) 3.1(3a)	4.0(4o)	4.0(1a)	4.1(1a)	4.1(3m)

Servers	Minimum Software Version UCS 6200 Series FI	Minimum Software Version UCS 6332, 6332-16UP FI	Minimum Software Version UCS 6332, 6332-16UP FI		Minimum Software Version UCS 6454 FI	Minimum Software Version UCS 64108 FI	Suggested Software Version UCS 6200 Series FI UCS 6332, 6332-16UP FI UCS 6400 Series FI
	UCS-IOM- 2204 UCS-IOM- 2208	UCS-IOM- 2204 UCS-IOM- 2208	UCS-IOM- 2304	UCS-IOM- 2304V2	UCS-IOM- 2204 UCS-IOM- 2208 UCS-IOM- 2408*	UCS-IOM- 2204 UCS-IOM- 2208 UCS-IOM- 2408*	UCS-IOM-2204 UCS-IOM-2208 UCS-IOM-2408*
					* UCS-IOM-2408 supported on M4 and M5 only with UCS 6400 Series FI & VIC 1300/1400		
B420 M3 E5-4600 B420 M3 E5-4600 v2 **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) 2.2(8a)	3.1(3a) 3.1(3a)	3.1(3a)	4.0(4o)	4.0(1a)	4.1(1a)	4.1(3m)
B420 M4 E5-4600 v3 B420 M4 E5-4600 v4	2.2(8a) 2.2(8b)	3.1(3a) 3.1(3a)	3.1(3a) 3.1(3a)	4.0(4o)	4.0(1a)	4.1(1a)	4.1(3m)
B460 M4 E7-4800 v2 B460 M4 E7-8800 v2 B460 M4 E7-4800 v3 B460 M4 E7-8800 v3	2.2(8a) 2.2(8a) 2.2(8a) 2.2(8a)	3.1(3a) 3.1(3a) 3.1(3a) 3.1(3a)	3.1(3a)	4.0(4o)	4.0(1a)	4.1(1a)	4.1(3m)
B460 M4 E7-4800 v4 B460 M4 E7-8800 v4	2.2(8b) 2.2(8b)	3.1(3a) 3.1(3a)	3.1(3a)	4.0(4o)	4.0(1a)	4.1(1a)	4.1(3m)
B480 M5	3.2(2b)	3.2(2b)	3.2(2b)	4.0(4o)	4.0(1a)	4.1(1a)	4.1(3m)

Rack Servers

Table 6: Minimum Host Firmware Versions for Rack Servers

Servers	Minimum Software Version UCS 6200 Series FI	Minimum Software Version UCS 6332, 6332-16UP	Minimum Software Version UCS 6454	Minimum Software Version UCS 64108	Suggested Software Version UCS 6200 Series FI UCS 6332, 6332-16UP FI UCS 6400 Series FI
C22 M3 and M3L	2.2(8a)	3.1(3a)	4.0(1a)	4.1(1a)	4.1(3m)
C24 M3, M3L, and M3S2	2.2(8a)	3.1(3a)	4.0(1a)	4.1(1a)	4.1(3m)

Servers	Minimum Software Version UCS 6200 Series FI	Minimum Software Version UCS 6332, 6332-16UP	Minimum Software Version UCS 6454	Minimum Software Version UCS 64108	Suggested Software Version UCS 6200 Series FI UCS 6332, 6332-16UP FI UCS 6400 Series FI
C220 M3	2.2(8a)	3.1(3a)	4.0(1a)	4.1(1a)	4.1(3m)
C220 M4	2.2(8a)	3.1(3a)	4.0(1a)	4.1(1a)	4.1(3m)
C220 M5	3.2(1d)	3.2(1d)	4.0(1a)	4.1(1a)	4.1(3m)
C240 M3	2.2(8a)	3.1(3a)	4.0(1a)	4.1(1a)	4.1(3m)
C240 M4	2.2(8a)	3.1(3a)	4.0(1a)	4.1(1a)	4.1(3m)
C240 M5	3.2(1d)	3.2(1d)	4.0(1a)	4.1(1a)	4.1(3m)
C460 M4 E7-2800 v2 C460 M4 E7-4800 v2 C460 M4 E7-8800 v2 C460 M4 E7-4800 v3 C460 M4 E7-8800 v3	2.2(8a) 2.2(8a) 2.2(8a) 2.2(8a) 2.2(8a)	3.1(3a) 3.1(3a) 3.1(3a) 3.1(3a) 3.1(3a)	4.0(1a)	4.1(1a)	4.1(3m)
C460 M4 E7-8800 v4	2.2(8b)	3.1(3a)	4.0(1a)	4.1(1a)	4.1(3m)
C480 M5	3.2(2b)	3.2(2b)	4.0(1a)	4.1(1a)	4.1(3m)
S3260 M4	3.1(2b)	3.1(3a)	4.0(1a)	4.1(1a)	4.1(3m)
S3260 M5	3.2(3a)	3.2(3a)	4.0(1a)	4.1(1a)	4.1(3m)
C125 M5	NA	4.0(1a)	4.0(1a)	4.1(1a)	4.1(3m) (only on UCS 6332, UCS 6332-16UP FI, and UCS 6400 Series FI
C480 M5 ML	4.0(2a)	4.0(2a)	4.0(2a)	4.1(1a)	4.1(3m)

Adapters

Table 7: Minimum Software Versions for Adapters

Adapters	Minimum Software Version UCS 6200 Series FI	Minimum Software Version UCS 6332, 6332-16UP	Minimum Software Version UCS 6332, 6332-16UP	Minimum Software Version UCS 6454	Minimum Software Version UCS 64108	Suggested Software Version UCS 6200 Series FI UCS 6332, 6332-16UP FI UCS 6400 Series FI
	UCS-IOM-2204 UCS-IOM-2208	UCS-IOM-2204 UCS-IOM-2208	UCS-IOM-2304 UCS-IOM-2304V2	UCS-IOM-2204 UCS-IOM-2208 UCS-IOM-2408*	UCS-IOM-2204 UCS-IOM-2208 UCS-IOM-2408*	UCS-IOM-2204 UCS-IOM-2208 UCS-IOM-2408*
				* UCS-IOM-2408 supported on M4 and M5 only with UCS 6400 Series FI		
UCSC-P-M5S100GF (Mellanox ConnectX-5 MCX515A-CCAT 1 x 100GbE QSFP PCI NIC)	4.1(1a)	4.1(1a)	4.1(1a)	4.1(1a)	4.1(1a)	Mellanox ConnectX-5 MCX512A-ACAT 2 x 25Gb/10GbE SFP PCI
UCSC-P-M5D25GF (Mellanox ConnectX-5 MCX512A-ACAT 2 x 25Gb/10GbE SFP PCI)	4.1(1a)	4.1(1a)	4.1(1a)	4.1(1a)	4.1(1a)	Mellanox ConnectX-5 MCX512A-ACAT 2 x 25Gb/10GbE SFP PCI
UCSC-O- M5S100GF (Mellanox ConnectX-5 MCX545B-ECAN 1 x 100GbE QSFP PCI NIC)	4.1(1a)	4.1(1a)	4.1(1a)	4.1(1a)	4.1(1a)	Mellanox ConnectX-5 MCX545B-ECAN 1 x 100GbE QSFP PCI
UCSC-P -M4D25GF (Mellanox MCX4121A-ACAT Dual Port 10/25G SFP28 NIC)	4.0(4o)	4.0(4o)	4.0(4o)	4.0(4o)	4.1(1a)	4.1(3m)
UCSC-PCIE-QS100GF (QLogic QL45611HLCU 100GbE)	4.0(4o)	4.0(4o)	4.0(4o)	4.0(4o)	4.1(1a)	4.1(3m)
UCSC-PCIE-C100-04 (UCS VIC 1495)	NA	4.0(2a)	4.0(2a)	NA	4.1(1a)	4.1(3m)(only on UCS 6332, 6332-16UP FI)
UCSC-MLOM-C100-04 (UCS VIC 1497)	NA	4.0(2a)	4.0(2a)	NA	4.1(1a)	4.1(3m)(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)	4.1(1a)	4.1(3m)
UCSB-VIC-M84-4P (UCS VIC 1480)	4.0(1a)	4.0(1a)	4.0(1a)	4.0(1a)	4.1(1a)	4.1(3m)
UCSC-PCIE-C25Q-04 (UCS VIC 1455)	4.0(1a)	4.0(1a)	4.0(1a)	4.0(1a)	4.1(1a)	4.1(3m)
UCSC-MLOM-C25Q-04 (UCS VIC 1457)	4.0(1a)	4.0(1a)	4.0(1a)	4.0(1a)	4.1(1a)	4.1(3m)
UCSC-PCIE-BD16GF (Emulex LPe31002 Dual-Port 16G FC HBA)	3.2(3a)	3.2(3a)	3.2(3a)	4.0(1a)	4.1(1a)	4.1(3m)
UCSC-PCIE-ID40GF (Intel XL710 adapter)	3.2(3a)	3.2(3a)	3.2(3a)	4.0(1a)	4.1(1a)	4.1(3f)

Adapters	Minimum Software Version UCS 6200 Series FI	Minimum Software Version UCS 6332, 6332-16UP	Minimum Software Version UCS 6332, 6332-16UP	Minimum Software Version UCS 6454	Minimum Software Version UCS 64108	Suggested Software Version UCS 6200 Series FI UCS 6332, 6332-16UP FI UCS 6400 Series FI
	UCS-IOM-2204 UCS-IOM-2208	UCS-IOM-2204 UCS-IOM-2208	UCS-IOM-2304 UCS-IOM-2304V2	UCS-IOM-2204 UCS-IOM-2208 UCS-IOM-2408*	UCS-IOM-2204 UCS-IOM-2208 UCS-IOM-2408*	UCS-IOM-2204 UCS-IOM-2208 UCS-IOM-2408*
				* UCS-IOM-2408 supported on M4 and M5 only with UCS 6400 Series FI		
UCSC-PCIE-IQ10GF (Intel X710-DA4 adapter)	3.2(3a)	3.2(3a)	3.2(3a)	4.0(1a)	4.1(1a)	4.1(3f)
UCSC-PCIE-ID10GF (Intel X710-DA2 adapter)	3.2(3a)	3.2(3a)	3.2(3a)	4.0(1a)	4.1(1a)	4.1(3f)
UCSC-PCIE-ID25GF (Intel XXV710-DA2 Dual port 25 Gigabit Ethernet PCIe adapter)	3.2(3a)	3.2(3a)	3.2(3a)	4.0(1a)	4.1(1a)	4.1(3f)
UCSC-PCIE-ID10GC (Intel X550-T2 adapter)	3.2(3a)	3.2(3a)	3.2(3a)	4.0(1a)	4.1(1a)	4.1(3m)
N2XX-AIPCI01 (Intel X520 dual port adapter)	3.2(3a)	3.2(3a)	3.2(3a)	4.0(1a)	4.1(1a)	4.1(3m)
UCSC-PCIE-ID25GF (Intel X710 25Gb Dual-port BaseT)	3.2(3a)	3.2(3a)	3.2(3a)	4.0(1a)	4.1(1a)	4.1(3f)
UCSC-PCIE-QD40GF (QLogic QL45412H 40GbE)	3.2(2b)	3.2(2b)	3.2(2b)	4.0(1a)	4.1(1a)	4.1(3m)
UCSC-PCIE-IQ10GC (Intel X710-T4)	3.2(2b)	3.2(2b)	3.2(2b)	4.0(1a)	4.1(1a)	4.1(3f)
UCSC-PCIE-QD16GF (QLogic QLE2692-CSC)	3.2(1d)	3.2(1d)	3.2(1d)	4.0(1a)	4.1(1a)	4.1(3m)
UCSC-PCIE-C40Q-03 (UCS VIC 1385) UCSC-MLOM-C40Q-03 (UCS VIC 1387)	2.2(8a)	3.1(3a)	3.1(3a)	4.0(1a)	4.1(1a)	4.1(3m)
UCS-VIC-M82-8P (UCS VIC 1280) UCSB-MLOM-40G-01 (UCS VIC 1240) UCSB-MLOM-PT-01 (Cisco Port Expander Card)	2.2(8a)	3.1(3a)	3.1(3a)	4.0(1a)	4.1(1a)	4.1(3m)
UCSB-MLOM-40G-03 (UCS VIC 1340) UCSB-VIC-M83-8P (UCS VIC 1380) UCSC-MLOM-CSC-02 (UCS VIC 1227)	2.2(8a)	3.1(3a)	3.1(3a)	4.0(1a)	4.1(1a)	4.1(3m)
UCSC-PCIE-CSC-02 (UCS VIC 1225)	2.2(8a)	3.1(3a)	3.1(3a)	4.0(1a)	4.1(1a)	4.1(3m)

Adapters	Minimum Software Version UCS 6200 Series FI	Minimum Software Version UCS 6332, 6332-16UP	Minimum Software Version UCS 6332, 6332-16UP	Minimum Software Version UCS 6454	Minimum Software Version UCS 64108	Suggested Software Version UCS 6200 Series FI UCS 6332, 6332-16UP FI UCS 6400 Series FI
	UCS-IOM-2204 UCS-IOM-2208	UCS-IOM-2204 UCS-IOM-2208	UCS-IOM-2304 UCS-IOM-2304V2	UCS-IOM-2204 UCS-IOM-2208 UCS-IOM-2408*	UCS-IOM-2204 UCS-IOM-2208 UCS-IOM-2408*	UCS-IOM-2204 UCS-IOM-2208 UCS-IOM-2408*
				* UCS-IOM-2408 supported on M4 and M5 only with UCS 6400 Series FI		
UCSC-F-FIO-1000MP (Cisco UCS Fusion ioMemory – PX600, 1.0TB) UCSC-F-FIO-1300MP (Cisco UCS Fusion ioMemory – PX600, 1.3TB) UCSC-F-FIO-2600MP (Cisco UCS Fusion ioMemory – PX600, 2.6TB) UCSC-F-FIO-5200MP (Cisco UCS Fusion ioMemory – PX600, 5.2TB)	2.2(8a)	3.1(3a)	3.1(3a)	4.0(1a)	4.1(1a)	4.1(3m)
UCSB-FIO-1600MS (Cisco UCS Fusion ioMemory Mezzanine SX300, 1.6TB) UCSB-FIO-1300MS (Cisco UCS Fusion ioMemory Mezzanine PX600, 1.3TB)	2.2(8a)	3.1(3a)	3.1(3a)	4.0(1a)	4.1(1a)	4.1(3m)
UCSC-INVADER-3108 UCSC-NYTRO-200GB (Cisco Nytro MegaRAID 200GB Controller)	2.2(8a)	3.1(3a)	3.1(3a)	4.0(1a)	4.1(1a)	4.1(3m)

Adapters	Minimum Software Version UCS 6200 Series FI	Minimum Software Version UCS 6332, 6332-16UP	Minimum Software Version UCS 6332, 6332-16UP	Minimum Software Version UCS 6454	Minimum Software Version UCS 64108	Suggested Software Version UCS 6200 Series FI UCS 6332, 6332-16UP FI UCS 6400 Series FI
	UCS-IOM-2204 UCS-IOM-2208	UCS-IOM-2204 UCS-IOM-2208	UCS-IOM-2304 UCS-IOM-2304V2	UCS-IOM-2204 UCS-IOM-2208 UCS-IOM-2408*	UCS-IOM-2204 UCS-IOM-2208 UCS-IOM-2408*	UCS-IOM-2204 UCS-IOM-2208 UCS-IOM-2408*
				* UCS-IOM-2408 supported on M4 and M5 only with UCS 6400 Series FI		
UCSC-MLOM-C10T-02 (UCS VIC 1227T) UCSC-PCIE-C10T-02 (UCS VIC 1225T) UCSC-F-FIO-785M (Cisco UCS 785GB MLC Fusion ioDrive2 for C-Series Servers) UCSC-F-FIO-365M (Cisco UCS 365GB MLC Fusion ioDrive2 for C-Series Servers) UCSC-F-FIO-1205M (Cisco UCS 1205GB MLC Fusion ioDrive2 for C-Series Servers) UCSC-F-FIO-3000M (Cisco UCS 3.0TB MLC Fusion ioDrive2 for C-Series Servers) UCSC-F-FIO-1000PS (UCS 1000GB Fusion ioMemory3 PX Performance line for Rack M4) UCSC-F-FIO-1300PS (UCSC-F-FIO-1300PS) UCSC-F-FIO-2600PS (UCS 2600GB Fusion ioMemory3 PX Performance line for Rack M4) UCSC-F-FIO-5200PS (UCS 5200GB Fusion ioMemory3 PX Performance line for Rack M4) UCSC-F-FIO-6400SS (UCS 6400GB Fusion ioMemory3 SX Scale line for C-Series) UCSC-F-FIO-3200SS (UCS 3200GB Fusion ioMemory3SX Scale line for C-Series)	2.2(8a)	3.1(3a)	3.1(3a)	4.0(1a)	4.1(1a)	4.1(3m)
UCSC-PCIE-E14102B (Emulex OCe14102B-F)	2.2(8a)	3.1(3a)	3.1(3a)	4.0(1a)	4.1(1a)	4.1(3m)

Adapters	Minimum Software Version UCS 6200 Series FI	Minimum Software Version UCS 6332, 6332-16UP	Minimum Software Version UCS 6332, 6332-16UP	Minimum Software Version UCS 6454	Minimum Software Version UCS 64108	Suggested Software Version UCS 6200 Series FI UCS 6332, 6332-16UP FI UCS 6400 Series FI
	UCS-IOM-2204 UCS-IOM-2208	UCS-IOM-2204 UCS-IOM-2208	UCS-IOM-2304 UCS-IOM-2304V2	UCS-IOM-2204 UCS-IOM-2208 UCS-IOM-2408*	UCS-IOM-2204 UCS-IOM-2208 UCS-IOM-2408*	UCS-IOM-2204 UCS-IOM-2208 UCS-IOM-2408*
				* UCS-IOM-2408 supported on M4 and M5 only with UCS 6400 Series FI		
UCSC-PCIE-IQ10GF (Intel X710-DA4 adapter) UCSC-PCIE-ID10GF (Intel X710-DA2 adapter) UCSC-PCIE-ID40GF (Intel XL710 adapter)	—	—	3.1(3a)	4.0(1a)	4.1(1a)	4.1(3f)
UCSC-F-I80010 (Intel P3700 HHHL 800GB NVMe PCIe SSD) UCSC-F-I12003 (Intel P3600 HHHL 1200GB NVMe PCIe SSD) UCSC-F-I160010 (Intel P3700 HHHL 1600GB NVMe PCIe SSD) UCSC-F-I20003 (Intel P3600 HHHL 2000GB NVMe PCIe SSD) UCS-PCI25-40010 (Intel P3700 400GB NVMe PCIe SSD) UCS-PCI25-8003 (Intel P3600 800GB NVMe PCIe SSD) UCS-PCI25-80010 (Intel P3700 800GB NVMe PCIe SSD) UCS-PCI25-16003 (Intel P3600 1600GB NVMe PCIe SSD) UCSC-F-H19001 (UCS Rack PCIe/NVMe Storage 1900GB HGST SN150) UCSC-F-H38001 (UCS Rack PCIe/NVMe Storage 3800GB HGST SN150) UCS-PCI25-38001 (UCS PCIe/NVMe2.5"SFF Storage 3800GB HGST SN100)	—	3.1(3a)	3.1(3a)	4.0(1a)	4.1(1a)	4.1(3m)

Adapters	Minimum Software Version UCS 6200 Series FI	Minimum Software Version UCS 6332, 6332-16UP	Minimum Software Version UCS 6332, 6332-16UP	Minimum Software Version UCS 6454	Minimum Software Version UCS 64108	Suggested Software Version UCS 6200 Series FI UCS 6332, 6332-16UP FI UCS 6400 Series FI
	UCS-IOM-2204 UCS-IOM-2208	UCS-IOM-2204 UCS-IOM-2208	UCS-IOM-2304 UCS-IOM-2304V2	UCS-IOM-2204 UCS-IOM-2208 UCS-IOM-2408*	UCS-IOM-2204 UCS-IOM-2208 UCS-IOM-2408*	UCS-IOM-2204 UCS-IOM-2208 UCS-IOM-2408*
				* UCS-IOM-2408 supported on M4 and M5 only with UCS 6400 Series FI		
UCSC-PCIE-QD32GF (Qlogic QLE2742) N2XX-AQPCI05 (Qlogic QLE2562) UCSC-PCIE-Q2672 (Qlogic QLE2672-CSC) UCSC-PCIE-BD32GF (Emulex LPe32002) UCSC-PCIE-BS32GF (Emulex LPe32000) N2XX-AEPCI05 (Emulex LPe12002)	—	3.1(3a)	3.1(3a)	4.0(1a)	4.1(1a)	4.1(3m)
UCSC-PCIE-E16002 (Emulex LPe16002-M6 16G FC rack HBA)	—	3.2(1d)	3.2(1d)	4.0(1a)	4.1(1a)	4.1(3m)
UCSC-PCIE-ID10GC (Intel X550 Dual-port 10GBase-T NIC)	3.1(2b)	3.1(3a)	3.1(3a)	4.0(1a)	4.1(1a)	4.1(3m)
UCSC-OCP-QD10GC (QLogic FastLinQ QL41132H Dual Port 10GbE Adapter)	4.0(1a)	4.0(1a)	4.0(1a)	4.0(1a)	4.0(1a)	4.1(3h) (C125 M5 only)
UCSC-PCIE-QD25GF (QLogic FastLinQ QL41212H 25GbE adapter)	3.1(3a)	3.1(3a)	3.1(3a)	4.0(1a)	4.0(1a)	4.1(3h) (M4, M5 servers)
UCSC-OCP-QD25GF (QLogic FastLinQ QL41232H Dual Port 25GbE Adapter)	4.0(1a)	4.0(1a)	4.0(1a)	4.0(1a)	4.0(1a)	4.1(3h) (C125 M5 only)
UCSC-PCIE-QD40GF (à QLogic FastLinQ QL45412H 40GbE adapter)	3.1(3a)	3.1(3a)	3.1(3a)	4.0(1a)	4.0(1a)	4.1(3h) (M4, M5 servers)
UCSC-PCIE-QD10GC (Qlogic QL41162HLRJ-11-SP dual-port 10GBase-T CAN)	4.0(2a)	4.0(2a)	4.0(2a)	4.0(2a)	4.0(2a)	4.1(3h) (C125 M5 only)
UCSC-PCIE-C100-04 (Cisco UCS VIC 1495)	4.0(1a)	4.0(1a)	4.0(1a)	4.0(1a)	4.0(1a)	4.1(3h) (M5, M6 servers)
UCSC-MLOM-C100-04 (Cisco UCS VIC 1497)	4.0(2a)	4.0(2a)	4.0(2a)	4.0(2a)	4.0(2a)	4.1(3h) (M5 servers)

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

Table 8: Supported Hardware for UCS 6400 Series Fabric Interconnects

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

Table 9: Supported Hardware for UCS 6332, UCS 6332-16UP Fabric Interconnects

Type	Details
Chassis	N20–C6508 UCSB-5108-DC UCSB-5108-AC2 UCSB-5108-DC2 UCSB-5108-HVDC
Fabric Interconnects	UCS 6332UP UCS 6332-16UP

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

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

Table 10: Supported Hardware for UCS 6200 Fabric Interconnects

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

GB Connector Modules, Transceiver Modules, and Cables

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

Note

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

Table 11: Supported Transceiver Modules and Cables for GB Connector Modules

Gb Connector Modules	Transceiver Modules and Cables
FC for UCS 6400 Series Fabric Interconnects	DS-SFP-FC8G-SW DS-SFP-FC8G-LW DS-SFP-FC16G-SW DS-SFP-FC16G-LW DS-SFP-FC32G-SW DS-SFP-FC32G-LW
100-Gb for UCS 6400 Series Fabric Interconnects	QSFP-40/100G-SRBD QSFP-100G-SR4-S QSFP-100G-LR4-S QSFP-100G-SM-SR QSFP-100G-CU1M QSFP-100G-CU2M QSFP-100G-CU3M QSFP-100G-AOC1M QSFP-100G-AOC2M QSFP-100G-AOC3M QSFP-100G-AOC5M QSFP-100G-AOC7M QSFP-100G-AOC10M QSFP-100G-AOC15M QSFP-100G-AOC20M QSFP-100G-AOC25M QSFP-100G-AOC30M

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

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

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

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

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

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

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

Cisco UCS Mini and Components

UCS Mini Supported Chassis

Table 12: Minimum Software Versions for UCS Mini Chassis

Chassis	Minimum Software Version	Suggested Software Version
UCSB-5108-AC2	3.0(1e)	4.1(3m)
UCSB-5108-DC2	3.0(2c)	4.1(3m)

UCS Mini Supported Blade and Rack Servers

Table 13: Minimum Host Firmware Versions for Blade and Rack Servers on UCS Mini

Servers	Minimum Software Version	Suggested Software Version
B200 M5	3.2(1d)	4.1(3m)
B200 M3	3.1(3a)	4.1(3m)
B200 M4	3.1(3a)	4.1(3m)
B260 M4	3.1(3a)	4.1(3m)
B420 M3	3.1(3a)	4.1(3m)
B420 M4	3.1(3a)	4.1(3m)
B460 M4	3.1(3a)	4.1(3m)
B480 M5	3.1(3a)	4.1(3m)
B22 M3	3.1(3a)	4.1(3m)
C220 M3	3.1(3a)	4.1(3m)
C240 M3	3.1(3a)	4.1(3m)
C220 M4	3.1(3a)	4.1(3m)
C240 M4	3.1(3a)	4.1(3m)
C460 M4	3.1(3a)	4.1(3m)
C220 M5	3.2(1d)	4.1(3m)

Servers	Minimum Software Version	Suggested Software Version
C240 M5	3.2(1d)	4.1(3m)
C480 M5	3.2(2b)	4.1(3m)

UCS Mini Supported Adapters

Adapters	Minimum Software Version	Suggested Software Version
UCSB-MLOM-40G-04 (UCS VIC 1440) UCSB-VIC-M84-4P (UCS VIC 1480)	4.0(2a)	4.1(3m)
UCSC-PCIE-IQ10GC (Intel X710-T4)	3.2(2b)	4.1(3a)
UCSC-PCIE-QD25GF (QLogic QL41212H 25GbE) UCSC-PCIE-QD40GF (QLogic QL45212H 40GbE)	3.2(2b)	4.1(3m)
UCSC-PCIE-C40Q-03 (UCS VIC 1385) UCSC-MLOM-C40Q-03 (UCS VIC 1387)	3.1(3a)	4.1(3m)
UCS-VIC-M82-8P (UCS VIC 1280) UCSB-MLOM-40G-01 (UCS VIC 1240) UCSB-MLOM-PT-01 (Cisco Port Expander Card)	3.1(3a)	4.1(3m)
UCSB-MLOM-40G-03 (UCS VIC 1340) UCSB-VIC-M83-8P (UCS VIC 1380) UCSC-MLOM-CSC-02 (UCS VIC 1227)	3.1(3a)	4.1(3m)
UCSC-PCIE-CSC-02 (UCS VIC 1225)	3.1(3a)	4.1(3m)

UCS Mini Supported Fabric Interconnects

Fabric Interconnects	Minimum Software Version	Suggested Software Version
Cisco UCS 6324	3.1(3a)	4.1(3m)

UCS Mini Supported Fabric Extenders for Secondary Chassis

Fabric Extenders	Minimum Software Version	Suggested Software Version
UCS 2204 XP	3.1(3a)	4.1(3m)
UCS 2208 XP	3.1(3a)	4.1(3m)

UCS Mini Supported Power Supplies

Power Supplies	Minimum Software Version	Suggested Software Version
UCSB-PSU-2500ACDV UCSB-PSU-2500DC48 UCSC-PSU-930WDC UCSC-PSU2V2-930WDC UCSC-PSUV2-1050DC UCSC-PSU1-770W UCSC-PSU2-1400 UCSC-PSU2V2-1400W UCSC-PSU2V2-650W UCSC-PSU2V2-1200W	3.1(3a)	4.1(3m)

UCS Mini Supported Gb Connector Modules

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

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

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

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

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 64108 Fabric Interconnects, you cannot downgrade from Cisco UCS Manager Release 4.1.

  See the *Cisco UCS Manager Firmware Management Guide*, Release 4.1 section Firmware Upgrade to Cisco UCS Manager Release 4.1 for detailed upgrade paths.

- 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.
- Upgrading to the latest Intel firmware images in Release 4.1(1a), requires Cisco UCS Manager to be updated to Release 4.1(1a) as well.
- RDMA upgrade/downgrade: if downgrading from RDMA-supported releases to non-RDMA-supported releases, you must manually remove all RDMA-related configurations before downgrade. If upgrading eNIC and eNIC RDMA drivers, upgrade all drivers to the same version at the same time; otherwise, functionality could be lost.

Downgrade Limitation for Cisco UCS C125 M5 Servers

- Starting with Release 4.1(3), AMD Platform Secure Boot (PSB) is introduced in Cisco UCS C125 M5 servers that implements hardware-rooted boot integrity. Once you upgrade to release 4.1(3) or later, you cannot:
  - downgrade Cisco UCS C125 M5 Rack Server Node based on 2nd generation AMD EPYC 7002 Series Processors (Rome) to any release earlier than 4.1(3).
  - downgrade Cisco UCS C125 M5 Rack Server Node based on AMD EPYC 7001 (Naples) to any release earlier than 4.0(2k).

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 14: Version Mapping

UCS Release	Catalog File Name	Additional PIDs In This Release
4.1(3m)	ucs-catalog.4.1.3n.T.bin	—
4.1(3l)	ucs-catalog.4.1.3n.T.bin	—
4.1(3k)	ucs-catalog.4.1.3n.T.bin	—
4.1(3j)	ucs-catalog.4.1.3m.T.bin	—
4.1(3i)	ucs-catalog.4.1.3l.T.bin	—
4.1(3h)	ucs-catalog.4.1.3k.T.bin	—
4.1(3f)	ucs-catalog.4.1.3h.T.bin	—
4.1(3e)	ucs-catalog.4.1.3h.T.bin	—
4.1(3d)	ucs-catalog.4.1.3f.T.bin	Drives for C125 M5, C220 M5, C240 M5, C240 SD M5, C480 M5, and C480 M5 ML servers: • UCS-SD960GBKNK9 • UCS-SD38TBKNK9 • UCS-SD800GBKNK9 • UCS-SD16TBKNK9 Drives for B200 M5 and B480 M5 servers: • UCS-SD960GBKBNK9 • UCS-SD38TBKBNK9 • UCS-SD800GBKBNK9 • UCS-SD16TBKBNK9 Drives for S3260 M5 server: • UCS-S3260-TSD8K9

UCS Release	Catalog File Name	Additional PIDs In This Release
4.1(3c)	ucs-catalog.4.1.3c.T.bin	

UCS Release	Catalog File Name	Additional PIDs In This Release
		Drives for C125 M5, C220 M5, C240 M5, C240 SD M5, C480 M5, and C480 M5 ML servers: • UCS-SD960GK1X-EV • UCS-SD19TK1X-EV • UCS-SD38TK1X-EV • UCS-SD76TK1X-EV • UCS-SD15TK1X-EV Drives for B200 M5 and B480 M5 servers: • UCS-SD960GKB1X-EV • UCS-SD19TKB1X-EV • UCS-SD38TKB1X-EV • UCS-SD76TKB1X-EV • UCS-SD15TKB1X-EV • UCS-SD800GKB3X-EP • UCS-SD16TKB3X-EP • UCS-SD32TKB3X-EP Drives for C125 M5, C220 M5, C240 M5, and C480 M5 servers: • UCS-SD800GK3X-EP • UCS-SD16TK3X-EP • UCS-SD32TK3X-EP Drives for S3260 M5 server: • UCS-S3260-3KSD8 • UCS-S3260-3KSD16 • UCS-S3260-3KSD32 Drives for C220 M5 and C240 M5 servers: • UCS-SD19TBEM2NK9 CPUs for C125 M5 server: • UCS-CPU-A7F32 • UCS-CPU-A7262 • UCS-CPU-A7272

UCS Release	Catalog File Name	Additional PIDs In This Release
		• UCS-CPU-A7282 • UCS-CPU-A7302 • UCS-CPU-A7402 • UCS-CPU-A7452
4.1(3b)	ucs-catalog.4.1.3b.T.bin	—
4.1(3a)	ucs-catalog.4.1.2e.T.bin	CPUs for C125 M5 servers: • UCS-CPU-A7F32 • UCS-CPU-A7302 • UCS-CPU-A7272
4.1(2c)	ucs-catalog.4.1.2g.T.bin	—
4.1(2b)	ucs-catalog.4.1.2b.T.bin	Micro-SD Card: • UCS-S-MSD960K9
4.1(2a)	ucs-catalog.4.1.1d.T.bin	CPUs for C240 M5 servers: • UCS-CPU-I6256 • UCS-CPU-I6250 Drives for C220 M5 and C240 M5 servers: • UCS-HD16T7KL4KN • UCS-HD14TT7KL4KN Drives for UCS S3260 M5 servers: • UCS-S3260-HDT14T • UCS-S3260-HDT14TR • UCS-S3260-HD16T • UCS-S3260-HD16TR
4.1(1e)	ucs-catalog.4.1.1e.T.bin	—

UCS Release	Catalog File Name	Additional PIDs In This Release
4.1(1d)	ucs-catalog.4.1.1d.T.bin	CPUs for C240 M5 servers: • UCS-CPU-I6256 • UCS-CPU-I6250 Drives for C220 M5 and C240 M5 servers: • UCS-HD16T7KL4KN • UCS-HD14TT7KL4KN Drives for UCS S3260 M5 servers: • UCS-S3260-HDT14T • UCS-S3260-HDT14TR • UCS-S3260-HD16T • UCS-S3260-HD16TR
4.1(1c)	ucs-catalog.4.1.1c.T.bin	—
4.1(1b)	ucs-catalog.4.1.1b.T.bin	CPUs for UCS B200 M5, C220 M5, and C240 M5 servers: • UCS-CPU-I6258R • UCS-CPU-I6248R • UCS-CPU-I6242R • UCS-CPU-I6246R Drives: • UCS-HD10T7K4KAN • UCS-S3260-HD10TA • UCS-S3260-10TARR • UCS-HD10T7K4KAN • UCS-SD960GBM2NK9 • UCS-SD38TBEM2NK9 • UCS-SD76TBEM2NK9

UCS Release	Catalog File Name	Additional PIDs In This Release
4.1(1a)	ucs-catalog.4.1.1a.T.bin	Cisco UCS 64108 Fabric Interconnect: • UCS-FI-6454 NICs for UCSC-C125 M5: • UCSC-PCIE-IQ10GF • UCSC-PCIE-ID25GF • UCSC-PCIE-ID10GF GPU for UCSC-C125 M5: • UCSC-GPU-T4-16 NVME Drives for UCSC-C125: • UCSC-NVME2H-I1000 • UCSC-NVME2H-I4000 • UCSC-NVME2H-I1600 • UCSC-NVME2H-I3200 HBA for UCSC-C125 M5: • UCSC-PCIE-QD16GF Mellanox NICs for UCS C220 M5, C240 M5, C480 M5: • UCSC-P-M5S100GF • UCSC-P-M5D25GF Mellanox NICs for UCS C125 M5: • UCSC-O-M5S100GF GPU in the IO Expander for UCSC-S3260 M5: • UCSC-GPU-T4-16

Default Open Ports

The following table lists the default open ports used in Cisco UCS Manager Release 4.1.

Port	Interface	Protocol	Traffic Type	Fabric Interconnect	Usage
22	CLI	SSH	TCP	UCS 6200 Series UCS 6300 Series UCS 6400 Series UCS 6500 Series	Cisco UCS Manager CLI access
80	XML	HTTP	TCP	UCS 6200 Series UCS 6300 Series UCS 6400 Series UCS 6500 Series	Cisco UCS Manager GUI and third party management stations. Client download
443	XML	HTTP	TCP	UCS 6200 Series UCS 6300 Series UCS 6400 Series UCS 6500 Series	Cisco UCS Manager login page access Cisco UCS Manager XML API access
743	KVM	HTTP	TCP	UCS 6200 Series UCS 6300 Series UCS 6400 Series	CIMC Web Service / Direct KVM
843	xmlPolicy	Adobe Flash	TCP	UCS 6200 Series UCS 6300 Series	Adobe Flash port used by KVM launcher
7546	CFS	CFSD	TCP	UCS 6400 Series UCS 6500 Series	Cisco Fabric Service

Cisco UCS Manager Network Management Guide, Release 4.1 provides a complete list of open TCP and UDP ports.

Security Fixes

Security Fixes in Release 4.1(3j)

Defect ID—CSCwa33718

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

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

For more information, see:

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

Security Fixes in Release 4.1(3i)

Defect ID—CSCwb67159

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

- CVE-2021-0189—Use of out-of-range pointer offset in the BIOS firmware for some Intel® Processors may allow a privileged user to potentially enable aescalation of privilege through local access.
- CVE-2021-0159—Improper input validation in the BIOS authenticated code module for some Intel® Processors may allow a privileged user to potentially enable aescalation of privilege through local access.
- CVE-2021-33123—Improper access control in the BIOS authenticated code module for some Intel® Processors may allow a privileged user to potentially enable aescalation of privilege through local access.
- CVE-2021-33124—Out-of-bounds write in the BIOS authenticated code module for some Intel® Processors may allow a privileged user to potentially enable aescalation of privilege through local access.
- CVE-2022-21131—Improper access control for some Intel® Xeon® Processors may allow an authenticated user to potentially enable information disclosure through local access.
- CVE-2022-21136—Improper input validation for some Intel® Xeon® Processors may allow a privileged user to potentially enable denial of service through local access.

Defect ID—CSCwb67158

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

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

Defect ID—CSCwb67157

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

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

Defect ID—CSCwa33718

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

- CVE-2021-34798—This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.

For more information, read:

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

Security Fixes in Release 4.1(3f)

Defect ID - CSCvy91321

CVE-2021-34736

UCS C-Series Rack Servers in standalone mode and UCS S-Series Storage Servers in standalone mode are affected by a vulnerability in the web-based management interface of Cisco Integrated Management Controller (IMC) Software could allow an unauthenticated, remote attacker to cause the web-based management interface to unexpectedly restart.

The vulnerability is due to insufficient input validation on the web-based management interface. CVE-2021-34736 could allow an attacker to exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause the interface to restart, resulting in a denial of service (DoS) condition.

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

Security Fixes in Release 4.1(3e)

Defect ID - CSCvy16762

Cisco UCS B-series M5 blade servers and C-series M5 rack servers that are based on Intel® processors are affected by vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) IDs:

- CVE-2020-12358: Out of bounds write in the firmware for some Intel(R) Processors may allow a privileged user to potentially enable denial of service via local access.
- CVE-2020-12360: Out of bounds read in the firmware for some Intel(R) Processors may allow an authenticated user to potentially enable escalation of privilege via local access.
- CVE-2020-24486: Improper input validation in the firmware for some Intel(R) Processors may allow an authenticated user to potentially enable denial of service via local access.
- CVE-2020-24511: Improper isolation of shared resources in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access.

This release includes BIOS revisions for Cisco UCS M5 blade and tack servers. These BIOS revisions include Microcode update for Cisco UCS M5 blade and rack servers, which is a required part of the mitigation for these vulnerabilities.

Security Fixes in Release 4.1(3d)

Defect ID - CSCvx82644

On March 25, 2021 - the OpenSSL Software foundation disclosed two high severity vulnerabilities affecting the OpenSSL software package.

- CVE-2021-3450 could allow a remote unauthenticated attacker to conduct a MiTM attack or to impersonate another user or device by providing a crafted certificate.
- CVE-2021-3449 could allow a remote unauthenticated attacker to crash a TLS server resulting in a Denial of Service (DoS) condition.

Cisco has evaluated the impact of the vulnerability on this product and concluded that Cisco UCS M5 B-series server Cisco IMCs are affected by CVE-2021-3449 .

However, all Cisco UCS M4 and earlier B-series server CIMCs are not affected by: CVE-2021-3450.

Cisco UCS Manager release bundle 4.1(3a)B through 4.1(3c)B packaged M5 CIMC is using CiscoSSL based on OpenSSL 1.1.1g. It was the first and only release to be affected by CVE-2021-3449..

It is not vulnerable to CVE-2021-3450 which only affects 1.1.1h-1.1.1j.

Security Fixes in Release 4.1(3a) and 4.1(2c)

Defect IDs

- CSCvw45654
- CSCvw38983
- CSCvv96107
- CSCvw38995

CVE-2021-1368

A vulnerability in the Unidirectional Link Detection (UDLD) feature of Cisco FXOS Software and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to execute arbitrary code with administrative privileges or cause a denial of service (DoS) condition on an affected device.

For more information on security advisory, see:

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-udld-rce-xetH6w35

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

Security Fixes in Release in 4.1(3a)

Defect ID - CSCvv34145

Cisco UCS B200 M5 blade servers that are based on Intel® processors are affected by vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) IDs:

- CVE-2020-8738: Improper conditions check in Intel BIOS platform sample code for some Intel® Processors before may allow a privileged user to potentially enable escalation of privilege via local access.
- CVE-2020-8764: Improper access control in BIOS firmware for some Intel® Processors may allow a privileged user to potentially enable escalation of privilege via local access.
- CVE-2020-0590: Improper input validation in BIOS firmware for some Intel® Processors may allow an authenticated user to potentially enable escalation of privilege via local access.
- CVE-2020-8745: Insufficient control flow management in subsystem for Intel® CSME versions before 11.8.80, 11.12.80, 11.22.80, 12.0.70, 13.0.40, 13.30.10, 14.0.45 and 14.5.25 , Intel® TXE versions before 3.1.80 and 4.0.30 may allow an unauthenticated user to potentially enable escalation of privilege via physical access.
- CVE-2020-8752: Out-of-bounds write in IPv6 subsystem for Intel® AMT, Intel® ISM versions before 11.8.80, 11.12.80, 11.22.80, 12.0.70, 14.0.45 may allow an unauthenticated user to potentially enable escalation of privileges via network access.

- CVE-2020-8753: Out-of-bounds read in DHCP subsystem for Intel® AMT, Intel® ISM versions before 11.8.80, 11.12.80, 11.22.80, 12.0.70 and 14.0.45 may allow an unauthenticated user to potentially enable information disclosure via network access.
- CVE-2020-8705: Insecure default initialization of resource in Intel® Boot Guard in Intel® CSME versions before 11.8.80, 11.12.80, 11.22.80, 12.0.70, 13.0.40, 13.30.10, 14.0.45 and 14.5.25, Intel® TXE versions before 3.1.80 and 4.0.30, Intel® SPS versions before E5_04.01.04.400, E3_04.01.04.200, SoC-X_04.00.04.200 and SoC-A_04.00.04.300 may allow an unauthenticated user to potentially enable escalation of privileges via physical access.
- CVE-2020-12297: Improper access control in Installer for Intel® CSME Driver for Windows versions before 11.8.80, 11.12.80, 11.22.80, 12.0.70, 13.0.40, 13.30.10, 14.0.45 and 14.5.25, Intel TXE 3.1.80, 4.0.30 may allow an authenticated user to potentially enable escalation of privileges via local access.
- CVE-2020-12303: Use after free in DAL subsystem for Intel® CSME versions before 11.8.80, 11.12.80, 11.22.80, 12.0.70, 13.0.40, 13.30.10, 14.0.45 and 14.5.25, Intel® TXE 3.1.80, 4.0.30 may allow an authenticated user to potentially enable escalation of privileges via local access.

Security Fixes in Release in 4.1(1a)

Defect ID - CSCvp31006

Cisco UCS Manager includes a version of the Apache HTTP Server that is affected by the vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) ID:

- CVE-2019-0211: In Apache HTTP Server 2.4 releases 2.4.17 to 2.4.38, with MPM event, worker or prefork, code executing in less-privileged child processes or threads (including scripts executed by an in-process scripting interpreter) could execute arbitrary code with the privileges of the parent process (usually root) by manipulating the scoreboard. Non-Unix systems are not affected.

Apache 2.4.39 is integrated in UCS Manager 4.1(1a) and beyond.

Security Fixes in Release in 4.1(1c)

Defect ID - CSCvw07430

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

- CVE-2020-0591: Improper buffer restrictions in BIOS firmware for some Intel® Processors may allow a privileged user to potentially enable escalation of privilege via local access.
- CVE-2020-0592: Out of bounds write in BIOS firmware for some Intel® Processors may allow an authenticated user to potentially enable escalation of privilege and/or denial of service via local access.
- CVE-2020-8738: Improper conditions check in Intel BIOS platform sample code for some Intel® Processors may allow a privileged user to potentially enable escalation of privilege via local access.
- CVE-2020-8740: Out of bounds write in Intel BIOS platform sample code for some Intel® Processors may allow a privileged user to potentially enable escalation of privilege via local access.
- CVE-2020-8764: Improper access control in BIOS firmware for some Intel® Processors may allow a privileged user to potentially enable escalation of privilege via local access.

Cisco has reviewed these products and concluded that they are affected by these vulnerabilities. However, the products are not affected by the following vulnerabilities:

CVE-2020-0587 CVE-2020-0588 CVE-2020-0590 CVE-2020-0593 CVE-2020-8696 CVE-2020-8698 CVE-2020-8695 CVE-2020-8694 CVE-2020-8752 CVE-2020-8753 CVE-2020-8745 CVE-2020-8750 CVE-2020-8757 CVE-2020-8756 CVE-2020-8760 CVE-2020-8744 CVE-2020-8751 CVE-2020-8754 CVE-2020-8761 CVE-2020-8747 CVE-2020-8755 CVE-2020-8746 CVE-2020-8749 CVE-2020-8705 CVE-2020-12303 CVE-2020-12304 CVE-2020-12354 CVE-2020-12355 CVE-2020-12356 CVE-2020-12297

Security Fixes in Release in 4.1(1e) and 4.1(2a)

Defect ID - CSCvu53094

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:

- 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.

Security Fixes in Release in 4.1(2a)

Defect IDs - CSCvt86097 and CSCvt86093

Cisco UCS M5 servers that are based on Intel® processors are affected by vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) IDs:

- CVE-2020-0548 affects when cleanup errors in some Intel® processors may allow an authenticated user to potentially enable information disclosure through local access.
- CVE-2020-0549 affects when cleanup errors in some data cache evictions for some Intel® processors may allow an authenticated user to potentially enable information disclosure through local access.

Security Fixes in Release in 4.1(1d)

Defect ID - CSCvt86093

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):

- CVE-2020-0548: Clean-up errors in some Intel® Processors may allow an authenticated user to potentially enable information disclosure via local access.
- 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.

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.

Security Fixes in Release in 4.1(1c)

Defect IDs - CSCvs81686 and CSCvs81690

Cisco UCS M5 servers that are based on Intel® processors are affected by vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) IDs:

- CVE-2020-0548 Cleanup errors in some Intel® Processors may allow an authenticated user to potentially enable information disclosure via local access.
- 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.

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.

Security Fixes in Release in 4.1(1a)

Defect IDs - CSCvr15082

CVE-2020-3120

A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could have allowed an unauthenticated, local attacker to reload an affected device, resulting in a denial of service (DoS) condition.

The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to reload.

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

Defect ID - CSCvp27917

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.

- 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.
- 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.
- 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.
- 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 Hypervisor patches from the appropriate vendors.

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.

Additional details about the vulnerabilities listed above can be found at http://cve.mitre.org/cve/cve.html

Defect IDs - CSCvr54409 and CSCvr54415

Cisco UCS B-Series and C-Series M5 servers that are based on Intel® processors are affected by vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) IDs:

- 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.
- 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.
- 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.
- 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.
- 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.
- 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.
- 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.

This release includes BIOS revisions for Cisco UCS B-Series and C-Series 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.

Defect ID - CSCvr54411

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:

- 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.

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.

Defect IDs - CSCvr54413 and CSCvr54414

Cisco UCS B-Series and C-Series M4 servers that are based on Intel® processors are affected by vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) IDs:

- 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.
- 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.

This release includes BIOS revisions for Cisco UCS B-Series and C-Series 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.

Defect ID - CSCvp30013

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.

- 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.
- 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.
- 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.
- 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 Hypervisor patches from the appropriate vendors.

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.

Defect ID - CSCvp27917

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.

- 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.
- 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.
- 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.
- 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 Hypervisor patches from the appropriate vendors.

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.

Additional details about the vulnerabilities listed above can be found at http://cve.mitre.org/cve/cve.html

Resolved Caveats

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

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

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

Resolved Caveats in Release 4.1(3m)

The following caveats are resolved in Release 4.1(3m):

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCwa11345	In a setup equipped with Cisco UCS 6200 FI series, the domain is unavailable and Cisco UCS Manager GUI is inaccessible after a complete power outage. This issue is resolved.	4.1(3c)A	4.1(3m)A

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCwe35644	Several ECCs are observed on a single DIMM with no fault from Cisco UCS Manager in Cisco UCS C-Series and B-Series M5 and M6 servers equipped with 64GB DIMMs (UCS-MR-X64G2RW) and ADDDC enabled. This issue is resolved.	4.1(3e)B and C	4.1(3m)B and C
CSCwh30074	Cisco UCS 6300 FI series unexpectedly reboots with the following reset reason: `vlan_mgr hap reset` This issue is resolved.	4.1(3l)A	4.1(3m)A
CSCwf39250	In a setup equipped with Cisco UCS 6400 FI series, multiple SSH failed authentication events exhaust the process memory limit. As a result, samcproxy and other services fail. This issue is resolved.	4.2(1m)A	4.1(3m)A
CSCwh31644	Cisco UCS Manager fails to discover any Chassis or rack servers. This issue is resolved.	4.2(3e)A	4.1(3m)A
CSCwd41247	Multiple instances of hung **Samcproxy** is observed in a setup equipped with Cisco UCS 6400 FI. There may also be other miscellaneous faults on the domain related to **Samcproxy** being in a bad state. This issue is resolved.	4.2(1i)A	4.1(3m)
CSCwb82433	Cisco UCS C220 M5 servers equipped with Cisco UCS VIC 1400 series adapter and have **Geneve** feature enabled, go offline after the Cisco UCS VIC adapters fail to respond. This issue is resolved.	4.1(3d)A	4.1(3m)

Resolved Caveats in Release 4.1(3l)

The following caveats are resolved in Release 4.1(3l):

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCwe54991	Following command is unavailable in Cisco UCS 6400 FI series: `show platform software enm internal info vlandb` This issue is resolved.	4.2(1m)A	4.1(3l)A
CSCwd19078	Cisco UCS Blade servers lose SAN connectivity when one of the FC up-link or FI is down because of the following reasons: • FC link is congested • Peer FC link is down due to peer system crash or errors on the receiving side This issue is resolved.	4.2(1f)A	4.1(3l)A
CSCwd20789	If the target received an abort for an IOM for which the target is unaware of, a reject is sent back to the initiator. This causes the driver to log out the target and then send GPNFT to re-initiate the target log in sequence. This issue is resolved.	4.1(3j)B	4.1(3l)B

Resolved Caveats in Release 4.1(3k)

The following caveats are resolved in Release 4.1(3k):

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCwd04797	Cisco UCS M5 servers equipped with NVMe drives get stuck at POST in legacy boot mode after UCS firmware upgrade. This issue is resolved.	4.1(3h)C	4.1(3k)C

Resolved Caveats in Release 4.1(3j)

The following caveats are resolved in Release 4.1(3j):

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCvt22099	In a setup equipped with Cisco UCS B200 M5 servers and 6248 FIs, the server discovery fails with the following FSM message even though the OS runs normally: `Unsupported adapter on the current UCS Firmware Version, therefore discovery of this system will not complete successfully.` This issue is resolved.	4.0(4e)A	4.1(3j)A

CSCvs45242	Following error is displayed while upgrading the A bundle:
	`info F1889 2018-07-30T16:25:33.989 59987120 1/34 on FI-A is connected by a unknown server device`
	`Info F1889 2018-07-30T16:25:23.855 59987130 1/35 on FI-A is connected by a unknown server device`
	This issue is resolved.
		4.0(4f)A	4.1(3j)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`. This issue is resolved.	4.0(4h)A	4.1(3j)A

Resolved Caveats in Release 4.1(3i)

The following caveats are resolved in Release 4.1(3i):

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCvz98195	If large numbers of LUNs are zoned to a Cisco UCS C-Series server, with Emulex HBA, integrated with Cisco UCS Manager using Cisco UCS 6200 FI, and if the HBA is not managed by Cisco UCS Manager, then it leads to discovery and re-acknowledgment failures. This issue is resolved.	4.1(3c)A	4.1(3i)A
CSCwa64691	After the primary FI reboot, Slow drain default setting gets automatically set. Slow drain default setting is **enabled**. This issue is resolved.	4.1(3d)A	4.1(3i)A

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCwa85770	Cisco UCS M4 servers show additional remote NDIS compatible devices in the Ethernet interfaces. This issue is resolved.	4.1(3h)C	4.1(3i)C

CSCwa88180	Following fault may be seen in the domain with the VLAN count optimization disabled after configuring a new ACI EPG:
	`Severity: Critical`
	`Code: F999675`
	`Description: [FSM:FAILED]:`
	`Uplink eth port`
	`configuration on B(FSM:sam:dme:`
	`SwEthLanBorderDeploy).`
	`Remote-Invocation-Error: Internal Error`
	This issue is resolved.
		4.1(3f)A	4.1(3i)A

CSCwb34837	Cisco UCS B-Series servers take a long time to load Microsoft Windows 2016 and 2019 login screen due to FC remote volume map attempts. This issue is resolved.	4.1(3b)B	4.1(3i)A
CSCwb83355	When SCSI reservation is used by ESX cluster software to manage access to shared volumes, Cisco UCS VIC 14xx reports firmware/SCSI status as DATA_CNT_MISMATCH/RESERVATION_CONFLICT if the target does not set RESID bits for any IO that receives RESERVATION_CONFLICT status. ESX SCSI layer considers DATA_CNT_MISMATCH as a failure and ignores the RESERVATION_CONFLICT SCSI status. When too many reservation conflicts are received, it degrades the Virtual Machines performance. This issue is resolved.	4.1(3g)	4.1(3i)
CSCwa57947	It is observed in Cisco UCS VIC 14xx series adapters that incoming LLDP/CDP packets are dropped. ESXi vmNIC does not report any details despite that the FI TX counters reports LLDP packets leaving the FIs. This issue is resolved.	4.1(1f)B	4.1(3i)B
CSCwa90880	Both the Cisco UCS 6330 FIs reboot after upgrading to release 4.1(3f) due to LLDP Hap reset. This issue is resolved.	4.1(3f)A	4.1(3i)A

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCvy32420	It is observed that while updating the IOM firmware, few IOMs go offline randomly and also come back online after few minutes. vHBAs on the specific IOM FI paths also disconnect and reconnect. This issue is resolved.	4.0(4h)A	4.1(3i)A
CSCwb33900	In a setup with Cisco UCS 6400 FIs, SNMPd crashes with core to a stateful crash. This issue is resolved.	4.1(3h)A	4.1(3i)A
CSCvx37634	Cisco UCS B200 M5 server discovery fails with the following fault message: `Setup of Vmediafailed(sam:dme: ComputeBladeDiscover:SetupVm` This issue is resolved.	4.1(1c)B	4.1(3i)B
CSCwa85667	BMC reset is observed on Cisco UCS C-Series and B-Series M5 servers due to kernel crash and watchdog reset. This issue is resolved.	4.0(4m)	4.1(3i)
CSCvz49048	In a setup equipped with Cisco UCS 2408 IOMs, it is observed that the I2C errors increase and this turns on amber LEDs for fans. This issue is resolved.	4.1(2b)A	4.1(3i)A
CSCwa58954	It is observed that in a setup equipped with 64xx FIs, you are unable to login to Cisco UCS Manager GUI or other issues like discovery or shallow discovery failure. This issue is resolved.	4.1(3e)A	4.1(3i)A
CSCwb89732	In a setup with 6400 FIs, while accessing the KVM IP address, you are redirected to Cisco UCS Manager GUI. This issue is resolved.	4.1(3f)A	4.1(3i)A
CSCvv57606	On installing a M5 server in a chassis for the first time, a service profile may fail and throw the connection placement error. This issue is seen as the path is not being established for the adapter on Fabric Interconnect A and Fabric Interconnect B. This issue is resolved.	4.0(4e)A	4.1(3i)A

Defect ID	Symptom	First Bundle Affected	Resolved in Release

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

CSCvz86823	On a Cisco UCS B200 M4 server, UEFI boot parameters were not written to BIOS NVRAM on first boot in UEFI Boot mode, although the issue resolved on reboot. This issue is resolved.	4.1(1a)	4.1(3i)A

Resolved Caveats in Release 4.1(3h)

The following caveats are resolved in Release 4.1(3h):

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCvy98914	Under certain conditions, Cisco UCS 6332 Fabric Interconnect experienced a DME crash and core dump while de-commissioning or re-commissioning the server. This issue is resolved.	4.1(2b)A	4.1(3h)A
CSCvz64536	A UCS C240 M5 Rack server failed discovery when all PCIe slots were populated. The message `HBA Firmware Version Error` was displayed. This issue is resolved.	4.1(3c)A	4.1(3h)A
CSCvz98572	Under certain conditions with small block size and sequential writes, HGST HUS728T8TAL4200 (Air Filled) drives may show higher latency when compared to the HGST HUH721008AL4200 (Helium Filled) drives This issue is resolved on update to firmware version A9GH.	4.1(3f)A	4.1(3h)A

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCvz74423	A 6400 series Fabric Interconnect running UCS Manager with NXOS crashed and rebooted. The system showed a reset reason: `Reset Reason (SW): Reset triggered due to HA policy of Reset (16) at time...` This issue is resolved.	4.1(3a)A	4.1(3h)A
CSCvz44891	On a Cisco UCS blade server with 2300 series fabric interconnect, IOM 2300 unexpectedly powered off the entire chassis. This issue is resolved.	4.1(2b)A	4.1(3h)A
CSCvy72488	A blade server with 6400 series fabric interconnect experienced a user account decryption failure. This issue is resolved.	4.1(3c)	4.1(3h)
CSCvz34187	Lower Non-Critical (LNC) thresholds were incorrect on PS2 and PS3 The fix for this defect removes the LNC thresholds altogether. This issue is resolved.	4.1(3d)A	4.1(3h)A
CSCvy74106	On a UCS-Managed B-series blade server with a 6200 Fabric Interconnect, the DME process in UCSM could dump core with memory limit exhaustion , if it experienced continuous authorized web logins with LDAP based remote user logins. This issue is resolved.	4.1(3b)A	4.1(3h)A
CSCvx18989	On a UCS-Managed B series blade server attached to a 64108 Fabric Interconnect, enabling ports from port 49 used a 100G license instead of a 10G license. This issue is resolved.	4.1(2b)	4.1(3h)A
CSCvy69605	Cisco UCS C240 M4 and M5 servers managed through LOM ports using FEXs connected to FI server ports failed discovery with the message: `ERR-insufficiently Equipped`. This issue is resolved.	4.(3d)C	4.1(3h)C
CSCvz72923	On UCS Managed blade servers with Series 1300 VIC adapters, intermittent connectivity loss occurred, followed by full connectivity loss. This issue is resolved.	4.1(3a)B	4.1(3h)B

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCvz86823	On a Cisco UCS B200 M4 server, UEFI boot parameters were not written to BIOS NVRAM on first boot in UEFI Boot mode, although the isssue resolved on reboot. This issue is resolved.	4.1(1a)	4.1(3h)
CSCvz08447	Fabric interconnect UCS-FI-6454 running 4.0(4a) unexpectedly rebooted Fabric Interconnect B. NXOS logs the following reset reason: `Reason: Reset triggered due to HA policy of Reset Service: sysmgr stateful recovery` This issue is resolved.	4.0(4a)A	4.1(3h)A
CSCvy52458	On a blade server connected to a 6400 series fabric interconnect, the UCS Manager NTP configuration was not pushed to NXOS. This issue is resolved.	4.0(4g)A	4.1(3h)A
CSCvz55331	6454, 64108, 6332, and 6332-16UP series Fabric Interconnect could reboot due to PFMA Hap reset. This issue is resolved only after upgrading to release 4.1(3h) or later. If you are running any release earlier than 4.1(3h), then disable SNMP before upgrading. You can enable SNMP once IOMs are online.	4.1(3e)A	4.1(3h)A
CSCvn71034	SNMP traps sent out for high value seen on rcvDelta counter on FI Ethernet Uplinks while there are no traces of the traps/counters seen in UCS-M Logs This issue is resolved.	4.0(4b)A	4.1(3h)A
CSCvz37497	A UCS 6332 Fabric Interconnect reset unexpectedly due to HA Policy reset. This issue is resolved.	4.0(4a)A	4.1(3h)A
CSCvx54145	When using the Chrome and Edge browsers, when navigating through Firmware Management by clicking Installed Firmware > Activate Firmware, then clicking on the + sign did not open the list view. This issue is resolved.	4.1(1c)A	4.1(3h)A

Resolved Caveats in Release 4.1(3f)

The following caveats are resolved in Release 4.1(3f):

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCvz21538	A Cisco UCS blade server running NXOS with a 2400 series fabric extender detected a drop in IOPS to FC storage during a fabric inerconnect reboot. This issue is resolved.	4.0(1)A	4.1(3f)A
CSCvz26396	A Cisco UCS blade server with VIC 1400 series adapter could abort or drop packets during the initial link-up period. This issue is resolved.	4.0(1)A	4.1(3f)A
CSCvz26417	On a Cisco UCS blade server with VIC 1400 series adapter, packet drops occurred during the first 2 seconds of link up between IOM and VIC adapter. This issue is resolved.	4.0(1)A	4.1(3f)A
CSCvx25595	A Cisco UCS B200 M6 server with a 6400 Series fabric interconnect experienced an abort while running fibre channel and ethernet traffic. This issue is resolved.	4.1(3e))A	4.1(3f)A

Resolved Caveats in Release 4.1(3e)

The following caveats are resolved in Release 4.1(3e):

Defect ID	Symptom	First Bundle Affected	Resolved in Release

CSCvw55803	A Cisco UCS 6454 Fabric Interconnect is rebooted and recovered during normal operation. The system displayed the message:
	`Last reset at 591270 usecs after Fri Nov 20 13:49:23 2020`
	`Reason: Kernel Panic`
	This issue is resolved.
		4.0(4g)A	4.1(3e)A

CSCvx02892	When a default gateway is modified on Cisco UCS 6400 Series Fabric Interconnects through GUI or CLI, the new IP route statement was appended and replaced with the old VRF (default) route and resulted in intermittent or failed connections from outside of the MGMT subset. This issue is resolved.	4.1(1a)C	4.1(3e)C

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCvx93523	While upgrading the server firmware from 4.1(1e) to 4.1(3b), the UCSC-PCIE-IQ10GF (Intel X710-DA4 adapter) failed to update the firmware image on Cisco UCS C220 M5 servers. This issue is resolved.	4.1(3b)C	4.1(3e)C
CSCvy80431	When a blade server was removed from a chassis and re-added, the core file dumps were created in the BladeAG service because of accessing the mgmtController-MO without checking the existing MO from computeExtBoard-MO. This operation further led to BladeAG service crash and continuous restarts. This issue is resolved.	4.1(2b)A	4.1(3e)A
CSCvx09287	When multiple SNMP queries are triggered at the same time from different queriers to Cisco UCS Manager on Cisco UCS 6454 Fabric Interconnect, Cisco UCS Manager may send SNMP responses to the wrong querier. This issue is resolved.	4.1(2b)A	4.1(3e)A
CSCvy39679	On Cisco UCS 6400 series Fabric Interconnect, (some) Ethernet ports with (certain) Fiber Channel SFPs can link-up. But these ports could see traffic issues (CRCs/Bad packets) and intermittent link drops. The issue has been fixed and Ethernet ports with Fiber Channel SFPs will not be brought-up.	4.0(1a)A	4.1(3e)A
CSCvy81441	In rare situations, on UCS 6324 Fabric Interconnect, it is observed that high availability is not ready in peer Fabric Interconnect and sam dme crash is seen. This issue is resolved.	4.1(2b)A	4.1(3e)A
CSCvy89884	On Cisco UCS 6400 series Fabric Interconnect, when VLAN1 is configured as non-native VLAN, the OS/Blade vNIC sends VLAN1 tagged traffic to Fabric Interconnect and the Fabric Interconnect sends return traffic to blade with Vlan1 as untagged. Thereby, resulting in network connectivity issues. Whereas, the C-series integrated traffic for non-native VLAN1 is not affected whether it is directly connected to C-series or through fabric extender. This issue is resolved.	4.1(3b)A	4.1(3e)A

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCvy69863	On Cisco UCS 6454 Fabric Interconnects, when the repeated Remote (LDAP, Radius, etc) logins occur from a monitoring service several times per minute, the "samcproxy_proxy" process is crashed and a core file is generated. Thereby, resulting in issue with NXOS process as the PortAG and dcosAG processes rely on samcproxy_proxy for communication to NXOS processes. The faults related to Fabric Interconnect ports or user login may also be present. This issue is resolved.	4.1(3d)A	4.1(3e)A
CSCvx88769	In situations during downgrade of Cisco UCS Manager from 4.2(x) to 4.1(3d) or earlier releases, Cisco UCS manager gets downgraded to 4.1(3d) or earlier release. And, if for some reason Fabric Interconnect reboot happens even before Fabric Interconnect gets downgraded to 4.1(x) or earlier releases, the Fabric Interconnect gets stuck in 4.2(x). This situation results in failure of user login. The defect is partially resolved to enable user login through CLI when Cisco UCS manager is up. So that, the user can recover the setup through CLI. **Note** Cisco UCS Manager GUI will still not be accessible. For more information, see CSCvy90962 in the Open Caveats section.	4.1(3c)	4.1(3e)
CSCvy01206	Discovery of blade servers are stuck as the duplicate Processor Node Utility Operating System (PNuOS) ISO image files are retained in the bootflash/mgmtxt folder, whereas, new ISO files are saved in the bootflash/pnuos folder. This issue is resolved.	4.1(3c)A	4.1(3e)A
CSCvw76521	On 6400 series Fabric Interconnect, if vHBA or vNIC is disabled when server is in shutdown state, vHBA or vNIC fails to come up when vHBA or vNIC is enabled after the server OS is booted up. This issue is resolved.	4.1(2)A	4.1(3e)A

Resolved Caveats in Release 4.1(3d)

The following caveats are resolved in Release 4.1(3d):

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCvx99917	After an upgrade, service profiles failed with the error: `Too many RoCE resources applied on the adaptor. Reduce number of RoCE enabled vNIC's/SubvNIC's or reduce total number of queue pairs or memory regions applied on the adaptor.not enough vNIC available.` This issue is resolved.	4.1(3c)B	4.1(3d)B
CSCvw64214	The Azure Stack Hub server failed due to a failure in the QLogic NIC driver. This issue is resolved.	4.0(4i)C	4.1(3d)C
CSCvw38535	A Cisco UCS S3260 SAS Expander was not accessible from CMC. This issue is resolved.	4.0(4f)C	4.1(3d)C
CSCvw82919	Under specific ECC error conditions in which an uncorrectable ECC error occured, the system flagged only one DIMM in the channel as encountering a UECC, but should have reported both DIMMs in the channel for the error. This issue is resolved.	4.0(4h)B	4.1(3d)B
CSCvy00304	On Cisco UCS M5 servers, `BIOSDetailedErrorLog` logged an incorrect Bank and Bank Group This issue is resolved.	4.1(3c)B	4.1(3d)B
CSCvx50456	A Cisco UCW B460 M4 with UCSB-MLOM-40G-03 VIC 1340 fabric interconnect, UCSB-MLOM-PT-01 port expander, and UCSB-VIC-M83-8P VIC 1380 fabric interconnect was generating CRC errors on the HIF port . This issue is resolved.	4.1(3b)A	4.1(3d)A
CSCvy11610	A Cisco UCS-managed blade server with a Cisco 2400 Series fabric extender was reporting 2408 IOMs were running with low amounts of memory available. This issue is resolved.	4.0(4g)A	4.1(3d)A
CSCvt94075	On a Cisco UCS blade server with a VIC 6400 series fabric interconnect, IOM discovery failed after chassis decommission/recommission. This issue is resolved.	4.1(200.18)A	4.1(3d)A

Defect ID	Symptom	First Bundle Affected	Resolved in Release

CSCvx07486	On a Cisco UCS B480-M5 blade server, the BMC/CIMC was rebooted after a BMC watchdog reset or kernel panic. The UCS CIMC logs showed the following messages:
	`- [platform_reset_init]:201:Using GPIO Based Platform Reset`
	`- [watchdog_init]:465:BMC Watchdog resetted BMC.`
	`- [watchdog_init]:467:BMC Watchdog System Bus Debug Status Registers: 0x0 and0x0`
	This issue is resolved.
		4.0(4h)B	4.1(3d)B

CSCvw82192	Global Service Profile association on a UCS managed blade server with Cisco 2100 series fabric extender was creating a critical alert on an already associated profile and giving the error `errorDescr="Insufficient space in array`. This issue is resolved.	4.0(1.45)A	4.1(3d)A

CSCvy02844	For firmware upgrade to 4.1(3a) or later, there is a one-time activation required for secure FPGA. The secure FPGA warning message that is currently present may lead users to manually reboot the FI after running these commands. If the FI is manually rebooted during this process it can cause the FI to brick and need to be replaced.
	Current message:
	`Warning: This command will reset Fabric Interconnect and the system will be down till the Fabric Interconnect is reset`
	New message:
	`Warning: This command will upgrade the FPGA and automatically reboot. Please don't reload or power-cycle during the upgrade. The system will reboot after upgrade is complete.`
	New behavior:
	Given the potential impact, the "reboot" command will be locked from local-mgmt context while this process has been committed.
		4.1(3a)A	4.1(3d)A

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCvx80747	On four identical Cisco UCS-FI-6332-16UP-U fabric interconnects with no errors on the GUI, one fabric interconnect always returned integer four to SNMP: `nmpwalk -v 1 -c public <FI IP> 1.3.6.1.3.94.1.6.1.6` This issue is resolved.	4.0(4i)A	4.1(3d)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. This issue is resolved.	4.0(4b)A	4.1(3d)A
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. This issue is resolved.	4.0(2b)A	4.1(3d)A
CSCvx51724	On a Cisco UCS BX210c-M6 server, the BMC rebooted with the message: `BMC Watchdog resetted BMC due to OOM`. This issue is resolved.	4.1(3b)B	4.1(3d)B
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. This issue is resolved.	4.1(2b)A	4.1(3d)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`. This issue is resolved.	4.0(4e)A	4.1(3d)A

Resolved Caveats in Release 4.1(3c)

The following caveats are resolved in Release 4.1(3c):

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCvu16747	Constant interface flapping occurred on a Cisco UCS 6454 Fabric Interconnect connected to an upstream catalyst 4500-x while using LACP port channel with SFP-H10GB-ACU7M. This issue is resolved.	4.1(1)A	4.1(3c)A
CSCvw79335	SNMP timeouts occurred when polling `dot1dTpPortTable` on a Cisco UCS 6332 Fabric Interconnect. This issue is resolved.	4.0(4e)A	4.1(3c)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. `[12679086.760577] [sap 28][pid 15470][comm:snmpd] WARNING: possible memory leak is detected on pers queue (len=729,bytes=208265168) - kernel` This issue is resolved.	4.0(4i)A	4.1(3c)A
CSCvx02918	If a faulty disk was present on a UCS-managed server attached to a 6400 Series Fabric Interconnect, the DME process failed while attempting to apply a storage policy, due to a disk zoning error. This issue is resolved.	4.1(1e)A	4.1(3c)A
CSCvx33064	After upgrading a 6454 Fabric Interconnect to Cisco UCS Manager release 4.1(3b), local login fails if LDAP was configured as Native Authentication This issue is resolved.	4.1(3b)A	4.1(3c)A
CSCvx15159	After the Firmware Upgrade of Cisco UCS 6300 Series Fabric Interconnect clusters from Cisco UCS Manager Release 3.2(2d) to Release 4.0(4h) or 4.1(2b), the following issues are faced on some domains: • The SNMP Collection Object gets timed out • SNMPwalk takes longer time for query This issue is resolved.	4.0(4h)B	4.1(3c)B

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCvx18169	On Cisco UCS 6248UP Fabric Interconnect, the fans were not detected by the switch though the fans were operating. This condition triggered alarms on the fan health status (Fan failure or Fan removed) and further resulted in switch shutdown. This issue is resolved.	3.2(3o)A	4.1(3c)A
CSCvx60544	On Cisco UCS IOM 2408, the B200 M5 server nodes failed to parse the MPLS and incorrectly alter the `dot1q` tag from the MPLS encapsulated PDUs. This issue is resolved.	4.0(4h)A	4.1(3c)A

Resolved Caveats in Release 4.1(3b)

The following caveats are resolved in Release 4.1(3b):

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCvx11527	During the upgrade of the infrastructure software bundle to the release 4.1(3a) for the first time, both the IOMs rebooted to update its BIOS without waiting for the user acknowledgment. This reboot affected the domain setups where UCS 5108 chassis with 2408 I/O Modules (IOM) is connected to UCS 6454 or UCS 64108 Fabric Interconnects resulting a complete loss of storage and network connectivity. This issue is resolved.	4.1(3a)	4.1(3b)
CSCvw49192	After upgrading to Cisco UCS Manager release 4.1(2b), some system configurations may be unable to perform power characterization resulting in a POST failure. System freezes at Loading PTU driver screen. CATERR is also logged in the SEL. This issue is now resolved.	4.1(2b)	4.1(2c) and 4.1(3b)

Resolved Caveats in Release 4.1(3a)

The following caveats are resolved in Release 4.1(3a):

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCvu24563	On Cisco UCS B460 M4 server, the health of the link between VIC 1240 and IOM HIF port going through the port expander card becomes poor which results in CRC errors and packet drops. This condition is seen in the UCS B460 M4 server with VIC 1240 in the MLOM slot and UCSB-MLOM-PT-01 in the Mezzanine slot with IOM 2204/2208. This issue is resolved.	3.1(2b)B, 3.2(3g)B	4.1(3a)B
CSCvu87940	After importing a VNIC config file on a standalone C-series VIC adapter, when the host was rebooted, VNICs did not receive a link-up, resulting in loss of network to the host OS. This occurred when all of the following conditions are met: • The user imported a VNIC configuration file that was exported when VIC was configured with **VNTAG** mode enabled. • VIC network ports are connected to Cisco Nexus switches supporting network interface virtualization. • The switch ports and/or portchannel are configured with switchport mode vntag. This issue is resolved.	4.0(4h)C	4.1(3a)C
CSCvw89416	During OS runtime, an unexpected power-off event comes from NMPowerManager. This issue is resolved.	4.1(2b)B	4.1(3a)B
CSCvv71216	In the Cisco UCS server, whenever the FlexFlash controller is reset, the operating mode of the SD card is switched between 3.3 V signaling (during initialization) and 1.8 V signaling (for data transfers). This condition results in the disappearance of SD card to OS. Thereby, resulting in OS crash. This issue is resolved.	4.0(1d)	4.1(3a)
CSCvu95889	In response to the read error on the SD cards of UCS servers, the FlexFlash controller re-initializes the SD cards. The re-initialization of the SD cards may be stuck or encounter errors. This issue is resolved.	4.0(4e)B	4.1(3a)B

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCvs06864	BSOD was seen on Win2019/Win2016 installation on fNIC SAN LUN with a service profile configured with 2 or more vHBAs on a VIC 14xx series adapter.	4.0(4a)A	4.1(3a)A
CSCvw47746	On a Blade server attached to a 2400 Series Fabric Extender running NXOS, chassis technical support triggered generation of IOM satctrl core.	4.1(2b)A	4.1(3a)A

Resolved Caveats in Release 4.1(2c)

The following caveats are resolved in Release 4.1(2c):

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCvv55541	On reboot of a UCS-Managed C240 M4 rack server, the server entered into the Bitlock Recovery screen. This issue is now resolved.	4.0(4b)C	4.1(2c)C
CSCvu79969	A Cisco UCS B200 M4 server running ESXi 6.5 experienced a `P2_TEMP_SENS` alarm. This issue is resolved.	4.0(4f)B	4.1(2c)B
CSCvv89724	When creating an appliance port-channel in Access mode on on a Cisco UCS 6400 Series Fabric Interconnect, the **borderDeployFSM** operation failed. This issue is resolved.	4.0(1a)A	4.1(2c)A
CSCvu87940	After importing a VNIC config file on a standalone C-series VIC adapter, when the host was rebooted, VNICs did not receive a link-up, resulting in loss of network to the host OS. This occurred when all of the following conditions are met: • The user imported a VNIC configuration file that was exported when VIC was configured with **VNTAG** mode enabled. • VIC network ports are connected to Cisco Nexus switches supporting network interface virtualization. • The switch ports and/or portchannel are configured with switchport mode vntag. This issue is resolved.	4.0(4h)C	4.1(2c)C

Defect ID	Symptom	First Bundle Affected	Resolved in Release
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. This issue is resolved.	4.1(1e)A	4.1(2c)A
CSCvw54180	Cisco UCS 6454 Fabric Interconnects reboot sequentially due to a `policyelem` failure.. This issue is resolved.	4.1(2b)A	4.1(2c)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. This issue is resolved.	4.0(1a)A	4.1(2c)A
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. This issue is resolved.	4,1(2,21)A	4.1(2c)A
CSCvw01292	A Cisco UCS 6400 Series fabric interconnect rebooted during upgrade and displayed the message `lldp hap reset`. This issue is resolved.	4.1(1c)A	4.1(2c)A
CSCvw89416	An unexpected power-off event occurred on a Cisco UCS M5 server. This issue is resolved.	4.0(4a)B and C	4.1(2c)B and C
CSCvv32315	On a Cisco UCS 6454 Fabric Interconnect, on initial boot or after an erase configuration, the fabric interconnect did not boot to the initial configuration prompt. The after finishing booting, the fabric interconnect showed a login prompt with the default hostname of `switch`. This issue is resolved.	4.0(4a)A	4.1(2c)A
CSCvw06021	SecureBoot Variables db/dbx on Cisco M4 EX servers were not always updated. This issue is resolved.	4.2(0.17)B??	4.1(2c)

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCvu16747	Constant interface flapping occurred on a Cisco UCS 6454 Fabric Interconnect connected to an upstream catalyst 4500-x while using LACP port channel with SFP-H10GB-ACU7M. This issue is resolved.	4.1(1)A	4.1(2c)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`. This issue is resolved.	4.0(4h)A	4.1(2c)A
CSCvw79335	SNMP timeouts occurred when polling `dot1dTpPortTable` on a Cisco UCS 6332 Fabric Interconnect. This issue is resolved.	4.0(4e)A	4.1(2c)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. `[12679086.760577] [sap 28][pid 15470][comm:snmpd] WARNING: possible memory leak is detected on pers queue (len=729,bytes=208265168) - kernel` This issue is resolved.	4.0(4i)A	4.1(2c)A
CSCvx02918	If a faulty disk was present on a UCS-managed server attached to a 6400 Series Fabric Interconnect, the DME process failed while attempting to apply a storage policy, due to a disk zoning error.	4.1(1e)A	4.1(2c)
CSCvw24269	UCS Manager was unable to download and extract an A-bundle with a size larger than 2G.	4.1(2b)	4.1(2c)
CSCvw49192	After upgrading to Cisco UCS Manager release 4.1(2b), some system configurations may be unable to perform power characterization resulting in a POST failure. System freezes at Loading PTU driver screen. CATERR is also logged in the SEL. This issue is now resolved.	4.1(2b)	4.1(2c) and 4.1(3b)

Resolved Caveats in Release 4.1(2b)

The following caveats are resolved in Release 4.1(2b):

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCvu59607	The login failure due to entry of wrong password for a valid user name, is captured in the audit logs of Cisco UCS Manager and remote syslog server.	4.0(4i)A	4.1(2b)A
CSCvv69160	On Cisco UCS B260 M4 and B460 M4 Blade servers, the upper non recoverable (UNR) threshold and upper critical (UC) threshold values of the P0V9_SAS sensor are updated as follows: • UC=1.022 • UNR=1.045	4.1(1a)B	4.1(2b)B
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. This issue is resolved.	4.1(1a)A	4.1(2b)A
CSCvv73735	Cisco UCS 6454 Fabric Interconnects are rebooted one at a time, due to the policyelem process crash. This issue is resolved.	4.1(1c)A	4.1(2b)A
CSCvv80576	After vNIC fabric failover, if there is no continuous traffic from vNIC source, the traffic is not switched over to the second fabric interconnect (FI). This condition resulted in traffic drop. This issue is resolved.	4.1(2a)A	4.1(2b)A
CSCvv89399	Fabric Login (FLOGI) can be dropped by fabric interconnect (FI) in the end host mode, with the reason as `Nested NPV connectivity is not supported`, when using certain combinations of PWWN and NWWN. This issue is resolved.	4.0(4i)B	4.1(2b)B

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCvv89810	Some or all the host vHBAs may not communicate with the SAN and the access to fibre channel storage may be lost with Fabric Login (FLOGI) failure in the following conditions: • Cisco UCS 6400 Fabric Interconnects with hosts configured for FC/FCoE connectivity using vHBAs. • WWxN pool is configured with prefix where third octet is non-zero. This issue is resolved.	4.1(1a)A	4.1(2b)A
CSCvv80576	After vNIC failover, the traffic does not switch to the other fabric interconnect. This issue is resolved.	4.1(2a)A	4.1(2b)A

Resolved Caveats in Release 4.1(2a)

The following caveats are resolved in Release 4.1(2a):

Defect ID	Symptom	First Bundle Affected	Resolved in Release
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 remain in the administratively down state with incomplete configuration. Hence, Cisco UCS S3260 Storage Server cannot be discovered. This issue is now resolved.	4.0(4g)A	4.1(1e)A, 4.1(2a)A
CSCvh30116	When a hot plug drive is replaced due to RAID 0 drive failure, the virtual drive is re-initialized automatically to bring back the failed RAID 0 online.	3.1(2b)A	4.1(2a)A

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCvj91628	LSI Logic MegaRAID SAS 9271-8i controller fails with the following errors: `T9: EVT#258908-06/04/18 3:49:08: 15=Fatal firmware error: Driver detected possible FW hang, halting FW. T9: EVT#258909-06/04/18 3:49:08: 15=Fatal firmware error: Line 1307 in ../../raid/1078dma.c T9: EVT#258910-06/04/18 3:49:08: 15=Fatal firmware error: Line 1307 in ../../raid/1078dma.c` Any filesystems on the RAID controller goes offline or be disconnected. This issue is now resolved.	3.2(3l)	4.1(2a)
CSCvr95393	A TACACS user is able to login to the Fabric Interconnect even when the NOLOGIN policy has been set.	4.0(1a)A	4.1(2a)A
CSCvt73487	Cisco UCS C480 M5 servers may stop responding at BIOS POST with the following SEL: `System Software event: Post sensor, System Firmware error (POST Error), No video adapter present/enabled [0x9263] was asserted` This issue is now resolved.	4.0(4h)	4.1(2a)
CSCvr70569	When updating the firmware on Cisco UCS S3260 Storage Server with DDRAID controller, using the Non-Interactive host update utility (NIHUU) tool, the drive firmware update is skipped. This issue is now resolved.	4.1(1)	4.1(2a)
CSCvr79299	The link between Cisco UCS 6400 Series Fabric Interconnect and VIC 1400 or Cisco UCS 2400 IOM adapters, with the SFP-10/25G-LR-S transceiver may go down when the UCS 6400 Series FI interface does not have "fec rs-fec" in the configuration and the type of transceiver is not displayed in Cisco UCS Manager. This issue is now resolved.	4.1(1)A	4.1(2a)A
CSCvs57940	When a non-RoCE vNIC is added to a server configured with two RoCE vNICs, Cisco UCS Manager displays the configuration failure message. This issue is now resolved.	4.1(1a)B	4.1(2a)B

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCvt63740	vMedia policy mapping fails when using HTTPS protocol without specifying username and password. This condition is seen when: • One or more mapping information is missing or invalid • Same device type exists more than once • Image file extension and device type mismatches in vMedia policy This issue is resolved.	3.1(3l)C, 4.0(4b)C	4.1(2a)C
CSCvt63778	On Cisco UCS C220 M5 Rack Server, the power capping setting is failed when configuring a service profile. This issue is resolved.	4.0(1a)B	4.1(2a)B
CSCvu33503	On triggering pending reboot in vNIC with VMQ policy, the VLAN configuration is changed to vNIC in service profile. This issue is resolved.	4.0(4h)A	4.1(2a)A
CSCvu52479	Cisco UCS 6454 Fabric Interconnect is rebooted due to nbproxy process crash. Thereby, resulting in loss of all the SAN and LAN traffic to the directly attached rack servers and blade servers. This issue is resolved.	4.0(4e)A	4.1(2a)A
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	4.1(2a)A

Resolved Caveats in Release 4.1(1e)

The following caveats are resolved in Release 4.1(1e):

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. This issue is resolved.	4.0(4h)	4.1(1e)

Defect ID	Symptom	First Bundle Affected	Resolved in Release
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 Fiber Channel port. This issue is resolved.	3.2(3g)A, 3.2(3j)A	4.1(1e)A
CSCvu25233	Link-flapping or link-down occurs on some ports of 6400 series Fabric Interconnet connected to VIC 1455/1457 using SFP-H25G-CU3M or SFP-H25G-CU5M and on VIC 1455/1457 connected to 2232PP using SFP-10GB-CUxM cable. This issue is resolved.	4.0(1a)A	4.1(1e)A
CSCvu03323	When Cisco IMC or VIC 1385/1387 adapter is rebooted due to firmware update or reset from Cisco UCS Manager Web UI or CLI, the following issue may occur: • In a C-series server managed by Cisco UCS Manager with Cisco VIC 1385/1387 adapter as a management adapter, firmware update of the server components may fail occasionally. This issue is resolved.	4.0(4g)A	4.1(1e)A
CSCvu10837	Discovery of Cisco UCS C240 M5 rack server integrated with Cisco UCS Manager, fails and gets stuck at 0% of FSM with the following error messages: • `lBits is 0#lBits is 0#ERROR: Error adding TLV` • As per the PortAG logs: `Error getting chassis inventory, details: ERROR: Error adding TLV` • As per the rsdAG logs, though the UCS C240 M5 server gets the DHCP address from Cisco UCS Manager, the server discovery fails with the error: `~ 100 - Rack server fails discovery with "Error adding TLV" message` This issue is resolved.	4.0(4g)A	4.1(1e)A
CSCvu25519	During server scale up, the rack server discovery may get stuck due to duplicate entries in chassis inventory. This issue is resolved.	4.0(4g)A	4.1(1e)A

Resolved Caveats in Release 4.1(1d)

The following caveats are resolved in Release 4.1(1d):

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCvq53066	During auto-upgrade of firmware from Cisco UCS Manager 4.0(2d) or earlier releases to Cisco UCS Manager 4.0(4b) or later releases, the SAS controller firmware is not activated on an integrated rack server. This issue is resolved.	4.0(4b)A and C	4.1(1d)A and C
CSCvt27869	In rare situations, on UCS 6200 Series Fabric Interconnect, the data sent from IOM are corrupted due to the corrupted parameter going out of bounds. This issue is resolved.	2.2(8)A	4.1(1d)A
CSCvs97236	On detecting an uncorrectable ECC error, the CPU Integrated Memory Controller (iMC) patrol scrubber logs a truncated system address (4KB page boundary) to the machine check banks. Cisco UCS C460 M4 Rack Server translates the truncated memory address to a physical DIMM address. Depending on system population and configuration, the system event log (SEL) message logging the uncorrectable ECC error may point to a wrong DIMM. This issue is resolved.	4.0(4g)B, 4.1(1c)B	4.1(1d)B
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. This issue is resolved.	4.0(4b)A	4.1(1d)A
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. This issue is resolved.	4.0(4g)A, 4.1(1a)A	4.1(1d)A

Defect ID	Symptom	First Bundle Affected	Resolved in Release
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. This issue is resolved.	4.0(2a)A	4.1(1d)A
CSCvt44506	Cisco UCS Manager receives multiple delta events for Graphics Processing Units (GPU) card. This issue is resolved.	4.0(4h)C	4.1(1d)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. 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	4.1(1d)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. For more information, see: • Intel® Xeon® Processor Scalable FamilySpecification Update (Errata > SKX108) • Second Generation Intel® Xeon® Scalable Processors Specification Update(Errata > CLX37)	4.0(4h)C	4.1(1d)C
CSCvu14656	On upgrade of BIOS to one of the following versions, the booting of M5 servers get stuck at the memory testing step: • C220M5.4.1.1c.0.0404202345 • C240M5.4.1.1c.0.0405200025 • B200M5.4.1.1c.0.0404202345 • B480M5.4.1.1c.0.0405200025 • S3X60M5.4.1.1c.0.0405200025	4.1(1c)C	4.1(1d)C

Defect ID	Symptom	First Bundle Affected	Resolved in Release
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: • C220M5.4.1.1c.0.0404202345 • C240M5.4.1.1c.0.0405200025 • B200M5.4.1.1c.0.0404202345 • B480M5.4.1.1c.0.0405200025 • S3X60M5.4.1.1c.0.0405200025	4.1(1c)B and C	4.1(1d)B and C

Resolved Caveats in Release 4.1(1c)

The following caveats are resolved in Release 4.1(1c):

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCvr79388	Cisco UCS servers stop responding and reboot after ADDDC virtual lockstep is activated. This results in #IERR and M2M timeout in the memory system. This issue is resolved.	4.0(4e)B	4.1(1c)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. This issue is resolved.	4.0(4e)B	4.1(1c)B
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. This issue is resolved.	4.0(1a)A	4.1(1c)A
CSCvs40873	FDMI rejection messages are generated when Fibre Channel HBA storage array attempts to register with the FDMI service on Cisco 6454 Fabric Interconnect, as the FDMI service is not enabled on Fabric Interconnect. FDMI service is now enabled.	4.0(4g)A	4.1(1c)A

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCvt48568	On Cisco UCS M5 Servers, soft UUID configured through Service Profile gets reset to hardware based UUID. This issue is resolved.	4.1(1a)C	4.1(1c)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. This issue is resolved.	4.0(4e)A	4.1(1c)A
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. The PIDs of affected SSDs are: • (400GB) UCS-SD400G1KHY-EP, UCS-SD400G12S4-EP, UCS-C3X60-12G240 • (1.6TB) UCS-SD16TG1KHY-EP, UCS-SD16TB12S4-EP, UCS-C3X60-12G2160 This issue is resolved.	3.2(1d)C	4.1(1c)C

Resolved Caveats in Release 4.1(1b)

The following caveats are resolved in Release 4.1(1b):

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCvt23481	After upgrading Cisco UCS C220 M5 or C125 M5 servers, which are equipped with a RAID controller to release 4.1(1a), **Thermal Threshold** drops to zero. As a result, the fans start running at maximum speed.	4.1(1a)C	4.1(1b)C

Resolved Caveats in Release 4.1(1a)

The following caveats are resolved in Release 4.1(1a):

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCvr98210	When upgrading from Cisco UCS Manager Release 3.2 to Release 4.0 or later releases 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.	4.0(1a)A	4.1(1a)A
CSCvr91399	The following BIOS tokens are reset to Platform Default when they are pushed from Cisco UCS Central to UCS Manager. • SelectMemoryRASConfiguration • LocalX2Apic • BMEDMAMitigation	3.2(3)A	4.1(1a)A
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: `Adapter uplink interface x/y/z link state: unavailable. Please verify connectivity to Fabric Interconnect. Acknowledging FEX might be required.`	4.0(2d)A	4.1(1a)A
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 This issue is resolved.	4.0(4a) B	4.0(4c)B and 4.1(1a)
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. This issue is resolved.	4.0(4b)A	4.0(4f)A and 4.1(1a)A
CSCvr47266	UCS 2208 IOMs will not come online after migration from a UCS 6248 Fabric Interconnect to a UCS 6454 Fabric Interconnect, if the burst size in QoS policy is set to invalid range (0-511) for UCS 6454 Fabric Interconnect. This issue is resolved.	4.0(4b)A	4.0(4f)A and 4.1(1a)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. This issue is resolved.	4.0(4e)A	4.0(4f)A and 4.1(1a)A
CSCvr78701	Cisco UCS Manager integrated C220 M5 rack servers experienced a Cisco IMC kernel panic during Cisco UCS Manager activation. This issue is resolved.	4.0(4c)C	4.0(4g)C and 4.1(1a)C
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: `mc_attrib_set_suboem_id failed to set the SubOEM ID`	4.0(4b)C	4.1(1a)C
CSCvr23136	On firmware upgrade of UCS C-series server from Cisco UCS Manager Release 4.0(1a) release to Cisco UCS Manager Release 4.0(1b) release, the server discovery fails with the subOEMID failure message or CIMC is unable to detect any drives. The issue is resolved.	4.0(4a)C, 4.0(4c)C, 4.0(4e)C	4.1(1a)C
CSCvs35789	When there is a failover in UCS 6454 Fabric Interconnect, the HIF ports are down causing the traffic to disrupt for more than 40 seconds. Hence, fabric interconnect reboot takes more than 40 secs to regain connectivity. This issue is resolved.	4.0(4c)A	4.1(1a)A
CSCvp65587	Call home XML <ch:Series> field value is incorrect for 6400 series Fabric Interconnects. This issue is resolved.	4.0(4a)A	4.1(1a)A
CSCvs41531	Cisco IMC no longer executes the watchdog timeout configured action under the following conditions: **1.** When IPMI restarts for any reason. **2.** If the watchdog set timer command is sent from the host OS within 100ms after IPMI restarts. This issue is resolved.	4.0(2d)	4.1(1a)

Defect ID	Symptom	First Bundle Affected	Resolved in Release
CSCvr74792	UCS 6454 Fabric Interconnect running with Cisco UCS Manager Release 4.0(2d), is rebooted due to kernel panic. This issue is resolved.	4.0(2d)A	4.1(1a)A
CSCvr16359	When UCS Fabric Interconnect in Ethernet switching mode is restored from full state backup, Fabric Interconnect is restored with incorrect Ethernet end-host mode instead of Ethernet switching mode. This issue is resolved.	4.0(4b)A	4.1(1a)A
CSCvp87622	When SNMP is utilized to query Cisco UCS manager running with firmware version 3.2(3g), the system manager service is crashed and the following message is logged. `FI-B %SYSMGR-2-SERVICE_CRASHED: Service "snmpd" (PID #) hasn't caught signal 11 (core will be saved).` This issue is resolved.	3.2(3g)A	4.1(1a)A
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. This issue is resolved.	4.0(4a)A	4.1(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 4.1(3i)

The following caveats are open in Release 4.1(3i):

Defect ID	Symptom	Workaround	First Bundle Affected
CSCvy52458	The system time on Cisco UCS Manager is not in synchronization with the NTP servers. This issue is seen when: • The NTP server configuration is present in Cisco UCS Manager but missing in the NXOS configuration. • The NTP server is configured with domain name.	Remove and re-add the NTP servers to Cisco UCS Manager. If the NTP server is connected to Cisco UCS Central, set Time Zone Management and Communication Services to Local and then remove and re-add the NTP servers.	4.0(4g)A

Open Caveats for Release 4.1(3e)

The following caveats are open in Release 4.1(3e):

Defect ID	Symptom	Workaround	First Bundle Affected
CSCvy90962	In situations during downgrade of Cisco UCS Manager from 4.2(x) to 4.1(3x) or earlier releases, Cisco UCS manager gets downgraded to 4.1(3x) or earlier release. And, if for some reason Fabric Interconnect reboot happens even before Fabric Interconnect gets downgraded to 4.1(3x) or earlier releases, the Fabric Interconnect gets stuck in 4.2(x). This situation results in failure of user login and high availability (HA) will also be down.	When Cisco UCS Manager comes up after downgrade, the user can login through CLI and recover the setup through CLI.	4.1(3c)

Open Caveats for Release 4.1(3d)

The following caveats are open in Release 4.1(3d):

Defect ID	Symptom	Workaround	First Bundle Affected

CSCvv57606	When installing a Cisco UCS M5 server connected to a Cisco 6400 Series Fabric Interconnect and 2408 IOM for the first time, the service profile could fail association and show a `Connection Placement Error` message. The UCS Manager did not create a path for both the A and B fabrics.
	Run this command from UCSM CLI to confirm symptoms:
	`UCS-FI-A# show server status detail`
	`Working:`
	`Server 2/4:`
	`  Slot Status: Equipped`
	`  Equipped Conn Path: A,B`
	`  Equipped Conn Status: A,B`
	`Problem:`
	`Server 2/5:`
	`  Slot Status: Equipped`
	`  Equipped Conn Path: A`
	`<<<<<`
	`  Equipped Conn Status: A`
		Re-acknowledge the IOM on the missing to re-establish connectivity and associate the service profile.	4.0(4e)A

Open Caveats for Release 4.1(3b)

The following caveats are open in Release 4.1(3b):

Defect ID	Symptom	Workaround	First Bundle Affected
CSCvx33064	After upgrading a 6454 Fabric Interconnect to Cisco UCS Manager release 4.1(3b), local login fails if LDAP was configured as Native Authenication	1. After upgrading to Cisco UCS Manager release 4.1(3b), set the Native Authentication domain to an unused realm like Radius and save: **Admin** > **User Management** > **Authentication** > **Native Authentication** > **Realm** Radius > **Save** 2. Set the Native Authentication domain to **Local** and save. 3. Configure Authentication Domain for LDAP: **Admin** > **User Management** > **Authentication** > Authentication Domains Local should now work and LDAP will also work when the domain is chosen from the drop down list.	4.1(3b)A
CSCvx23029	Cisco UCS Manager Authentication Domain with a period, hyphen, and underscore causes Update Realm failures post upgrade to 4.1(3b) code	Revert Authentication to **Local**, delete the Authentication Domain, create a new Authentication Domain avoiding a period (see example for "LDAP" in CSCvx33064), and then set to the Remote Access of choice.	4.1(3b)A

Open Caveats for Release 4.1(3a)

The following caveats are open in Release 4.1(3a):

Defect ID	Symptom	Workaround	First Bundle Affected
CSCvx11527	During the upgrade of the infrastructure software bundle to the release 4.1(3a) for the first time, both the IOMs reboot to update its BIOS without waiting for the user acknowledgment. This reboot affects the domain setups where UCS 5108 chassis with 2408 I/O Modules (IOM) is connected to UCS 6454 or UCS 64108 Fabric Interconnects resulting a complete loss of storage and network connectivity.	The UCSM 4.1(3a) release has been deferred. If the IOM 2408 has already been upgraded to 4.1(3a) release, then that IOM has already received the updated BIOS and will not incur further reboots. For more information, see the deferral notice.	4.1(3a)
CSCvv64331	In a Rack-Mount server-only environment, due to multiple host entries in the DHCP leases or unavailability of DHCP leases, the server discovery and high availability fail.	Contact TAC to load the debug plugin on the Fabric Interconnect to restart the DHCP process and clear the DHCP leases. After the restart, DHCP re-assigns the IP addresses. Hence, server discovery will be successful.	2.5(1.1)
CSCvw76890	The delete operation triggered by a user from the Cisco UCS Manager GUI, will delete the cores. But, in case, if it is the switch core, the deleted switch core is restored after few seconds. The above issue is seen as the switch cores are available under both Cisco UCS Manager and Switch sides. The cores are restored from switch if it is not available under Cisco UCS Manager directory, as part of core monitoring.	Contact TAC to get the required core removed when there are space constraints.	4.1(3a)A
CSCvu90488	During Infrastructure upgrade of Cisco UCS 6400 Series Fabric Interconnects, the upgrade fails and retries multiple times continuously.	Restart Data Management Engine (DME) and reboot Fabric Interconnect to recover the setup.	4.1(2)A
CSCvv57606	On installing a M5 server in a chassis for the first time, a service profile may fail and throw the connection placement error. This issue is seen as the path is not being established for the adapter on Fabric Interconnect A and Fabric Interconnect B.	Re-acknowledge IOM on path that is missing to re-establish connectivity and associate the service profile.	4.0(4e)A

Defect ID	Symptom	Workaround	First Bundle Affected
CSCvw58884	On applying Host Firmware Pack (HFP) of version 4.1(1d) from Cisco UCS Central, the multiple local-disk and storage-controller faults are reported on the UCS Manager Domains. These faults have occurred as the B-Series and C-Series bundles firmware package exists on the UCS Manager domain even after deleting the images post the service profile update.	Upload the same B-Series and C-Series bundles firmware package to the Cisco UCS Manager domain to clear the local-disk and storage-controller faults.	4.1(1c)A
CSCvv87212	After decommission and recommission of the Cisco UCSC-C240-M5SN server, the server gets discovered successfully. But, Cisco UCS Manager GUI and CLI show only B as the Conn Path and Conn Status instead of A and B for the server.	Re-acknowledge the affected server or decommission and recommission the affected server.	4.1(2a)A
CSCvw87665	During upgrade of Cisco UCS S3260 Storage Server from Cisco UCS Manager Release 4.0(4k)C release to Cisco UCS Manager Release 4.1(3)C release, the chassis profile association may get stuck with the following message: • `waiting for board controller activation to complete(FSM-STAGE:sam:dme:EquipmentChassisAssociate:RollBrdCtlrActivation`	There is no known workaround.	4.0(4k)C

CSCvv15754	On the Cisco UCS domain running with a high capacity of servers (100+) and chassis, you might get a timeout error when you update VLANs for a UCS vNIC template with more number of VLANs (150+) through Cisco UCS Manager GUI.	VLANs can be added through the CLI of Cisco UCS Manager, using the following commands:
		`UCSM /org # scope org sub-org`
		`UCSM /org # scope vnic-templ templ_name`
		`UCSM /org/vnic-templ # create eth-if VLAN_name`
		`UCSM /org/vnic-templ/eth-if* # commit-buffer`
			4.0(4c)A

Defect ID	Symptom	Workaround	First Bundle Affected
CSCvw91528	After decommission and recommission of a chassis, the Power Save Policy Mode of the chassis is disabled.	If you have already enabled the power save mode before recommission, you have to manually enable the power save mode again after recommission of chassis. To enable the Power Save Policy mode, perform the following: **1.** Log in to Cisco UCS Manager GUI **2.** Navigate to **Equipment** > **Policies** > **Global Policies**. **3.** In the **Power Save Policy Mode** field, click **Disable** and then click **Enable**.	4.1(3)A
CSCvw93034	On the 6300 Series Fabric Interconnect with Micron M500IT SSD running a firmware version different from MC03.00 or MU05.00, the SSD will become unresponsive after approximately 28224 (or ~3.2 years) of accumulated Power-On-Hours. This will cause file system operations on the Fabric Interconnect to fail, and could even trigger a reboot of the Fabric Interconnect. A power cycle of the Fabric Interconnect restores normal operation of the SSD, which then will continue to operate normally for 1008 Power-On-Hours (or ~1.5 months) before the same condition will be hit again. This cycle will continue to repeat for each additional ~1.5 months of accumulated Power-On-Hours unless the firmware of the SSD is updated to resolve this behavior.	Open a TAC case; TAC can perform the firmware upgrade for the SSD manually without requiring a Fabric Interconnect reboot.	4.1(2b)A

Defect ID	Symptom	Workaround	First Bundle Affected
CSCvw31796	During discovery of a new server, the pre-existing LUNs under NV and/or Persistent Memory, are not scrubbed even if a global scrub policy is in place.	During discovery of a new server, the pre-existing LUNs under NV and/or Persistent Memory, are not scrubbed even if a global scrub policy is in place. Associate the server with a service profile and add a scrub policy(with persistent memory/disks) to this service profile. Disassociation will cause the Persistent Memory and LUNs to be cleared. This is recommended only on trusted servers.	4.1(2.55)C
CSCvw57512	Disk scrub fails for PCH and UCS-M2-HWRAID contollers during factory reset of M5 Servers.	Attaching a scrub policy in a service profile and dis-associating will scrub the disks.	4.1(2.74)C

Defect ID	Symptom	Workaround	First Bundle Affected

CSCvy46626	When upgrading to UCSM 4.1.3 firmware, you may see the following faults for the primary fabric interconnect, once the UCS Manager and subordinate fabric interconnect have been successfully upgraded to 4.1.3 while the primary fabric interconnect is still on old firmware version.
	`sys/switch-X/oui-pool-default`
	`[FSM:FAILED]: Deploy OUI to Fabric-Interconnect(FSM-STAGE:sam:dme:FcpoolOuiDeploy). Remote-Invocation-Error: SCI_GetAllOUIEntries API is not supported in running Switch Version`
	`[FSM:STAGE:FAILED]: Deploy OUI to Local Fabric-Interconnect(FSM-STAGE:sam:dme:FcpoolOuiDeploy:Local)`
	`[FSM:STAGE:REMOTE-ERROR]: Result: resource-unavailable Code: unspecified Message: SCI_GetAllOUIEntries API is not supported in running Switch Version(sam:dme:FcpoolOuiDeploy:Local)`
		Acknowledge the reboot of the primary fabric interconnect and allow the upgrade to proceed and complete on the primary fabric interconnect. Once the upgrade is complete, the faults will clear.	4.1(3a)A

Open Caveats for Release 4.1(2b)

The following caveats are open in Release 4.1(2b):

Defect ID	Symptom	Workaround	First Bundle Affected
CSCvw49192	After upgrading to Cisco UCS Manager release 4.1(2b), some system configurations may be unable to perform power characterization. Hence, resulting in a POST failure (hang at loading PTU driver) and erroneous DIMM errors.	After upgrading to Cisco UCS Manager release 4.1(2b), apply or update the BIOS policy with the **MemoryRefreshRate** token set to **1x Refresh**. Then, reboot the server to apply the BIOS policy.	4.1(2b)C

Defect ID	Symptom	Workaround	First Bundle Affected
CSCvs72258	After changing the Best Effort weight or MTU value in the QOS configuration on Cisco UCS 6332 Fabric Interconnect of Cisco UCS Manager, an unexpected extended storage traffic disruption may be experienced.	There is no known workaround.	4.0(4c)A

Open Caveats for Release 4.1(2a)

The following caveats are open in Release 4.1(2a):

Defect ID	Symptom	Workaround	First Bundle Affected
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
CSCvs72258	After changing the Best Effort weight or MTU value in the QOS configuration on Cisco UCS 6332 Fabric Interconnect of Cisco UCS Manager, an unexpected extended storage traffic disruption may be experienced.	There is no known workaround.	4.0(4c)A
CSCvq73225	When a journaling drive attached to a volume is removed, I/O activity may stop in the other volumes on the servers running on Windows operating system.	Use partial parity log.	4.1(1c)

Defect ID	Symptom	Workaround	First Bundle Affected
CSCvu24563	On Cisco UCS B460 M4 server, the health of the link between VIC 1240 and IOM HIF port going through the port expander card become poor resulting in CRC errors and packet drops. This condition is seen in UCS B460 M4 server with VIC 1240 in the MLOM slot and UCSB-MLOM-PT-01 in the Mezzanine slot with IOM 2204/2208.	Remove UCSB-MLOM-PT-01 from the Mezzanine slot. In this case, VIC 1240 will have only 2x10G connection port-channel with 2208 IOM and 1x10G connection with 2204 IOM. VIC 1240 will not have 4x10G connection with 2208 and 2x10G connection with 2204 IOM. Thereby, reducing the overall bandwidth from the impacted VIC 1240 adapter. To provide additional bandwidth, install VIC 1280 adapter in the second Mezzanine slot and re-associate or redeploy the service profile to distribute some of the vNICs to VIC 1280 adapter.	3.1(2b)B, 3.2(3g)B
CSCvp35008	SLES/RHEL OS installation in UEFI mode fails on Cisco UCS C-Series M5 servers when they are equipped with Intel Xx710 adapters, and one or more of these adapters has the Option ROM enabled.	Disable the Option ROMs for all Intel adapters, including LOM, in the server.	4.0(4b)

Defect ID	Symptom	Workaround	First Bundle Affected

CSCvu31747	Local disk configured using Cisco 12G Modular RAID controller with 2GB cache (UCSC-RAID-M5), or Cisco 12G Modular RAID controller with 2GB cache UCSC-SAS9460-8i (UCSC-SAS9460-8i), or Cisco 12G Modular SAS HBA max 16 drives (UCSC-SAS-M5) is not discovered during the installation of Citrix XEN 7.1 Hypervisor on Cisco UCS M5 servers.	Perform the following steps:
		1. During the installation of Citrix XEN 7.1 Hypervisor, press **F9** and load the megaraid_sas driver.
		2. Once the driver is loaded, press **Ctrl + Alt + F1** to enter to Linux shell and execute the following command
		• For RAID Controller
		`modprobe megaraid_sas`
		• For SAS HBA
		`modprobe mpt3sas`
		3. Ensure that the module is loaded successfully. Execute the following command to verify:
		• For RAID Controllers
		`lsmod | grep megaraid_sas`
		• For SAS HBA
		`lsmod | grep mpt3sas`
		4. Press **Ctrl + Alt + F2** to switch back to Citrix XEN 7.1 Hypervisor installer, and proceed with the OS installation.
		5. Once the OS installation is complete, provide the MegaRAID or mpt3sas DUD as a supplementary package.
			4.1(2a)

Open Caveats for Release 4.1(1d)

The following caveats are open in Release 4.1(1d):

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 and when both the server BIOS and adapter are updated.	Log into Cisco UCS Manager and reset the adapter. If resetting the adapter fails, re-acknowledge the server.	4.1(1b)C
CSCvs06864	During installation of Windows 2019 on Cisco UCS fNIC LUN with service profile configured with 2 or more vHBAs on a Cisco UCS VIC 14xx series adapter, blue screen of death (BSoD) is observed.	On each Cisco UCS VIC 14xx series adapters, limit the number of vHBAs to one during Windows 2019 installation on SAN LUN. Add the remaining vHBAs after installation.	4.0(4a)

Open Caveats for Release 4.1(1c)

The following caveats are open in Release 4.1(1c):

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. For more information, see: • Intel® Xeon® Processor Scalable FamilySpecification Update (Errata > SKX108) • Second Generation Intel® Xeon® Scalable Processors Specification Update(Errata > CLX37)	If the server crashes many times after activating ADDDC virtual lockstep, disable ADDDC. 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(4h)C Resolved in 4.1(1d).

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: • C220M5.4.1.1c.0.0404202345 • C240M5.4.1.1c.0.0405200025 • B200M5.4.1.1c.0.0404202345 • B480M5.4.1.1c.0.0405200025 • S3X60M5.4.1.1c.0.0405200025	To boot the server, perform the following: 1. Revert BIOS to prior working version and boot the system to OS. 2. Review logs to determine DIMMs with correctable or uncorrectable ECC errors and replace or remove faulty DIMMs. 3. Upgrade to BIOS version included in 4.1(1c) bundle and make sure that the system boots as expected.	4.1(1c)C Resolved in 4.1(1d).
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: • C220M5.4.1.1c.0.0404202345 • C240M5.4.1.1c.0.0405200025 • B200M5.4.1.1c.0.0404202345 • B480M5.4.1.1c.0.0405200025 • S3X60M5.4.1.1c.0.0405200025	There is no known workaround.	4.1(1c)B and C

Open Caveats for Release 4.1(1a)

The following caveats are open in Release 4.1(1a):

Defect ID	Symptom	Workaround	First Bundle Affected
CSCvt23481	After upgrading Cisco UCS C220 M5 or C125 M5 servers, which are equipped with a RAID controller to release 4.1(1a), **Thermal Threshold** drops to zero. As a result, the fans start running at maximum speed.	Downgrade Cisco UCS Manager to release 4.0(4g).	4.1(1a)

Defect ID	Symptom	Workaround	First Bundle Affected
CSCvs51433	During an upgrade of the infrastructure bundle of a UCS 6200 Series secondary Fabric Interconnect, the Appliance port channel 2 goes down unexpectedly.	Reconfigure the Appliance port channel 2.	3.2(1d)A
CSCvr95393	A TACACS user is able to login to the Fabric Interconnect even when the NOLOGIN policy has been set.	There is no known workaround.	4.0(1a) A
CSCvr54853	HTML KVM displays unrecognized character error message while pasting special characters like = and >.	There is no known workaround.	4.1(1a)
CSCvs29252	Cisco IMC Scriptable Vmedia does not support `vers` option with NFS and CIFS mount options in Cisco UCS M4 servers.	There is no known workaround.	4.1(1a)
CSCvs34262	In UCS S3260 M5 server, BMC displays that IPMI is enabled even in non-IPMI user mode, and IPMI over LAN communication fails.	There is no known workaround. You can ignore the message because Cisco IMC is set to non-IPMI mode.	4.1(1a)
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
CSCvs72258	After changing the Best Effort weight or MTU value in the QOS configuration on Cisco UCS 6332 Fabric Interconnect of Cisco UCS Manager, an unexpected extended storage traffic disruption may be experienced.	There is no known workaround.	4.0(4c)A

Defect ID	Symptom	Workaround	First Bundle Affected
CSCvs19402	When the Cisco UCS Manager A-bundle software is downgraded from Cisco UCS Manager Release 4.1(1a) to Cisco UCS Manager Release 4.0(x) and B-bundle software is not downgraded from Cisco UCS Manager Release 4.1(1a), the discovery of Cisco UCS M4 Blade Server fails during decommission or recommission of a B-Series blade server and C-Series rack server.	Reset Cisco IMC.	4.0(4o)A
CSCvs07801	After upgrading a Fabric Interconnect using the auto-install option with fabric evacuation mode enabled, link failure faults existed in Cisco UCS Manager which were cleared on the Fabric Interconnect after upgrade. This might be seen in rare conditions with specific combinations of firmware.	There is no known workaround.	4.1(1a)
CSCvs94504	BIOS Parameters (HyperThreading and NUMA Optimized) change are not updated in the Server BIOS even after performing re-acknowledgement of the B-Series servers.	Create a new BIOS policy and apply it to **Service Profile** > **Re-acknowledge server**.	4.0(4c)A
CSCvt09966	On UCS 6454 Fabric Interconnect, local-mgmt commands including reboot are missing from the subordinate Fabric Interconnect.	Reboot can be done from the primary Fabric Interconnect local-mgmt prompt.	4.0(2d)A and 4.0(4o)A

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: • Switch to UEFI boot mode. Or 1. When system is hung, set the LOM Option to disable using the CIMC feature to set the BIOS tokens. 2. Reboot the server to the UEFI shell. 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). 4. On next boot, during BIOS post enter into Intel OPROM Utility(Ctrl +D), enable the ISCSI mode for X550 LOM. Save and restart. 5. LOM ISCSI LUN will boot without any issue.	4.0(4c)C
CSCvo39645	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

Behavior Changes and Known Limitations

Behavior Changes and Known Limitations in Release 4.1(3)

Cisco UCS Manager GUI will not list out VLANs in Navigation pane

Starting with Cisco UCS Manager Release 4.1(3a), Cisco UCS Manager will not display the list of VLANs in the left navigation pane. Still, the list of VLANs can be viewed under the **VLANs** tab in the working pane.

VMD/VROC is not supported

CSCvw22319—VMD/VROC is not supported on Cisco UCS C480 M5 server with NVME drives.

Effect of Faulty DIMM on Cisco UCS C125 M5 Rack Server

CSCvw29423—On connecting a faulty DIMM, Cisco UCS C125 M5 Rack Server Node with AMD EPYC 2 7002 (ROME) processors will not boot. The workaround is to replace the faulty DIMM and then boot the server.

Behavior Changes and Known Limitations in Release 4.1(2)

Behavior Changes and Known Limitations in Release 4.1(2a)

The following caveats are the known limitations in Release 4.1(2a):

Bug ID	Symptom	Workaround	First Affected Release
CSCvu80469	Installation of mpt3sas driver fails after installing i40e drivers on SLES 12.5 OS in Cisco UCS servers equipped with Intel 710 series adapters and pass through HBA controller. Following warning message is displayed: `Updating / installing... 1:lsi-mpt3sas-kmp-default -30.00.01.# [100%]depmod: WARNING: //lib/modules/4.12.14-119-default /kernel/drivers/infiniband/hw /i40iw/i40iw.ko disagrees about version of symbol i40e_unregister_client depmod: WARNING: //lib/modules /4.12.14-119-default/kernel /drivers/infiniband/hw/i40iw /i40iw.ko disagrees about version of symbol i40e_register_client Warning: /lib/modules/4.12.14-119 -default is inconsistent Warning: weak-updates symlinks might not be created`	Perform one of the following: 1. Uninstall i40e driver 2. Change the order of installation. Install mpt3sas driver first and then i40e driver.	4.1(2a)

Bug ID	Symptom	Workaround	First Affected Release
CSCvu06698	Cavium and Qlogic Network and iSCSI driver updates fail on ESXi OS version 7.0 and 6.5U3 with the dependency error. ESXi OS image has inbox Cavium and QLogic Network and iSCSI driver which is incompatible with latest asynchronous drivers packaged as part of driver ISO.	Perform the following steps: **1.** Move the ESXi host to maintenance mode. **2.** Unload the inbox Cavium/QLogic drivers (qedentv/qedrntv/qedil) esxcli software vib remove, hwere vibname=VIB File of Driver **3.** Load the latest driver packaged as part of Driver ISO esxcli software vib install -v <VIB File of driver> **4.** Reboot the ESXi host. **5.** Once the OS boots up, exit the maintenance mode.	4.1(2a)

Behavior Changes and Known Limitations in Release 4.1(1a)

Failure of Secure LDAP after upgrade of UCS Infrastructure to Cisco UCS Manager Release 4.1(1a)

CSCvt31344—Cisco UCS 6200 and 6300 series Fabric Interconnects (FIs): After upgrade of UCS Infrastructure A-bundle to Cisco UCS Manager Release 4.1(1a) from any previous release, the user authentication fails when logging into Cisco UCS Manager through secure LDAP. This behaviour is expected after infrastructure upgrade, as OpenLDAP security has strengthened security for Cisco UCS 6200 and 6300 series FIs.

To ensure successful login to Cisco UCS manager through secure LDAP, do one of the following:

- LDAP server needs a new multiple domain certificate. This new certificate must include all possible names of the LDAP server configured in Cisco UCS manager, like Fully Qualified Domain Name(FQDN), hostname, and IP address in Subject Alternative Name (SAN) extension field of the certificate.
- Obtain the SANs of the current LDAP server certificate using the following command:

  ```
  openssl s_client -connect <LDAP Provider ip/hostname>:636 | openssl x509 -noout -text
  | grep -b1 DNS
  ```

  In Cisco UCS manager, update one of the SANs as the LDAP provider to LDAP group that is being used in the LDAP authentication.

Cisco UCS Manager Shows Complete Reboot Impact for Multiple Users

CSCvp45607—In releases prior to Cisco UCS Manager Release 4.1(1),when you clicked on **Show Current User's Activities** and then on the **Acknowledge All** checkbox, you could reboot all servers that had a pending reboot from all users without understanding the full impact.

Selecting the **Acknowledge All** checkbox in Cisco UCS Manager Release 4.1(1) and later releases automatically deactivates **Show Current User's Activities** to ensure full visibility of the reboot impacts.

Cisco UCS Manager GUI Displays the Correct PSU Order

CSCvq93295—When using UCS 6332-16UP Fabric Interconnect integrated with UCS C240 M5SX servers, there is a mismatch between the power supply unit (PSU) positions displayed by the Cisco UCS Manager GUI and mentioned in the server specification document.

The Cisco UCS Manager GUI displays the power supply unit (PSU) positions incorrectly as:

- PSU 1 — Upper
- PSU 2 — Lower

The server specification sheet displays the correct information:

- PSU 01 — Lower
- PSU 02 — Upper

In Cisco UCS Manager Release 4.1(1) and later releases, the GUI displays the PSU position correctly.

Cisco UCS Manager GUI Displays Chassis Statistics Incorrectly

After a UCS 5108 chassis is powered off, Cisco UCS Manager displays the chassis status as **Inaccessible**. However, all chassis status statistics and chassis PSU statistics are incorrectly either displayed as **OK** or based on previous known statistics.

Algorithm Support in OpenSSH to Log into Servers through the SSH

Starting with Cisco UCS Manager Release 4.1(1c), 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
    - For Cisco Fabric Interconnect 6454
        - diffie-hellman-group-exchange-sha256
        - diffie-hellman-group16-sha512
    - 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

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).

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