Release Notes for Cisco UCS Rack Server Software, Release 4.1(1)

First Published: 2020-02-20

Last Modified: 2020-11-03

Cisco UCS C-Series Servers

Cisco UCS C-Series and S-Series Servers deliver unified computing in an industry-standard form factor to reduce total cost of ownership and increase agility. Each product addresses varying workload challenges through a balance of processing, memory, I/O, and internal storage resources.

About the Release Notes

This document describes the new features, system requirements, open caveats and known behaviors for C-Series and S-Series software release 4.1(1) including Cisco Integrated Management Controller (Cisco IMC) software and any related BIOS, firmware, or drivers. Use this document in conjunction with the documents listed in the Related Documentation, on page 44 section.

Note We sometimes update the documentation after original publication. Therefore, you should also refer to the documentation on Cisco.com for any updates.

Deprecation Notice

Deprecated Release 4.1(1f)

Release 4.1(1f) 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(1g) or later.

Revision History

Revision	Date	Description
F1	November 03, 2020	Added new section - Deprecation Notice

Revision	Date	Description
F0	September 02, 2020	Updated release notes for 4.1(1h). • Updated the Resolved Caveats section. • Updated the Open Caveats section. The firmware files in Cisco Host Upgrade Utility for individual releases are available at: Cisco UCS C-Series Integrated Management Controller Firmware Files, Release 4.1
E1	July 30, 2020	Updated the Known Behaviors and Limitations in Release 4.1(1g) section.
E0	July 10, 2020	Updated release notes for 4.1(1g). • Updated the Resolved Caveats section. • Updated the Open Caveats section. The firmware files in Cisco Host Upgrade Utility for individual releases are available at: Cisco UCS C-Series Integrated Management Controller Firmware Files, Release 4.1
D0	May 21, 2020	Updated release notes for 4.1(1c). • Updated the Open Caveats section.

Revision	Date	Description
C0	April 20, 2020	Created release notes for 4.1(1f). • Updated the Security Fixes section. • Updated the Resolved Caveats section. • Updated the Open Caveats section. The firmware files in Cisco Host Upgrade Utility for individual releases are available at: Cisco UCS C-Series Integrated Management Controller Firmware Files, Release 4.1
B0	March 12, 2020	Created release notes for 4.1(1d). • Updated the Resolved Caveats section. The firmware files in Cisco Host Upgrade Utility for individual releases are available at: Cisco UCS C-Series Integrated Management Controller Firmware Files, Release 4.1
A0	February 20, 2020	Created release notes for 4.1(1c). The firmware files in Cisco Host Upgrade Utility for individual releases are available at: Cisco UCS C-Series Integrated Management Controller Firmware Files, Release 4.1
	March 04, 2020	Updated Open Caveats section for 4.1(1c).

Supported Platforms and Release Compatibility Matrix

Supported Platforms in this Release

The following servers are supported in this release:

- UCS C125 M5
- UCS C220 M5
- UCS C240 M5

- UCS C480 M5
- UCS C480 ML M5
- UCS S3260 M5
- UCS C220 M4
- UCS C240 M4
- UCS C460 M4
- UCS S3260 M4

For information about these servers, see Overview of Servers.

Cisco IMC and Cisco UCS Manager Release Compatibility Matrix

Cisco UCS C-Series and S-Series Rack-Mount Servers are managed by built-in standalone software —Cisco IMC. However, when a Rack-Mount Server is integrated with Cisco UCS Manager, the Cisco IMC does not manage the server anymore.

The following table lists the supported platforms, Cisco IMC releases, and Cisco UCS Manager releases for Rack-Mount Servers:

Table 1: Cisco IMC and UCS Manager Software Releases for Rack Mount Servers for Cisco IMC 4.1(1) Release

Cisco IMC Release	Cisco UCS Manager Release	Rack Mount Servers
4.1(1h)	4.1(1e)	Cisco UCS C220 M5, C240 M5, C480 M5, C480 ML M5, S3260 M5, C125 M5, C220 M4, C240 M4, C460 M4, and S3260 M4 servers
4.1(1g)	4.1(1d)	Cisco UCS C220 M5, C240 M5, C480 M5, C480 ML M5, S3260 M5, C125 M5, C220 M4, C240 M4, C460 M4, and S3260 M4 servers
4.1(1f)	4.1(1c)	Cisco UCS C220 M5, C240 M5, C480 M5, C480 ML M5, S3260 M5, C125 M5, C220 M4, C240 M4, C460 M4, and S3260 M4 servers
4.1(1d)	4.1(1b)	Cisco UCS C220 M5, C240 M5, C480 M5, and C480 ML M5 servers
4.1(1c)	4.1(1a)	Cisco UCS C220 M5, C240 M5, C480 M5, C480 ML M5, S3260 M5, C125 M5, C220 M4, C240 M4, C460 M4, and S3260 M4 servers

Table 2: Cisco IMC and UCS Manager Software Releases for Rack Mount Servers for Cisco IMC 4.0(4) Release

Cisco IMC Release	Cisco UCS Manager Release	Rack Mount Servers
4.0(4m)	4.0(4j)	Cisco UCS C220 M5, C240 M5, C480 M5, and S3260 M5 servers
4.0(4l)	4.0(4i)	Cisco UCS C220 M5, C240 M5, C480 M5, and S3260 M5 servers
4.0(4k)	4.0(4h)	Cisco UCS C220 M5, C240 M5, and S3260 M5 servers
4.0(4j)	No Support	Cisco UCS S3260 M5 servers
4.0(4i)	4.0(4g)	Cisco UCS C220 M5, C240 M5, C480 M5 and S3260 M5 servers
4.0(4h)	4.0(4e)	Cisco UCS C220 M5, C240 M5, C480 M5 and S3260 M5 servers
4.0(4f)	4.0(4d)	Cisco UCS C220 M5, C240 M5, C480 M5, S3260 M5 and C480 ML M5 servers
4.0(4e)	4.0(4c)	Cisco UCS C220 M5, C240 M5, C480 M5, S3260 M5 and C480 ML M5 servers
4.0(4d)	No Support	Cisco UCS C220 M5, C240 M5, C480 M5 and S3260 M5 servers
4.0(4b)	4.0(4a)	Cisco UCS C220 M5, C240 M5, C480 M5, S3260 M5 and C480 ML M5 servers

Table 3: Cisco IMC and UCS Manager Software Releases for Rack Mount Servers for Cisco IMC 4.0(3) Release

Cisco IMC Release	Cisco UCS Manager Release	Rack Mount Servers
4.0(3b)	4.0(3a)	Cisco UCS C220 M5 and C240 M5 servers

Table 4: Cisco IMC and UCS Manager Software Releases for Rack Mount Servers for Cisco IMC 4.0(2) Release

Cisco IMC Release	Cisco UCS Manager Release	Rack Mount Servers
4.0(2o)	4.0(4j)	Cisco UCS C220 M5, C240 M5, C480 M5, C480 ML M5, S3260 M5, C125 M5, C220 M4, C240 M4, C460 M4, and S3260 M4 servers

Cisco IMC Release	Cisco UCS Manager Release	Rack Mount Servers
4.0(2n)	No support.	Cisco UCS C220 M5, C240 M5, C480 M5, C480 ML M5, S3260 M5, C125 M5, C220 M4, C240 M4, C460 M4, and S3260 M4 servers
4.0(2m)	No support.	Cisco UCS S3260 M4 and M5 servers
4.0(2l)	No support.	Cisco UCS C220 M5, C240 M5, C480 M5, C480 ML M5, S3260 M5, C220 M4, C240 M4, C460 M4, and S3260 M4 servers
4.0(2k)	No support.	Cisco UCS S3260 M4 and M5 servers
4.0(2i)	No support.	Cisco UCS C460 M4, S3260 M4, and S3260 M5 servers
4.0(2h)	4.0(2e)	Cisco UCS C220 M5, C240 M5, C480 M5, C480 ML M5, S3260 M5, C125 M5, C220 M4, C240 M4, C460 M4, and S3260 M4 servers
4.0(2f)	4.0(2d)	Cisco UCS C220 M5, C240 M5, C480 M5, C480 ML M5, S3260 M5, C125 M5, C220 M4, C240 M4, C460 M4, and S3260 M4 servers
4.0(2d)	4.0(2b)	Cisco UCS C220 M5, C240 M5, C480 M5, C480 ML M5, S3260 M5, C125 M5, C220 M4, C240 M4, C460 M4, and S3260 M4 servers
4.0(2c)	4.0(2a)	Cisco UCS C220 M5, C240 M5, C480 M5, C480 ML M5, S3260 M5, C125 M5, C220 M4, C240 M4, C460 M4, and S3260 M4 servers

Table 5: Cisco IMC and UCS Manager Software Releases for Rack Mount Servers for Cisco IMC 4.0(1) Release

Cisco IMC Release	Cisco UCS Manager Release	Rack Mount Servers
4.0(1e)	No support.	Cisco UCS M4, M5 servers and C125 M5
4.0(1d)	4.0(1d)	Cisco UCS M4, M5 servers and C125 M5
4.0(1c)	4.0(1c)	Cisco UCS M4, M5 servers and C125 M5

Cisco IMC Release	Cisco UCS Manager Release	Rack Mount Servers
4.0(1b)	4.0(1b)	Cisco UCS M4, M5 servers and C125 M5
4.0(1a)	4.0(1a)	Cisco UCS M4, M5 servers and C125 M5

Table 6: Cisco IMC and UCS Manager Software Releases for Rack Mount Servers for Cisco IMC 3.1(3) Release

Cisco IMC Release	Cisco UCS Manager Release	Rack Mount Servers
3.1(3k)	3.2(3p)	Cisco UCS C480 M5, C220 M5, C240 M5, and S3260 M5 servers
3.1(3j)	No Support **Note** We support discovery and upgrade or downgrade functions with Cisco UCS Manager.	Cisco UCS C480 M5, C220 M5, C240 M5, and S3260 M5 servers
3.1(3i)	3.2(3i)	Cisco UCS C480 M5, C220 M5, C240 M5, and S3260 M5 servers
3.1(3h)	3.2(3h)	Cisco UCS C480 M5, C220 M5, C240 M5, and S3260 M5 servers
3.1(3g)	3.2(3g)	Cisco UCS C480 M5, C220 M5, C240 M5, and S3260 M5 servers
3.1(3d)	3.2(3e)	Cisco UCS C480 M5, C220 M5, C240 M5, and S3260 M5 servers
3.1(3c)	3.2(3d)	Cisco UCS C480 M5, C220 M5, C240 M5, and S3260 M5 servers
3.1(3b)	3.2(3b)	Cisco UCS C480 M5, C220 M5, and C240 M5 servers
3.1(3a)	3.2(3a)	Cisco UCS C480 M5, C220 M5, C240 M5, and S3260 M5 servers

Table 7: Cisco IMC and UCS Manager Software Releases for Rack Mount Servers for Cisco IMC 3.1(2) Release

Cisco IMC Release	Cisco UCS Manager Release	Rack Mount Servers
3.1(2d)	3.2(2d)	Cisco UCS C480 M5, C220 M5, and C240 M5
3.1(2c)	3.2(2c)	Cisco UCS C480 M5, C220 M5, and C240 M5

Cisco IMC Release	Cisco UCS Manager Release	Rack Mount Servers
3.1(2b)	3.2(2b)	Cisco UCS C480 M5, C220 M5, and C240 M5

Table 8: Cisco IMC and UCS Manager Software Releases for Rack Mount Servers for Cisco IMC 3.1(1) Release

C-Series Standalone Release	Cisco UCS Manager Release	C-Series Servers
3.1(1d)	3.2(1d)	Cisco UCS C220 M5/C2540 M5

Table 9: Cisco IMC and UCS Manager Software Releases for Rack Mount Servers for Cisco IMC 3.0(4) Release

Cisco IMC Release	Cisco UCS Manager Release	Rack-Mount Servers
3.0(4r)	No support	Cisco UCS C220 M4, C240 M4, C460 M4, S3260 M4, C22 M3, C24 M3, C220 M3, C240 M3, C3160 M3, S3260 M3
3.0(4q)	No support	Cisco UCS C220 M4, C240 M4, C460 M4, S3260 M4, C22 M3, C24 M3, C220 M3, C240 M3, C3160 M3, S3260 M3
3.0(4p)	3.2(3o)	Cisco UCS C220 M4, C240 M4, C460 M4, S3260 M4, C22 M3, C24 M3, C220 M3, C240 M3, C3160 M3, S3260 M3
3.0(4o)	No support	Cisco UCS C220 M4, C240 M4, C460 M4, S3260 M4, C22 M3, C24 M3, C220 M3, C240 M3, C3160 M3, S3260 M3
3.0(4n)	No support.	Cisco UCS C220 M4, C240 M4, C460 M4, S3260 M4, C22 M3, C24 M3, C220 M3, C240 M3, C3160 M3, S3260 M3
3.0(4m)	No support.	Cisco UCS C220 M4, C240 M4, C460 M4, S3260 M4, C22 M3, C24 M3, C220 M3, C240 M3, C3160 M3, S3260 M3
3.0(4l)	No support.	Cisco UCS C220 M4, C240 M4, C460 M4, S3260 M4, C22 M3, C24 M3, C220 M3, C240 M3, C3160 M3, S3260 M3

Cisco IMC Release	Cisco UCS Manager Release	Rack-Mount Servers
3.0(4k)	No support.	Cisco UCS C220 M4, C240 M4, C460 M4, S3260 M4, C22 M3, C24 M3, C220 M3, C240 M3, C3160 M3, S3260 M3
3.0(4j)	3.1(3k)	Cisco UCS C220 M4, C240 M4, C460 M4, S3260 M4, C22 M3, C24 M3, C220 M3, C240 M3, C3160 M3, S3260 M3
3.0(4i)	3.1(3j)	Cisco UCS C220 M4, C240 M4, C460 M4, S3260 M4, C22 M3, C24 M3, C220 M3, C240 M3, C3160 M3, S3260 M3
3.0(4e)	No support	Cisco UCS C220 M4, C240 M4, C460 M4, S3260 M4, C22 M3, C24 M3, C220 M3, C240 M3, C3160 M3, S3260 M3
3.0(4d)	3.1(3h)	Cisco UCS C220 M4, C240 M4, C460 M4, S3260 M4, C22 M3, C24 M3, C220 M3, C240 M3, C3160 M3, S3260 M3
3.0(4a)	3.1(3f)	Cisco UCS C220 M4, C240 M4, C460 M4, S3260 M4, C22 M3, C24 M3, C220 M3, C240 M3, C3160 M3, S3260 M3

Table 10: Cisco IMC and UCS Manager Software Releases for Rack Mount Servers for Cisco IMC 3.0(3) Release

Cisco IMC Release	Cisco UCS Manager Release	Rack-Mount Servers
3.0(3f)	-	Cisco UCS C240 M4, and C220 M4
3.0(3e)	3.0(3e)	Cisco UCS C22 M3, C24 M3, C220 M3, C240 M3, C220 M4, C240 M4, C460 M4, C3160 M3, S3260 M4 and S3260 M3 servers
3.0(3c)	3.0(3c)	Cisco UCS C240 M4, and C220 M4
3.0(3b)	3.0(3b)	Cisco UCS S3260 M3, C3160 M3, C460 M4, C240 M4, and C220 M4
3.0(3a)	3.1(3a)	Cisco UCS C22 M3, C24 M3, C220 M3, C240 M3, C220 M4, C240 M4, C460 M4, C3160 M3, S3260 M4 and S3260 M3 servers

Table 11: Cisco IMC and UCS Manager Software Releases for Rack Mount Servers for Cisco IMC 3.0(2) Release

Cisco IMC Release	Cisco UCS Manager Release	Rack-Mount Servers
3.0(2b)	No Support **Note** We support discovery and upgrade or downgrade functions with Cisco UCS Manager.	C220 M4/C240 M4 only

Table 12: Cisco IMC and UCS Manager Software Releases for Rack Mount Servers for Cisco IMC 3.0(1) Release

Cisco IMC Release	Cisco UCS Manager Release	Rack-Mount Servers
3.0(1d)	No Support **Note** We support discovery and upgrade or downgrade functions with Cisco UCS Manager.	All M3/M4 except C420 M3
3.0(1c)	No Support	All M3/M4 except C420 M3

Cisco IMC Release	UCS Manager Release	Rack Mount Servers
2.0(13e)	3.1(2b)	All M3/M4 except C420 M3
2.0(10b)	3.1(1g)	C220 M4/C240 M4 only
2.0(9c)	3.1(1e)	All other M3/M4
2.0(9f)	2.2(7b)	For all other M3/M4
2.0(10b)	2.2(7b)	C220 M4/C240 M4 only
1.5(9d)	2.2(7b)	C420-M3, C260-M2, C460-M2 only
1.5(9d)	2.2(8f)	C420-M3, C260-M2, C460-M2 only
2.0(9c)	2.2(8f)	For all other M3/M4
2.0(10b)	2.2(8f)	C220 M4/C240 M4 only
2.0(12b)	2.2(8f)	C460 M4 only
1.5(8a)	2.2(6g)	C420 M3, C260 M2, C460 M2 only
2.0(8d)	2.2(6c)	For all other M3/M4

Cisco IMC Release	UCS Manager Release	Rack Mount Servers
1.5(7f)	2.2(5b)	C420 M3, C260 M2, C460 M2 only
2.0(6d)	2.2(5a)	For all other M3/M4
1.5(7a)2	2.2(4b)	C420 M3, C260 M2, C460 M2 only
2.0(4c)	2.2(4b)	For all other M3/M4
1.5(7c)1	2.2(3b)	C420 M3, C260 M2, C460 M2 only
2.0(3d)1	2.2(3a)	For all other M3/M4

System Requirements

The management client must meet or exceed the following minimum system requirements:

- HTML based interfaces are supported on:
  - Microsoft Internet Explorer 10.0 or 11
  - Mozilla Firefox 47 or higher
  - Google Chrome 50 or higher
  - Safari 9 or higher

Note If the management client is launched using an unsupported browser, check the help information from the `For best results use supported browsers` option available in the login window for the supported browser versions.

- Microsoft Windows 10, Microsoft Windows 7, Microsoft Windows XP, Microsoft Windows Vista, Apple Mac OS, Red Hat Enterprise Linux 5.0 or higher operating systems
- Transport Layer Security (TLS) version 1.2.

Hardware and Software Interoperability

For detailed information about storage switch, operating system and adapter, see the *Hardware and Software Interoperability Matrix* for your release located at:

http://www.cisco.com/en/US/products/ps10477/prod_technical_reference_list.html

Note Connectivity is tested between the server and the first connected device. Further connections, such as to storage arrays after a switch are not listed in the Cisco UCS Hardware Compatibility List though they may be highlighted in the vendor support matrix for those devices.

For details about transceivers and cables that are supported on VIC cards, see the Transceiver Modules Compatibility Matrix

You can also see the VIC data sheets for more compatibility information: Cisco UCS Virtual Interface Card Data Sheets

Upgrade Paths to Release 4.1

The section provides information on the upgrade paths to release 4.1.

Important While upgrading Cisco UCS C220 M5 or C480 M5 servers to release 4.1 under the following conditions:

- if you are upgrading from any release earlier than 4.0(4)
- if **Legacy Boot Mode** is enabled and no **Cisco IMC Boot Order** is configured
- and, if the server is booting from Cisco HWRAID adapter

then, you should perform one of the following before upgrading:

- Run XML-API scripts and UCSCFG based scripts provided at Configuring UCS Boot Order using the XML API.

  OR

- Manually configure the intended boot order through Cisco IMC GUI or CLI interfaces.

Refer to the table for upgrade paths for various Cisco UCS C-series IMC versions.

Table 13: Upgrade Paths to Release 4.1

Upgrade From Release	Upgrade To Release	Recommended Upgrade Path
All M4 and M5 Servers from 4.0	4.1	Follow below upgrade path: • You can use Interactive HUU or Non-Interactive HUU (NIHUU) script to update the server. • While updating the firmware using the NIHUU tool, use the Python scripts that are released with version 4.1(1c). • Use OpenSSL 1.0.1e-fips on the client side (where the NIHUU python scripts are running). • Download HUU iso from here. • Download NIHUU script from here.

Upgrade From Release	Upgrade To Release	Recommended Upgrade Path
All M5 Servers from 3.1	4.1	Follow below upgrade path: • You can use Interactive HUU or NIHUU script to update the server. • While updating the firmware using the NIHUU tool, use the Python scripts that are released with version 4.1(1c). • Use OpenSSL 1.0.1e-fips on the client side (where the NIHUU python scripts are running). • Download HUU iso from here. • Download NIHUU script from here.
For all M4 servers for releases greater than 2.0(4c) For all M4 servers from 3.0	4.1	Follow below upgrade path: • You can use Interactive HUU or NIHUU script to update the server. • While updating the firmware using the NIHUU tool, use the Python scripts that are released with version 4.1(1c). • Use OpenSSL 1.0.1e-fips on the client side (where the NIHUU python scripts are running). • If you wish to secure Cimc Boot, set flag **use_cimc_secure** as **yes** in **multiserver_config** file present with python script. • Download HUU iso from here. • Download NIHUU script from here.

Upgrade From Release	Upgrade To Release	Recommended Upgrade Path
For all M4 servers for release lesser than 2.0(4c)	4.1	Follow these steps to upgrade from releases less than 2.0(4c) to 4.1: **Upgrade from version less than 2.0(4c) to 2.0(4c)** • You can use Interactive HUU or NIHUU script to update the server. • While updating the firmware using the Non-Interactive HUU (NIHUU) tool, use the Python scripts that are released with version 3.0(3a). • Use OpenSSL 1.0.0-fips on the client side (where the NIHUU python scripts are running). • Download HUU iso from here. • Download NIHUU script from here. **Upgrade from 2.0(4c) to 4.1** • You can use Interactive HUU or NIHUU script to update the server. • While updating the firmware using the NIHUU tool, use the Python scripts that are released with version 4.1(1c). • Use OpenSSL 1.0.1e-fips on the client side (where the NIHUU python scripts are running). • If you wish to secure Cimc Boot, set flag **use_cimc_secure** as **yes** in **multiserver_config** file present with python script. • Download HUU iso from here. • Download NIHUU script from here.

Firmware Upgrade Details

Firmware Files

The C-Series software release 4.1(1) includes the following software files:

CCO Software Type	File name(s)	Comment

Unified Computing System (UCS) Server Firmware	ucs-c125-huu-4.1 .1d.iso ucs-c220m5-huu-4.1.1d.iso ucs-c240m5-huu-4.1.1d.iso ucs-c480m5-huu-4.1.1d.iso ucs-s3260-huu-4.1.1c.iso ucs-c240m4-huu-4.1.1c.iso ucs-c220m4-huu-4.1.1c.iso ucs-c460m4-huu-4.1.1c.iso For release specific ISO versions, see Cisco UCS C-Series Integrated Management Controller Firmware Files, Release 4.1	Host Upgrade Utility
Unified Computing System (UCS) Drivers	ucs-cxxx-drivers.4.1.1c.iso	Drivers
Unified Computing System (UCS) Utilities	ucs-cxxx-utils-efi.4.1.1c.iso ucs-cxxx-utils-linux.4.1.1c.iso ucs-cxxx-utils-vmware.4.1.1c.iso ucs-cxxx-utils-windows.4.1.1c.iso	Utilities

Note Always upgrade the BIOS, the Cisco IMC and CMC from the HUU ISO. Do not upgrade individual components (only BIOS or only Cisco IMC), since this could lead to unexpected behavior. If you choose to upgrade BIOS, and the Cisco IMC individually and not from the HUU ISO, make sure to upgrade both Cisco IMC, and BIOS to the same container release. If the BIOS and the Cisco IMC versions are from different container releases, it could result in unexpected behavior. Cisco recommends that you use the Update All option from the Host Upgrade Utility to update the firmware versions of Cisco IMC, BIOS, and all other server components (VIC, RAID Controllers, PCI devices, and LOM) together.

Host Upgrade Utility

The Cisco Host Upgrade Utility (HUU) is a tool that upgrades the Cisco UCS C-Series firmware.

The image file for the firmware is embedded in the ISO. The utility displays a menu that allows you to choose which firmware components to upgrade. For more information on this utility, see http://www.cisco.com/en/US/products/ps10493/products_user_guide_list.html.

For details of firmware files in Cisco Host Upgrade Utility for individual releases, see Cisco UCS C-Series Integrated Management Controller Firmware Files, Release 4.1.

Updating the Firmware

Use the Host Upgrade Utility to upgrade the C-Series firmware. Host Upgrade Utility can upgrade the following software components:

- BIOS

- Cisco IMC
- CMC
- Cisco VIC Adapters
- LSI Adapters
- LAN on Motherboard
- PCIe adapter firmware
- HDD firmware
- SAS Expander firmware
- DCPMM Memory

All firmware should be upgraded together to ensure proper operation of your server.

Note We recommend that you use the **Update All** option from the Host Upgrade Utility to update the firmware versions of Cisco IMC, BIOS and all other server components (VIC, RAID Controllers, PCI devices, and LOM) together. Click **Exit** once you deploy the firmware.

For more information on how to upgrade the firmware using the utility, see:

http://www.cisco.com/c/en/us/support/servers-unified-computing/ucs-c-series-rack-servers/products-user-guide-list.html

New Software Features in Release 4.1

New Software Features in 4.1(1h)

There are no new software features in release 4.1(1h).

New Software Features in 4.1(1g)

There are no new software features in release 4.1(1g).

New Software Features in 4.1(1f)

There are no new software features in release 4.1(1f).

New Software Features in 4.1(1d)

There are no new software features in release 4.1(1d).

New Software Features in 4.1(1c)

New Software Features in Release 4.1(1c)

The following new software features are supported in Release 4.1(1c):

- Release 4.1 introduces a new user configuration option called **User Mode** that allows you to switch between IPMI and non-IPMI user modes. Introduction of the non-IPMI user mode provides enhanced

password management and enhancements to the BMC database that were restricted in earlier releases due to the constraints posed by the IPMI 2.0 standards.

- A new fan policy called **Acoustic** policy is available for Cisco UCS C240 M5 servers. This option can be used for configuring the fan noise level, thereby enabling noise reduction in the servers.

  Note Application of this policy might result in performance throttling impacting system performance. If excessive thermal or performance events are recorded in the event logs, select a standard fan control policy like **Low Power**, which is a non-disruptive change.

- 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.
- **Multi Queue** RoCEv2 properties are added for Cisco UCS 14xx series adapters.
- The following mount options are added for virtual media creation using CIFS:
  - **rw**
  - **ro**
  - **vers**
- You can now delete PID catalogs using the **Delete PID Catalog** option available under **Utilities**.
- DRAM Post Package Repair - Cisco IMC supports Post Package Repair as memory repair scheme. Under PPR, Cisco IMC supports Hard-PPR (hPPR), which permanently remaps accesses from a designated faulty row to a designated spare row.
- Partial Memory Mirroring - Cisco IMC supports this memory (reliability, availability, and serviceability) RAS feature which enables duplicating memory content at a remote DIMM in the partition.
- 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.
- The following BIOS tokens are added:
  - NetworkStack
  - IPV4PXE

  Note Java-based KVM is not supported 4.1(1c) onwards.

- Limit Memory Capacity - Using Cisco IMC release 4.1(1c) and later, you can configure physical memory capacity in the **Memory Size Limit in GB** field (under Memory BIOS tokens). The limit memory capacity is transparent to the operating system and is available for all the UCS Cisco M5 servers with DDR4 configurations.

Note

- Persistent memory configuration is not supported with limit memory capacity.
- The value for the **Memory Size Limit in GB** field must be 4GB or higher.

New Hardware Features in Release 4.1

New Hardware in Release 4.1(1h)

There are no new hardware in release 4.1(1h).

New Hardware in Release 4.1(1g)

There are no new hardware in release 4.1(1g).

New Hardware in Release 4.1(1f)

There are no new hardware in release 4.1(1f).

New Hardware in Release 4.1(1d)

There are no new hardware in release 4.1(1d).

New Hardware in Release 4.1(1c)

- 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 Cisco UCS C125 M5 servers.
- Support for the Intel X710-DA2 2 x 10GbE SFP+ PCIe Network Interface Card on Cisco UCS C125 M5 servers.
- Support for the Mellanox ConnectX-5 MCXM516A-CDAT 2 x 100GbE QSFP PCI Network Interface Card on Cisco UCS C220 M5, C240 M5, C480 M5, and C480 M5 ML servers.
- Support for the Mellanox ConnectX-5 MCX515A-CCAT 1 x 100GbE QSFP PCI Network Interface Card on Cisco UCS C220 M5, C240 M5, and C480 M5 servers.
- Support for the Mellanox ConnectX-5 MCX512A-ACAT 2 x 25Gb/10GbE SFP PCI Network Interface Card on Cisco UCS C220 M5, C240 M5, and C480 M5 servers
- Support for the following NVMe drives on Cisco UCS C125 M5 servers:

NVMe Drive	PID
Intel P4510 1TB (SSDPE2KX010T8K)	UCSC-NVME2H-I1000
Intel P4510 4TB (SSDPE2KX040T8K)	UCSC-NVME2H-I4000
Intel P4610 1.6TB (SSDPE2KE016T8K)	UCSC-NVME2H-I1600
Intel P4610 3.2TB (SSDPE2KE032T8K)	UCSC-NVME2H-I3200

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

Software Utilities

The following standard utilities are available:

- Host Update Utility (HUU)
- BIOS and Cisco IMC Firmware Update utilities
- Server Configuration Utility (SCU)
- Server Diagnostic Utility (SDU)

The utilities features are as follows:

- Availability of HUU, SCU on the USB as bootable images. The USB also contains driver ISO, and can be accessed from the host operating system.

SNMP

The supported MIB definition for this release and later releases can be found at the following link:

ftp://ftp.cisco.com/pub/mibs/supportlists/ucs/ucs-C-supportlist.html

Note The above link is incompatible with IE 9.0.

Security Fixes

Security Fixes in Release 4.1(1f)

The following Security Fixes were added in Release 4.1(1f):

Release	Defect ID	CVE ID	Description
4.1(1f)	CSCvs81690	• CVE-2020-0548 • CVE-2020-0549	Cisco UCS C-Series and S-Series 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.

Resolved Caveats

Resolved Caveats in 4.1(1h)

The following caveats were resolved in Release 4.1(1h):

Defect ID	Symptom	First Release Affected	Resolved in Release
CSCvu93105	For Cisco UCS C125 M5 servers, modifying Memory Interleaving BIOS token from Cisco IMC or BIOS setup window does not trigger the feature functionality even though the BIOS token value is updated correctly. This issue is now resolved.	4.0(2m)	4.1(1h)

Resolved Caveats in 4.1(1g)

The following caveats were resolved in Release 4.1(1g):

Table 14: BIOS

Defect ID	Symptom	First Release Affected	Resolved in Release

CSCvu47239	Cisco UCS S3260 M5 servers with UCSC-C3260-SIOC VIC adapter and Network Boot enabled (PXE) in legacy or UEFU boot mode, alert CATERR and fail to complete POST. The following messages are displayed:
	`Configuring memory`
	OR
	`Configuring Platform Hardware`
	If FRB2 timer is enabled, servers proceed to auto reset after a ten minute period. This warm boot completes the POST and the boot attempt is successful.
	This issue is now resolved.
		4.0(4h)	4.1(1g)

Defect ID	Symptom	First Release Affected	Resolved in Release
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. The servers get stuck at the memory testing step, which results in boot loop triggering #IERR and M2M timeout in the memory system. For more information, see: • Intel Errata - SKX108 • Intel Errata - CLX37 This issue is now resolved.	4.0(4e)	4.1(1g)

Defect ID	Symptom	First Release Affected	Resolved in Release
CSCvu14656	On upgrade of BIOS to one of the following versions, the booting of Cisco UCS C220 M5, C240 M5, and S3260 M5 servers gets stuck at the memory testing step: • C220M5.4.0.4p.0.0224200755 • C240M5.4.0.4r.0.0305200743 • S3X60M5.4.0.4o.0.0224200755 • C220M5.4.1.1c.0.0404202345 • C240M5.4.1.1c.0.0405200025 • S3X60M5.4.1.1c.0.0405200025 This issue is now resolved.	4.0(4h)	4.1(1g)

Defect ID	Symptom	First Release Affected	Resolved in Release
CSCvu11155	After upgrading the BIOS to one of the following versions, you may experience performance degradation with Cisco UCS C220 M5, C240 M5, and S3260 M5 servers running on Second Generation Intel® Xeon® Scalable Processors: • C220M5.4.0.4p.0.0224200755 • C240M5.4.0.4r.0.0305200743 • S3X60M5.4.0.4o.0.0224200755 • C220M5.4.1.1c.0.0404202345 • C240M5.4.1.1c.0.0405200025 • S3X60M5.4.1.1c.0.0405200025 This issue is now resolved.	4.0(4k)	4.1(1g)

Table 15: External Controllers

Defect ID	Symptom	First Release Affected	Resolved in Release
CSCvq53066	Upgrading host firmware from any release 4.0(2x) or earlier to release 4.0(4b) using auto-install in a Cisco UCS C240 M5 server, results in SAS controller firmware activation failure. Following faults are seen: • `F78413 - Update Failed on Storage Controller` • `F0181 - Drive state: unconfigured bad` • `F0856 - Activation failed and Activate Status set to failed` This issue is now resolved.	4.0(4d)	4.1(1g)

Table 16: VIC Firmware

Defect ID	Symptrom	First Release Affected	Resolved in Release
CSCvm59040	Cisco UCS C220 servers with an up-time of over 180 days and equipped with Cisco UCS VIC 1225 may report loss of connectivity from the host. This issue is now resolved with the latest firmware version.	2.0(13f)	4.1(1g)

Resolved Caveats in 4.1(1f)

The following caveats were resolved in Release 4.1(1f):

Table 17: BIOS

Defect ID	Symptom	First Release Affected	Resolve in Release
CSCvr79388	Cisco UCS C-Series 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 now resolved. For more information, see the below links: • Intel® Xeon® Processor Scalable Family Specification Update (Errata > SKX108) • Second Generation Intel® Xeon® Scalable Processors Specification Update (Errata > CLX37) This issue is resolved in release 4.1(1g) for Cisco UCS C480 M5 and Cisco UCS 480 M5 ML servers. For more information, see CSCvt64871 in the Resolved Caveats section.	4.0(4e)	4.1(1f)
CSCvq81611	DCPMM performance related BIOS tokens are now displayed in Cisco IMC GUI and CLI interfaces, and can be updated as required.	4.0(4b)	4.1(1f)

Table 18: BMC

Defect ID	Symptom	First Release Affected	Resolved in Release

CSCvs92008	Socket connection between Cisco IMC and BMC reaches a max limit and blocks further connection with the following error message:
	`Error: Maxed out all client socket connections to remote manager in BMC. Please retry after a while`
	OR
	`Communication to peer CMC remote manager. Internal Error. Please retry`
	This issue is now resolved.
		4.0(4b)	4.1(1f)

Table 19: External Controllers

Defect ID	Symptom	First Release Affected	Resolved in Release
CSCvr89052	In S3260 M5 server, the assigned drives are not displayed correctly in SBMezz1 and SBMezz2 controllers when the below command is executed: `storcli /cX/eall/sall show` This issue is now resolved.	4.1(1c)	4.1(1f)

Table 20: Host Firmware Upgrade

Defect ID	Symptom	First Release Affected	Resolved in Release
CSCvt61633	The following LT0400MO and LT1600MO SSD models report 0GB of available storage space remaining under normal operating conditions for forty thousand power on hours: • UCS-SD400G12S4-EP • UCS-C3X60-12G240 • UCS-SD16TB12S4-EP • UCS-C3X60-12G2160 The drives go offline and become unusable after a power-cycle. This issue now resolved with the new firmware version.	3.0(4p)	4.1(1f)

Resolved Caveats in 4.1(1d)

The following defect is resolved in Release 4.1(1d):

Table 21: BMC

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

Resolved Caveats in 4.1(1c)

The following defects were resolved in Release 4.1(1c):

Table 22: BIOS

Defect ID	Symptom	First Affected Release	Resolved in Release
CSCvp21118	Precision boot order (L2 boot order) feature of Cisco UCS C480 M5 servers now list the external physical USB drives in the boot order. This issue is now resolved.	4.0(4b)	4.1(1c)
CSCvr05344	Disabling onboard LOM controller from BIOS settings disables the LOM controller. The controller no longer appears in the inventory. This issue is now resolved.	4.0(2f)	4.1(1c)

Table 23: BMC

Defect ID	Symptom	First Affected Release	Resolved in Release
CSCvq63344	While running Intel® Intelligent Power Technology Node Manager (NM) PTU, the server does not respond after BIOS POST. This issue is now resolved.	4.0(4b)	4.1(1c)
CSCvr71907	On S3260 M4 servers, NIHUU firmware upgrade or downgrade may fail with the `timeout error`. When this happens firmware of only some components are updated and firmware of some components have to be updated again. This issue is now resolved.	4.0(2k)	4.0(2m)
CSCvs86186	NIHUU fails to recognize special characters in share server password and the following error message is displayed: `Permission denied.` This issue is now resolved.	4.0(2h)	4.1(1c)

Defect ID	Symptom	First Affected Release	Resolved in Release
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 now resolved.	4.0(2d)	4.1(1c)
CSCvs67980	HUU files hosted on NFS/CIFS share with hidden folders (folder name format *folder_name$*) fail to map with the following error: `ERROR: Illegal remoteShare` This issue is now resolved.	4.0(4d)	4.1(1c)
CSCvs40156	SNMPv3 credentials are no longer visible in clear text after exporting the configuration file from any Cisco UCS C Series server. This issue is now resolved.	4.0(2g)	4.1(1c)

Table 24: CMC

Defect ID	Symptom	First Affected Release	Resolved in Release
CSCvr54532	Cisco IMC logs show `PSUx_AC_OK` alarms for Cisco UCS S3260 M5 servers even though there is no actual power loss. This issue is now resolved.	4.0(2c)	4.1(1c)

Table 25: External Controllers

Defect ID	Symptom	First Affected Release	Resolved in Release
CSCvs17338	Cisco IMC displays Intel® Youngsville SSD and other SATA drives to be in **Unconfigured Bad** state in Cisco UCS C240 M5 servers when Cisco IMC is upgraded from 4.0(2c) to any later release and the controller firmware version is 00.00.00.58. This issue is now resolved.	4.0(2c)	4.1(1c)
CSCvr23136	Discovery of a Cisco UCS C240 M5 server, equipped with Cisco 12G Modular SAS HBA controller, fails with one of the following errors: • `mc_attrib_set_suboem_id failed to set the SubOEM ID` • `Cisco IMC is not able to detect any drives.` This issue is now resolved.	4.0(4i)	4.1(1c)
CSCvm78123	ISCSI Boot protocol for Intel® XXV710-DA2 and X710-T4 cards is now displayed in the Boot Utility (bootutil) for all servers. This issue is now resolved.	4.0(2c)	4.1(1c)
CSCvq50290	Cisco IMC no longer fails to recognize SATA disk UCS-SD960G63X-EP after an upgrade. This issue is now resolved.	4.0(4b)	4.1(1c)

Table 26: External PSU

Defect ID	Symptom	First Affected Release	Resolved in Release
CSCvp10085	For Cisco UCS C220 M5 servers, Cisco IMC occasionally falsely reported critical PSU inlet over temperature alert to the BMC. The issue did not have any functionality impact on the system and has now been resolved. Cisco IMC no longer reports this false alert.	3.(1d)	4.1(1c)

Table 27: FlexFlash

Defect ID	Symptom	First Affected Release	Resolved in Release

CSCvr54071	FlexFlash no longer displays the following error messages after an upgrade:
	`CYWB_LOG: CYWB FWLOG (usbapp): USB SetConfig event, data=1`
	`CYWB_LOG: CYWB: USB connection status, 3.0 enable=1, 3.0 mode=0`
	`CYWB_LOG: CYWB FWLOG (usbapp): USB Reset event, data=0`
	This issue is now resolved.
		4.0(2g)	4.1(1c)

Table 28: Host Firmware Upgrade

Defect ID	Symptom	First Affected Release	Resolved in Release
CSCvs48461	While upgrading Cisco IMC to 4.0(2m) or 4.0(4i) in Cisco UCS S3260 M5 and M4 servers, HUU and NIHUU report HDD firmware updates as failed, even after the actual update is successful. This issue is now resolved.	4.0(2m)	4.1(1c)
CSCvp28719	Cisco UCS C240 M5 servers no longer fail to upgrade to latest Cisco IMC version when HBA FC links are enabled using the Qlogic cards. This issue is now resolved.	4.0(1c)	4.1(1c)

Table 29: Intel® Optane™ Data Center Persistent Memory Modules

Defect ID	Symptom	First Affected Release	Resolved in Release
CSCvp15031	Intel® Optane™ Data Center persistent memory module health state no longer changes to **Non-functional** after upgrading the firmware. This issue is now resolved.	4.0(4b)	4.1(1c)
CSCvp03376	Fault engine displays `mismatch FW revision` warning for persistent memory DIMMs though the firmware version is the same on the DIMMs. This issue is now resolved.	4.0(4b)	4.1(1c)

Defect ID	Symptom	First Affected Release	Resolved in Release
CSCvp11872	Duplicate faults are reported for Intel® Optane™ Data Center persistent memory module. Existing persistent memory module faults are reported again (duplicates) after every host reboot. This issue is now resolved.	4.0(4b)	4.1(1c)

Table 30: SNMP

Defect ID	Symptom	First Affected Release	Resolved in Release
CSCvq43587	The following issues were noticed in Cisco UCS C-Series M5 servers, which are monitored by SNMPv3: • servers losing connectivity after a restart • few server settings impacted after a restart These issues are now resolved.	3.1(3h)	4.1(1c)

Open Caveats

Open Caveats in Release 4.1(1h)

The following defects are open in Release 4.1(1h):

Table 31: BIOS

Defect ID	Symptom	Workaround	First Affected Release
CSCvu76649	Cisco UCS C220 and C240 M4 servers stop responding at **Configuring Platform Hardware** screen and do not proceed to Cisco splash screen in vKVM. As a result, F2, F6, and F8 options are not available. You cannot perform the following: • boot the server to HUU through virtual image • configure BIOS setup • shift between standalone and Cisco UCS manager modes	There is no known workaround.	4.1(1g)

Open Caveats in Release 4.1(1g)

The following defects are open in Release 4.1(1g):

Table 32: BIOS

Defect ID	Symptom	Workaround	First Affected Release
CSCvu37394	Cisco UCS C480 M5 servers equipped with AMD Firepro 7150X2 16 GB GPU and set to Legacy boot mode, display the following error while booting: `System Software Event : Post sensor , System firmware error(Post error) , Unrecoverable video controller failure [0xFF09] was asserted` There is no functionality impact from this issue.	Change to UEFI boot mode.	3.1(2b)

Open Caveats in Release 4.1(1f)

The following defects are open in Release 4.1(1f):

Table 33: BIOS

Defect ID	Symptom	Workaround	First Affected Release
CSCvt25443	After updating the BIOS, Cisco UCS C480 M5 ML servers stop responding at BIOS POST causing CATER/IERR.	Power cycle from Cisco IMC GUI or from KVM console (**Power** > **Power cycle system(cold reboot)**.	4.0(4h)

Defect ID	Symptom	Workaround	First Affected Release
CSCvt64871	In rare situations, Cisco UCS C480 M5 ML and UCS C480 M5 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)	Temporarily 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)

Open Caveats in Release 4.1(1d)

There are no Open Caveats in release 4.1(1d).

Open Caveats in Release 4.1(1c)

Release 4.1(1c)

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

Table 34: BIOS

Defect ID	Symptom	Workaround	First Affected Release
CSCvs62684	After upgrading to 4.1.(1c), Cisco UCS C480 M5 servers do not respond at BIOS POST.	Disable PCIe RAS support or create vNIC fNIC endpoints.	4.1(1c)

Defect ID	Symptom	Workaround	First Affected Release
CSCvr82915	In Cisco UCS C240 M4 servers, Primary Wireless LAN Controller (WLC) does not respond to SSH, telnet, ping, or ARP, even though the LEDs are solid green. Primary WLC is also visible through CDP neighbors and is accessible through the Cisco IMC port. Moreover, secondary WLC does not becomes active, instead, it goes to maintenance mode. It is also accessible through the console but in maintenance mode. It does not receive data from the active WLC.	There is no known workaround.	4.1(1c)
CSCvt11230	Upgrading Cisco UCS C220 M5 or C480 M5 servers to release 4.1 under the following conditions causes a boot order change: • If you are upgrading from any release earlier than 4.0(4x) • If **Legacy Boot Mode** is enabled with no **Cisco IMC Boot Order** configured • and, if the server is booting from Cisco HWRAID adapters	Perform one of the following before upgrading: • Run XML-API scripts and UCSCFG based scripts provided here. OR • Manually configure the intended boot order through Cisco IMC GUI or CLI interfaces.	4.0(4x)

Table 35: BMC

Defect ID	Symptom	Workaround	First Affected Release
CSCvs61162	If Cisco UCS C125 server nodes are running on different Cisco IMC firmware versions, then Cisco IMC GUI and CLI display a false message that low level firmware update is required.	Ignore the error message. No action is required. Action may be required only when the node is running on Cisco IMC version 4.1 and chassis has at least one node with Cisco IMC release higher than 4.1.	4.1(1c)

Defect ID	Symptom	Workaround	First Affected Release
CSCvr54853	HTML KVM displays unrecognized character error message while pasting special characters like = and >.	Use Java KVM.	4.1(1c)
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(1c)
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(1c)
CSCvt05404	When you change the system host name and choose to generate a new certificate, the details for the fields like state, locality, organisation and so on, in the current certificate are displayed as NULL.	Do not generate a new certificate after changing the host name. Or upload the existing certificate again.	4.1(1c)
CSCvs26792	Cisco IMC GUI is inaccessible from Chrome web browser in macOS Catalina.	Use the Firefox web browser or from other OS. OR perform the following steps in macOS Catalina: **1.** Open the key-chain tool. **2.** Select the server certificate from **keychain** > **logins**. **3.** Right-click on the server certificate and select the **GetInfo** option. **4.** Expand the **Trusts** panel. **5.** From the drop-down list, select **when using the certificate**. **6.** Select **Always Trust** from options. **7.** Save and close the certificate. **8.** Reload Cisco IMC GUI in Chrome web browser.	4.1(1c)

Table 36: External Controllers

Defect ID	Symptom	Workaround	First Affected Release
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)
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 user guide 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(4e)

Defect ID	Symptom	Workaround	First Affected Release
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(4b)

Table 37: Host Firmware Upgrade

Defect ID	Symptom	Workaround	First Affected Release
CSCvr99365	Drive firmware upgrade fails on Cisco UCS M5 C-Series servers, and as a result, NIHUU upgrade times out.	Re-try NIHUU upgrade.	4.0(4h)

Known Behaviors and Limitations

Known Behaviors and Limitations in Release 4.1(1h)

There are no new known limitations in release 4.1(1h).

Known Behaviors and Limitations in Release 4.1(1g)

The following caveats are known limitations in release 4.1(1g):

Table 38: BIOS

Defect ID	Symptom	Workaround	First Affected Release
CSCvu62006	SLES 15.2 and Ubuntu 20.04 OS successfully install on Cisco UCS C-Series and S-Series M4 servers with UEFI boot entry. However, booting to UEFI default boot entry deactivates after a reboot.	Perform the following steps: **1.** Enter BIOS setup and create an admin password. **2.** Go to **Advanced** > **Trusted Computing** > and select TCG_2 for TPM 1.2 or 2.0 UEFI version. **3.** Press **F10** to save and exit.	4.0(2m)

Known Behaviors and Limitations in Release 4.1(1f)

There are no new known limitations in release 4.1(1f).

Known Behaviors and Limitations in Release 4.1(1d)

There are no new known limitations in release 4.1(1d).

Known Behaviors and Limitations in Release 4.1(1c)

The following caveats are known limitations in release 4.1(1c):

Table 39: BMC

Defect ID	Symptom	Workaround	First Affected Release
CSCvp66282	KVM console does not respond while activating vMedia after Cisco IMC GUI session times out.	Restart the KVM console.	4.0(4x)
CSCvr88858	When Cisco IMC is in non-IPMI mode, you cannot set more than 20 characters for the admin password in F8 utility.	Use the interfaces like Cisco IMC GUI, CLI, and XML interfaces to set the admin password.	4.1(1c)
CSCvs04850	You cannot create an image using HTML-based KVM on Web browsers like Mozilla Firefox and Internet Explorer. The following error message is displayed: `Your Browser does not support create image feature.`	Use Google Chrome Web browser to create an image using HTML-based KVM.	4.1(1c)
CSCvr66211	While launching KVM console for the first time using Safari web browser, Cisco IMC login screen is displayed instead of the KVM console.	Disable the pop-up blocker on the host.	4.1(1c)

Defect ID	Symptom	Workaround	First Affected Release
CSCvs11210	Login authentication fails after downgrading Cisco IMC to any release before 4.1(1c) while in non-IPMI user mode. This occurs because the login credentials are set to default after the downgrade. As a result, an NIHUU authentication error is also observed as the script is not able to login with credentials mentioned in config file.	Initiate NIHUU verification in Cisco IMC with the default admin password.	4.1(1c)

Table 40: External Controllers

Defect ID	Symptom	Workaround	First Affected Release

CSCvr01489	If Cisco UCS C480 M5 servers, having Mellanox 100G dual port cards connected to Cisco swtich, are configured for UEFI boot, the green LED on both the ports blink. When the boot mode is changed to Legacy and back to UEFI boot mode, LED on one of the ports starts blinking amber.	Run the following commands:
		`mlxconfig -e -d 5e:00.0 set ADVANCED_POWER_SETTINGS=True`
		`mlxconfig -e -d 5e:00.0 set DISABLE_SLOT_POWER_LIMITER=True`
			4.1(1c)

CSCvr10729	In Cisco UCS C240 M5 and C480 M5 servers with Mellanox ConnectX-5 cards, Mellanox HII iSCSI configuration does not work.	Configure the iSCSI using BIOS - Advance - iSCSI Configuration option.	4.1(1c)

Table 41: UCSCFG

Defect ID	Symptom	Workaround	First Affected Release
CSCvs39893	UCSCFG is unable to run CENT RHEL 8 due to unavailable packages and displays the following error message: `compact open-ssl Libraries missing in the installed Linux OS where command being executed.`	Install SSL, Crypto and compact OpenSSL libraries.	4.1(1c)

Related Documentation

For configuration information for this release, refer to the following:

- Cisco UCS C-Series Servers Integrated Management Controller CLI Configuration Guide
- Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide
- Cisco UCS Rack-Mount Servers Cisco IMC API Programmer's Guide

For information about installation of the C-Series servers, refer to the following:

- Cisco UCS C-Series Rack Servers Install and Upgrade Guides

The following related documentation is available for the Cisco Unified Computing System:

- Cisco UCS C-Series Servers Documentation Roadmap
- Cisco UCS Site Preparation Guide
- Regulatory Compliance and Safety Information for Cisco UCS
- For information about supported firmware versions and supported UCS Manager versions for the rack servers that are integrated with the UCS Manager for management, refer to Release Bundle Contents for Cisco UCS Software.

Refer to the release notes for Cisco UCS Manager software and the *Cisco UCS C Series Server Integration with Cisco UCS Manager Guide* at the following locations:

- Cisco UCS Manager Release Notes
- Cisco UCS C Series Server Integration with Cisco UCS Manager Guides