Release Notes for Cisco UCS Rack Server Software, Release 6.0(1)

First Published: 2025-09-02

Last Modified: 2026-03-04

Cisco UCS C-Series Servers

Cisco UCS C-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 software release 6.0(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 35 section.

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

Revision History

Revision	Date	Description
D1	March 04, 2026	Added CSCwt41941 in the section **Open Caveats** for the release 6.0(1.250192).

Revision	Date	Description
E0	January 14, 2026	Created release notes for 6.0(1.250194) for the following servers: • Cisco UCS C240 M8 servers This release includes a BMC firmware update that addresses a critical power-on issue affecting the Cisco UCS C240 M8 server. This release does not include any new hardware, security fixes, resolved caveats, or open caveats. The firmware files in Cisco Host Upgrade Utility for individual releases are available at: Cisco UCS C-Series Integrated Management Controller Firmware Files, Release 6.0
D0	December 18, 2025	Created release notes for 6.0(1.250192) for the following servers: • Cisco UCS C220 M8, C240 M8, C225 M8 and C245 M8 servers • Cisco UCS C220 M7 and C240 M7 servers • Cisco UCS C220 M6, C240 M6, C225 M6 and C245 M6 servers The firmware files in Cisco Host Upgrade Utility for individual releases are available at: Cisco UCS C-Series Integrated Management Controller Firmware Files, Release 6.0
A1	December 10, 2025	Added CSCws30219 in the section **Open Caveats**for the release 6.0(1.250127).

Revision	Date	Description
C0	November 12, 2025	Created release notes for 6.0(1.250174) for the following servers: • Cisco UCS C220 M8, C240 M8, C225 M8 and C245 M8 servers • Cisco UCS C220 M7 and C240 M7 servers • Cisco UCS C220 M6, C240 M6, C225 M6 and C245 M6 servers The firmware files in Cisco Host Upgrade Utility for individual releases are available at: Cisco UCS C-Series Integrated Management Controller Firmware Files, Release 6.0
B0	October 09, 2025	Created release notes for 6.0(1.250131) for the following servers: • Cisco UCS C220 M8, C240 M8, C225 M8 and C245 M8 servers • Cisco UCS C220 M7 and C240 M7 servers • Cisco UCS C220 M6, C240 M6, C225 M6 and C245 M6 servers The firmware files in Cisco Host Upgrade Utility for individual releases are available at: Cisco UCS C-Series Integrated Management Controller Firmware Files, Release 6.0

Revision	Date	Description
A0	September 02, 2025	Created release notes for 6.0(1.250130) for the following servers: • Cisco UCS C245 M8 servers The firmware files in Cisco Host Upgrade Utility for individual releases are available at: Cisco UCS C-Series Integrated Management Controller Firmware Files, Release 6.0
		Created release notes for 6.0(1.250127) for the following servers: • Cisco UCS C220 M8, C225 M8 and C240 M8 servers • Cisco UCS C220 M7 and C240 M7 servers • Cisco UCS C220 M6, C240 M6, C225 M6 and C245 M6 servers The firmware files in Cisco Host Upgrade Utility for individual releases are available at: Cisco UCS C-Series Integrated Management Controller Firmware Files, Release 6.0

Cisco IMC Release Number and .ISO Image Names

Beginning with the release 4.3, Cisco is updating the release number naming convention to align with the .ISO images.

Example: **4.3.1.YYXXXX**

- **4.3**—Represents the main release.
- **.1**—Represents the first release.

  For the current 4.3 main release, **.1** represents the first release number.

  For subsequent maintenance releases, this number will represent the related maintenance release number.
- **YY**—Represents the year of release.

  For the current 4.3 main release, **23** is derived from the year 2023.
- **XXXX**—The final 4 digits represent the increasing sequence of build numbers every year.

For the first 4.3 main release, the number is **0097**.

New Hardware in Release 6.0

New Hardware in Release 6.0(1.250194)

There are no new hardware features introduced for this release.

New Software in Release 6.0

New Software in Release 6.0(1.250194)

There are no new software features introduced for this release.

New Software Features in Release 6.0(1.250127)

The following new software features are supported in Release 6.0(1.250127).

- iSCSI UEFI boot support using Internet Protocol version 6 (IPv6) for Cisco UCS servers, enabling seamless integration into IPv6-capable IP networks. This addresses IPv4 limitations and offers improved scalability and management for next-generation infrastructure deployments.
- Support for KVM direct access over inband on Cisco UCS C-Series M8, M7, M6, and M5 servers, enabling administrators to securely access and manage server consoles directly over the inband network and improving operational efficiency and flexibility for Cisco UCS C-Series servers.
- On Cisco UCS M8 servers, Cisco IMC allows you to manage the SSD slot locator LED for individual drives through the Redfish API interface.

Resolved Caveats

Resolved Caveats in Release 6.0(1.250192)

The following defects were resolved in Release 6.0(1.250192):

Defect ID	Symptom	First Release Affected	Resolved in Release
CSCwi71153	In Cisco UCS M5 and M6 servers, BMC reset occurs due to watchdog reset caused by kernel scheduler null pointer dereference. In addition, kernel panic might also occur in the server. This issue is resolved.	4.2(3b)	6.0(1.250192)

Defect ID	Symptom	First Release Affected	Resolved in Release
CSCws30219	Cisco UCS M7 servers are susceptible to host lockups triggered by ECC (Error Correcting Code) memory events. This issue is specifically related to how the server BIOS interacts with the EFI (Extensible Firmware Interface) during error conditions. During these events, the BIOS does not correctly retrieve a required variable, causing EFI to return an invalid parameter. As a result, the operating system is unable to continue normal operation and freezes without logging any errors. When this occurs, the host becomes unresponsive and KVM (keyboard, video, mouse) input is not accepted. Single-bit ECC errors—while not logged due to DDR5 specifications—can trigger this condition, resulting in complete loss of host responsiveness. This issue is resolved.	4.3(6.250053)	6.0(1.250192)

Resolved Caveats in Release 6.0(1.250174)

The following defects were resolved in Release 6.0(1.250174):

Defect ID	Symptom	First Release Affected	Resolved in Release
CSCwq61388	On Cisco UCS C-Series M6 servers running Cisco IMC 4.3.5 or later, enabling VMD in BIOS with multiple NVME drives can cause storage subsystem initialization to exceed 15 minutes, leading to Intersight Server Profile deployment failures. Disabling VMD or reducing the number of drives can resolve the issue. Earlier firmware versions may not be affected.	4.3(5.250001)	6.0(1.250174)
CSCwq74490	On Cisco UCS C245 M8 platform with AMD EPYC 9655 processors, fully loaded NVIDIA L4 GPUs occasionally experience PCIe link width downgrades on random slots when running the Linux Rebooter Stress test. This can cause GPUs to operate at reduced speeds in the OS environment.	4.3(6.250053)	6.0(1.250174)
CSCwq01863	When attempting to use LDAPS authentication on a Cisco UCS C225 or C245 M8 servers with a port other than the default 636, the server will fall back to using standard LDAP methods to reach the LDAP server.	4.3(6.250044)	6.0(1.250174)

Resolved Caveats in Release 6.0(1.250131)

The following defects were resolved in Release 6.0(1.250131):

Defect ID	Symptom	First Release Affected	Resolved in Release
CSCwq58890	The firmware for the Cisco UCS VIC 15000 series adapters is updated to fix a rare, intermittently seen memory issue and to ensure more robust and consistent operation across diverse memory types and configurations. **Note** If you continue to experience any memory error, then contact Cisco TAC for support.	• 6.0(1.250130) • 6.0(1.250127)	• 6.0(1.250131)

Resolved Caveats in Release 6.0(1.250127)

The following defects were resolved in Release 6.0(1.250127):

Defect ID	Symptom	First Release Affected	Resolved in Release
CSCwn99720	On Cisco UCS C-Series M8 servers with Intel processors and an R1S CPU configured in a single-CPU setup on the 2-socket platform, Intel SGX remains disabled even after being enabled in the BIOS. This issue does not occur with a dual CPU configuration. This issue is resolved.	4.3(6.250039)	• 6.0(1.250130) • 6.0(1.250127)

Open Caveats

Open Caveats in Release 6.0(1.250192)

The following defects are open in Release 6.0(1.250192):

Defect ID	Symptom	Workaround	First Affected Release
CSCwt41941	In Cisco UCS M8 servers, the system may become stuck in the KVM console and fail to boot, accompanied by BIOS attestation failure messages. POST processes might hang or not complete, and CATERR events can be logged. NVME devices may become inoperable, and temperature sensor failures along with critical thermal threshold errors can occur. These issues arise when downgrading firmware from the following release versions to earlier releases that use SSP 1.6. • 4.3(6.260003) • 6.0(1.250192) The above release versions are integrated with SSP Protocol Version 2.0. The SSP Protocol Version 2.0 introduced in these later releases is not backward compatible with SSP 1.6, causing the BMC to fail BIOS attestation and resulting in system stability and hardware errors.	1. Upgrade only the BMC firmware component to the latest version using the Host Server Utility (HSU) or the Cisco IMC interface. 2. Perform a host reset. Performing a host reset may help recover the state, but it is not guaranteed to be 100% effective. The supported latest release versions include: • 4.3(6.260003) • 6.0(1.250192) The above release versions are integrated with SSP Protocol Version 2.0. Avoid downgrading from these versions to earlier releases that do not support SSP Protocol Version 2.0.	• 4.3(6.260003) • 6.0(1.250192)
CSCwr82017	Cisco UCS C220 M8 server and C240 M8 server will continuously reset if the Intel SGX PRMRR size is configured to an unsupported size in the system memory settings.	There is no workaround. Intel SGX is disabled, by default. When enabling Intel SGX, make sure to configure the PRMRR size to a supported value.	6.0(1.250192)

Defect ID	Symptom	Workaround	First Affected Release
CSCwr66581	In Cisco UCS C220 M8 and Cisco UCS C240 M8 servers, the following drives are not discovered by sedutil tool (for managing the SED drives) on Microsoft Windows operating system: • Samsung E3.S PM1743/PM1745 drives • Micron 7500 FIPS drives These drives are populated in the server with VMD Enabled mode.	There is no workaround.	6.0(1.250192)
CSCws37718	In Cisco UCS servers, Micron 7500 FIPS drives are listed without the 'FIPS' designation in their **Drive Description** section within the **BIOS HII** Page (path: **Advanced** > **PCI Slot Configuration** > **PCI Slot Inventory**). This results in both FIPS and non-FIPS drives having identical descriptions. For example, a drive typically described as '1.9TB 2.5in U.3 15mm Micron 7500 HgPerf MedEnd 1X NVMe FIPS' is displayed simply as '1.9TB 2.5in U.3 15mm Micron 7500 HgPerf Med End 1X NVMe'. This issue does not impact the drive's functionality.	There is no workaround.	6.0(1.250192)

Open Caveats in Release 6.0(1.250174)

The following defects are open in Release 6.0(1.250174):

Defect ID	Symptom	Workaround	First Affected Release
CSCwr78181	In Cisco UCS C240 M8 servers, when secure boot is enabled, a Secure Boot key error can arise during OS installation or during subsequent reboots.	There is no workaround.	6.0(1.250174)

Open Caveats in Release 6.0(1.250127)

The following defects are open in Release 6.0(1.250127):

Defect ID	Symptom	Workaround	First Affected Release
CSCws30219	Cisco UCS M7 servers are susceptible to host lockups triggered by ECC (Error Correcting Code) memory events. This issue is specifically related to how the server BIOS interacts with the EFI (Extensible Firmware Interface) during error conditions. During these events, the BIOS does not correctly retrieve a required variable, causing EFI to return an invalid parameter. As a result, the operating system is unable to continue normal operation and freezes without logging any errors. When this occurs, the host becomes unresponsive and KVM (keyboard, video, mouse) input is not accepted. Single-bit ECC errors—while not logged due to DDR5 specifications—can trigger this condition, resulting in complete loss of host responsiveness.	Downgrade to version 4.3(6.250044) or an earlier release.	4.3(6.250053)

Defect ID	Symptom	Workaround	First Affected Release
CSCwr10524			4.3(4.240152)

Defect ID	Symptom	Workaround	First Affected Release
	In Cisco UCS M6 servers with firmware release version 4.3(2.230207) and secure VIC 15xxx adapters, the firmware upgrade to the release versions 4.3(4.xxxxx) / 4.3(5.xxxxx) / 4.3(6.xxxxx) / 6.0(1.250127) using the HUU Web UI or NI-HUU results in BIOS activation failure. The issue occurs if any one or both of the following secure VICs are present: • Cisco UCS VIC 15235 • Cisco UCS VIC 15425 If the update is initiated through the HUU GUI, then the interface first displays a failure message regarding secure VIC activation, followed by another message to proceed with a host power cycle. After a manual host power cycle, all the component firmware are activated with the latest firmware except for BIOS. Retriggering firmware update does not help in activating the BIOS component. If the update is initiated through NI-HUU, then the script execution fails with the following error message: Error - Firmware update	You can perform any one of the following workarounds: Perform the firmware upgrade using the HSU Redfish. OR Perform a step upgrade as listed below: **1.** Upgrade from the release version 4.3(2.230207) to 4.3(2.230270) **2.** Upgrade from the release version 4.3(2.230270) to any of the following releases - • 4.3(4.xxxxx) • 4.3(5.xxxxx) • 4.3(6.xxxxx) • 6.0(1.xxxxx) OR Perform the following steps in Cisco IMC Web UI: **1.** From the **Apps** drop-down list, select **Administration**. **2.** In the **Navigation** pane, click **Firmware Management** menu. **3.** In the **Firmware Management** area, select a component from the **Component** column and click **Upload**. **4.** The **Update Firmware** dialog box	

Defect ID	Symptom	Workaround	First Affected Release
	failed because it timed out. Check host for details. After a manual host power cycle, all the component firmware are activated with the latest firmware except for BIOS. Retriggering firmware update does not help in activating the BIOS component.	appears. 5. Update the secure VIC 15xxx firmware. 6. Update the remaining components by booting HUU.	
CSCwq61388	On Cisco UCS C-Series M6 servers running Cisco IMC 4.3.5 or later, enabling VMD in BIOS with multiple NVME drives can cause storage subsystem initialization to exceed 15 minutes, leading to Intersight Server Profile deployment failures. Disabling VMD or reducing the number of drives can resolve the issue. Earlier firmware versions may not be affected.	If VMD is not needed, then disable VMD. If disabling VMD is not feasible, then use the minimum number of NVME drives for setup, as more drives slow down system startup.	4.3(5.250001)
CSCwm33093	On Microchip-based storage cards, the Virtual Drive (VD) shows as "Inoperable" even when all disks are online because the firmware automatically changes drive assignments to optimize performance, ignoring user settings from management tools.	Use **arcconf** output to check drive assignments in spans. Firmware may override management tool settings for better performance.	6.0(1.250127)

Known Behaviour and Limitations

Known Behaviors and Limitations in Release 6.0(1.250127)

The following caveats are known limitations in release 6.0(1.250127):

Defect ID	Symptom	Workaround	First Affected Release
CSCwn95239	On Cisco UCS C-series servers, the server may fail to power on due to BIOS corruption. The following message is displayed: Power on failure asserted [Power on Fail, Server failed to power-on] This issue can occur in the following scenarios, particularly when BIOS update operations are disrupted: • Interrupting a BIOS flash or update (For example: forcing a power cycle during update) • Initiating a CMOS clear operation during a BIOS update • Restoring factory defaults during BIOS update • Rebooting Cisco IMC during a BIOS update • Performing other unexpected operations that disrupt the BIOS update process	Do one of these: • Reboot Cisco IMC. • Activate the Backup BIOS. • Re-flash or update the BIOS using the latest supported firmware, and activate it.	4.3(6.250039)

Defect ID	Symptom	Workaround	First Affected Release
CSCwo68248	On Cisco UCS C220 M7 and C240 M7 servers running HUU 4.3(3.240xxx) level firmware with 2 PCIe VICs and 1 MLOM VIC, upgrading the server firmware to HUU 4.3(4.xxxxxx), 4.3(5.xxxxxx), 4.3(6.xxxxx), or later using the Redfish API interface may cause the UCS Update task to falsely report an update failure for the PCIe VIC (riser1) through which CiscoCard mode is configured. However, the firmware is actually updated and activated successfully in the background. **Note** In the mentioned HUU version numbers, "xxxx" represents all versions available within the series.	There is no workaround.	4.3(3.240043)
CSCwk83741	When the controller claims the Micron SED drivers for encryption, PSID revert is required to perform any data sanitization on them. This must be performed also to ensure that all the security ranges are cleared inside the drive.	PSID revert is required to perform any data sanitization on the SED drivers.	4.3(4.241063)

Security Fixes in Release 6.0(1)

Security Fixes in Release 6.0(1.250174)

Defect ID - CSCwq36171

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

- CVE-2025-21096—Improper buffer restrictions in the firmware for some Intel(R) TDX may allow a privileged user to potentially enable escalation of privilege via local access.
- CVE-2025-20053—Improper buffer restrictions for some Intel(R) Xeon(R) Processor firmware with SGX enabled may allow a privileged user to potentially enable escalation of privilege via local access.
- CVE-2025-24305—Insufficient control flow management in the Alias Checking Trusted Module (ACTM) firmware for some Intel(R) Xeon(R) processors may allow a privileged user to potentially enable escalation of privilege via local access.
- CVE-2025-20613—Predictable Seed in Pseudo-Random Number Generator (PRNG) in the firmware for some Intel(R) TDX may allow an authenticated user to potentially enable information disclosure via local access.
- CVE-2025-21090—Missing reference to active allocated resource for some Intel(R) Xeon(R) processors may allow an authenticated user to potentially enable denial of service via local access.
- CVE-2025-22853—Improper synchronization in the firmware for some Intel(R) TDX may allow a privileged user to potentially enable escalation of privilege via local access.

Defect ID - CSCwq36167

Cisco UCS C-Series M6 Rack Servers include an Intel CPU that is affected by the vulnerability identified by the following Common Vulnerability and Exposures (CVE) IDs:

- CVE-2025-20067—Observable timing discrepancy in firmware for some Intel(R) CSME and Intel(R) SPS may allow a privileged user to potentially enable information disclosure via local access.

Defect ID - CSCwq17911

Cisco UCS C-Series M8 Servers include an Intel CPU that is affected by the vulnerability identified by the following Common Vulnerability and Exposures (CVE) IDs:

- CVE-2025-0033—Improper access control within AMD SEV-SNP could allow an admin privileged attacker to write to the RMP during SNP initialization, potentially resulting in a loss of SEV-SNP guest memory integrity.

Supported Platforms and Release Compatibility Matrix

Supported Platforms in this Release

The following servers are supported in this release:

- Cisco UCS C220 M8

- Cisco UCS C240 M8
- Cisco UCS C225 M8
- Cisco UCS C245 M8
- Cisco UCS C220 M7
- Cisco UCS C240 M7
- Cisco UCS C220 M6
- Cisco UCS C240 M6
- Cisco UCS C245 M6
- Cisco UCS C225 M6

For information about these servers, see Overview of Servers.

Cisco IMC and Cisco UCS Manager Release Compatibility Matrix

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

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

Cisco IMC and Cisco UCS Manager Release Compatibility Matrix

Cisco UCS C-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, UCSM end-user interface is used to manage the server.

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 6.0(1) Release

Cisco IMC Release	Cisco UCS Manager Release	Rack Mount Servers
6.0(1.250194)	NA	• Cisco UCS C240 M8 servers
6.0(1.250192)	6.0(1e)	• Cisco UCS C220 M8, C240 M8, C225 M8 and C245 M8 servers • Cisco UCS C220 M7 and C240 M7 servers • Cisco UCS C220 M6, C240 M6, C225 M6 and C245 M6 servers

Cisco IMC Release	Cisco UCS Manager Release	Rack Mount Servers
6.0(1.250174)	6.0(1d)	• Cisco UCS C220 M8, C240 M8, C225 M8 and C245 M8 servers • Cisco UCS C220 M7 and C240 M7 servers • Cisco UCS C220 M6, C240 M6, C225 M6 and C245 M6 servers
6.0(1.250131)	6.0(1c)	• Cisco UCS C220 M8, C240 M8, C225 M8 and C245 M8 servers • Cisco UCS C220 M7 and C240 M7 servers • Cisco UCS C220 M6, C240 M6, C225 M6 and C245 M6 servers
6.0(1.250130)	6.0(1b)	• Cisco UCS C245 M8 servers
6.0(1.250127)		• Cisco UCS C220 M8, C225 M8 and C240 M8 servers • Cisco UCS C220 M7 and C240 M7 servers • Cisco UCS C220 M6, C240 M6, C225 M6 and C245 M6 servers

Table 2: Cisco IMC and UCS Manager Software Releases for Rack Mount Servers for Cisco IMC 4.3(6) Release

Cisco IMC Release	Cisco UCS Manager Release	Rack Mount Servers
4.3(6.2600xx)	TBD	• Cisco UCS C220 M8, C225 M8, C240 M8 and C245 M8 servers • Cisco UCS C220 M7 and C240 M7 servers • Cisco UCS C220 M6, C240 M6, C225 M6 and C245 M6 servers • Cisco UCS S3260 M5 servers

Cisco IMC Release	Cisco UCS Manager Release	Rack Mount Servers
4.3(6.260033)	TBD	• Cisco UCS C220 M8, C225 M8, C240 M8 and C245 M8 servers • Cisco UCS C220 M7 and C240 M7 servers • Cisco UCS C220 M6, C240 M6, C225 M6 and C245 M6 servers • Cisco UCS S3260 M5 servers
4.3(6.260017)	4.3(6f)	• Cisco UCS C220 M8, C225 M8, C240 M8 and C245 M8 servers • Cisco UCS C220 M7 and C240 M7 servers • Cisco UCS C220 M6, C240 M6, C225 M6 and C245 M6 servers • Cisco UCS S3260 M5 servers
4.3(6.260003)	4.3(6e)	• Cisco UCS C220 M8 and C240 M8 servers • Cisco UCS C220 M7 and C240 M7 servers
4.3(6.250117)	NA	• Cisco UCS C220 M7 servers
4.3(6.250101)	4.3(6d)	• Cisco UCS C220 M8, C225 M8, C240 M8 and C245 M8 servers • Cisco UCS C220 M7 and C240 M7 servers • Cisco UCS C220 M6, C240 M6, C225 M6 and C245 M6 servers • Cisco UCS S3260 M5 servers
4.3(6.250060)	NA	• Cisco UCS C245 M8 servers

Cisco IMC Release	Cisco UCS Manager Release	Rack Mount Servers
4.3(6.250053)	4.3(6c)	• Cisco UCS C220 M8, C225 M8, C240 M8 and C245 M8 servers • Cisco UCS C220 M7 and C240 M7 servers • Cisco UCS C220 M6, C240 M6, C225 M6 and C245 M6 servers • Cisco UCS S3260 M5 servers
4.3(6.250044)	4.3(6b)	• Cisco UCS C220 M8, C225 M8, C240 M8 and C245 M8 servers • Cisco UCS C220 M7 and C240 M7 servers
4.3(6.250039)	4.3(6a)	• Cisco UCS C220 M8 and C240 M8 servers • Cisco UCS S3260 M5 servers
4.3(6.250040)		• Cisco UCS C225 M8 and C245 M8 servers • Cisco UCS C220 M7 and C240 M7 servers • Cisco UCS C220 M6, C240 M6, C225 M6 and C245 M6 servers

Table 3: Cisco IMC and UCS Manager Software Releases for Rack Mount Servers for Cisco IMC 4.3(5) Release

Cisco IMC Release	Cisco UCS Manager Release	Rack Mount Servers
4.3(5.250045)	NA	• Cisco UCS C225 M8 servers
4.3(5.250043)	NA	• Cisco UCS C225 M8 and C245 M8 servers

Cisco IMC Release	Cisco UCS Manager Release	Rack Mount Servers
4.3(5.250033)	NA	• Cisco UCS C225 M8 and C245 M8 servers • Cisco UCS C220 M7 and C240 M7 servers • Cisco UCS C220 M6, C240 M6, C225 M6, C245 M6 servers and S3260 M5 servers
4.3(5.250030)	4.3(5d)	• Cisco UCS C225 M8 and C245 M8 servers • Cisco UCS C220 M7 and C240 M7 servers • Cisco UCS C220 M6, C240 M6, C225 M6, C245 M6 servers and S3260 M5 servers
4.3(5.250001)	4.3(5c)	• Cisco UCS C225 M8 and C245 M8 servers • Cisco UCS C220 M7 and C240 M7 servers • Cisco UCS C220 M6, C240 M6, C225 M6, C245 M6 servers and S3260 M5 servers
4.3(5.240021)	4.3(5a)	• Cisco UCS C225 M8 and C245 M8 servers • Cisco UCS C220 M7 and C240 M7 servers • Cisco UCS C220 M6, C240 M6, C225 M6, C245 M6 servers and S3260 M5 servers

Table 4: Cisco IMC and UCS Manager Software Releases for Rack Mount Servers for Cisco IMC 4.3(4) Release

Cisco IMC Release	Cisco UCS Manager Release	Rack Mount Servers
• 4.3(4.252002) • 4.3(4.252001)	NA	• 4.3(4.252002) - Cisco UCS C225 M6 servers • 4.3(4.252001) - Cisco UCS C220 M6, C240 M6 servers

Cisco IMC Release	Cisco UCS Manager Release	Rack Mount Servers
4.3(4.242066)	4.3(4f)	• Cisco UCS C220 M7 and C240 M7 servers • Cisco UCS C220 M6, C240 M6, C225 M6 and C245 M6 and S3260 M5 servers
4.3(4.242038)	NA	• Cisco UCS C220 M7 and C240 M7 servers • Cisco UCS C220 M6, C240 M6, C225 M6 and C245 M6 and S3260 M5 servers
4.3(4.242028)	NA	• Cisco UCS C220 M7 and C240 M7 servers
4.3(4.241063)	4.3(4b)	• Cisco UCS C220 M7 and C240 M7 servers • Cisco UCS C220 M6, C240 M6, C225 M6 and C245 M6 and S3260 M5 servers
4.3(4.241014)	4.3(4b)	Cisco UCS C245 M8 server
4.3(4.240152)	4.3(4a)	• Cisco UCS C220 M7 and C240 M7 servers • Cisco UCS C220 M6, C240 M6, C225 M6 and C245 M6 and S3260 M5 servers

Table 5: Cisco IMC and UCS Manager Software Releases for Rack Mount Servers for Cisco IMC 4.3(3) Release

Cisco IMC Release	Cisco UCS Manager Release	Rack Mount Servers
4.3(3.240043)	NA	• Cisco UCS C220 M7 and C240 M7 servers • Cisco UCS C220 M6, C240 M6, C225 M6 and C245 M6 servers
4.3(3.240041)	NA	• Cisco UCS S3260 M5 servers

Cisco IMC Release	Cisco UCS Manager Release	Rack Mount Servers
4.3(3.240022)	4.3(3a)	• Cisco UCS C220 M7 and C240 M7 servers • Cisco UCS C220 M6, C240 M6, C225 M6 and C245 M6 and S3260 M5 servers

Table 6: Cisco IMC and UCS Manager Software Releases for Rack Mount Servers for Cisco IMC 4.3(2) Release

Cisco IMC Release	Cisco UCS Manager Release	Rack Mount Servers
4.3(2.260007)	4.3(6f)	Cisco UCS C220 M5, C240 M5, C480 M5 and C125 M5 servers
4.3(2.250063)	NA	Cisco UCS C220 M5, C240 M5, C480 M5 and C125 M5 servers
4.3(2.250045)	NA	Cisco UCS C220 M5, C240 M5, C480 M5 and C125 M5 servers
4.3(2.250037)	4.3(6c)	Cisco UCS C220 M5, C240 M5, C480 M5 servers
4.3(2.250022)	NA	Cisco UCS C125 M5 servers
4.3(2.250021)	NA	Cisco UCS C240 M5 servers
4.3(2.250016)	NA	Cisco UCS C220 M5, C240 M5, C480 M5, C125 M5 and S3260 M5 servers
4.3(2.240107)	NA	Cisco UCS C220 M5, C240 M5, C480 M5, C125 M5 and S3260 M5 servers
4.3(2.240090)	NA	Cisco UCS C220 M5, C240 M5, C480 M5, C125 M5 and S3260 M5 servers
4.3(2.240077)	NA	Cisco UCS C220 M5, C240 M5, C480 M5, C125 M5 and S3260 M5 servers
4.3(2.240053)	NA	Cisco UCS C220 M5, C240 M5, C480 M5, C125 M5 and S3260 M5 servers
4.3(2.240037)	NA	• Cisco UCS C225 M6 and C245 M6 servers

Cisco IMC Release	Cisco UCS Manager Release	Rack Mount Servers
4.3(2.240009)	NA	• Cisco UCS C220 M6, C240 M6, C225 M6 and C245 M6 servers • Cisco UCS C220 M5, C240 M5, C480 M5, C125 M5 and S3260 M5 servers
4.3(2.240002)	4.3(2)	• Cisco UCS C220 M7 and C240 M7 servers • Cisco UCS C220 M6, C240 M6, C225 M6 and C245 M6 servers • Cisco UCS C220 M5, C240 M5, C480 M5, C125 M5 and S3260 M5 servers
4.3(2.230270)	4.3(2)	• Cisco UCS C220 M7 and C240 M7 servers • Cisco UCS C220 M6, C240 M6, C225 M6 and C245 M6 servers • Cisco UCS C220 M5, C240 M5, C480 M5, C125 M5 and S3260 M5 servers
4.3(2.230207)	4.3(2)	• Cisco UCS C220 M7 and C240 M7 servers • Cisco UCS C220 M6, C240 M6, C225 M6 and C245 M6 servers • Cisco UCS C220 M5, C240 M5, C480 M5, C125 M5 and S3260 M5 servers

Table 7: Cisco IMC and UCS Manager Software Releases for Rack Mount Servers for Cisco IMC 4.3(1) Release

Cisco IMC Release	Cisco UCS Manager Release	Rack Mount Servers
4.3(1.230138)	No Support	Cisco UCS C220 M7 and C240 M7 servers
4.3(1.230124)	No Support	Cisco UCS C220 M7 and C240 M7 servers

Cisco IMC Release	Cisco UCS Manager Release	Rack Mount Servers
4.3(1.230097)	No Support	Cisco UCS C220 M7 and C240 M7 servers

Table 8: Cisco IMC and UCS Manager Software Releases for Rack Mount Servers for Cisco IMC 4.2(3) Release

Cisco IMC Release	Cisco UCS Manager Release	Rack Mount Servers
4.2(3q)	NA	Cisco UCS C220 M6, C225 M6, C240 M6, and C245 M6 servers Cisco UCS C220 M5, C240 M5, C480 M5, S3260 M5, and C125 M5 servers
4.2(3p)	4.2(3o)	Cisco UCS C220 M6, C225 M6, C240 M6, and C245 M6 servers Cisco UCS C220 M5, C240 M5, C480 M5, S3260 M5, and C125 M5 servers
4.2(3o)	4.2(3n)	Cisco UCS C220 M6, C225 M6, C240 M6, and C245 M6 servers Cisco UCS C220 M5, C240 M5, C240 SD M5, C480 M5, C480 ML M5, S3260 M4, S3260 M5, and C125 M5 servers
4.2(3n)	4.2(3m)	Cisco UCS C220 M6, C225 M6, C240 M6, and C245 M6 servers Cisco UCS C220 M5, C240 M5, C240 SD M5, C480 M5, C480 ML M5, S3260 M4, S3260 M5, and C125 M5 servers
4.2(3m)	4.2(3l)	Cisco UCS C220 M6, C225 M6, C240 M6, and C245 M6 servers Cisco UCS C220 M5, C240 M5, C240 SD M5, C480 M5, C480 ML M5, S3260 M4, S3260 M5, and C125 M5 servers
4.2(3l)	4.2(3k)	Cisco UCS C220 M6, C225 M6, C240 M6, and C245 M6 servers Cisco UCS C220 M5, C240 M5, C240 SD M5, C480 M5, C480 ML M5, S3260 M4, S3260 M5, and C125 M5 servers

Cisco IMC Release	Cisco UCS Manager Release	Rack Mount Servers
4.2(3k)	NA	Cisco UCS S3260 M5 servers
4.2(3j)	4.2(3j)	Cisco UCS C220 M6, C225 M6, C240 M6, and C245 M6 servers Cisco UCS C220 M5, C240 M5, C240 SD M5, C480 M5, C480 ML M5, S3260 M4, S3260 M5, and C125 M5 servers
4.2(3i)	4.2(3i)	Cisco UCS C220 M6, C225 M6, C240 M6, and C245 M6 servers Cisco UCS C220 M5, C240 M5, C240 SD M5, C480 M5, C480 ML M5, S3260 M4, S3260 M5, and C125 M5 servers
4.2(3g)	4.2(3g)	Cisco UCS C220 M6, C225 M6, C240 M6, and C245 M6 servers Cisco UCS C220 M5, C240 M5, C240 SD M5, C480 M5, C480 ML M5, S3260 M4, S3260 M5, and C125 M5 servers
4.2(3e)	4.2(3e)	Cisco UCS C220 M6, C225 M6, C240 M6, and C245 M6 servers Cisco UCS C220 M5, C240 M5, C240 SD M5, C480 M5, C480 ML M5, S3260 M4, S3260 M5, and C125 M5 servers
4.2(3d)	4.2(3d)	Cisco UCS C220 M6, C225 M6, C240 M6, and C245 M6 servers Cisco UCS C220 M5, C240 M5, C240 SD M5, C480 M5, C480 ML M5, S3260 M4, S3260 M5, and C125 M5 servers
4.2(3b)	4.2(3b)	Cisco UCS C220 M6, C225 M6, C240 M6, and C245 M6 servers Cisco UCS C220 M5, C240 M5, C240 SD M5, C480 M5, C480 ML M5, S3260 M4, S3260 M5, and C125 M5 servers

Table 9: Cisco IMC and UCS Manager Software Releases for Rack Mount Servers for Cisco IMC 4.2(2) Release

Cisco IMC Release	Cisco UCS Manager Release	Rack Mount Servers
4.2(2g)	4.2(2d)	Cisco UCS C220 M6, C225 M6, C240 M6, and C245 M6 servers Cisco UCS C220 M5, C240 M5, C240 SD M5, C480 M5, C480 ML M5, S3260 M4, S3260 M5, and C125 M5 servers
4.2(2f)	4.2(2c)	Cisco UCS C220 M6, C225 M6, C240 M6, and C245 M6 servers Cisco UCS C220 M5, C240 M5, C240 SD M5, C480 M5, C480 ML M5, S3260 M4, S3260 M5, and C125 M5 servers
4.2(2a)	4.2(2a)	Cisco UCS C220 M6, C225 M6, C240 M6, and C245 M6 servers Cisco UCS C220 M5, C240 M5, C240 SD M5, C480 M5, C480 ML M5, S3260 M4, S3260 M5, and C125 M5 servers

Table 10: Cisco IMC and UCS Manager Software Releases for Rack Mount Servers for Cisco IMC 4.2(1) Release

Cisco IMC Release	Cisco UCS Manager Release	Rack Mount Servers
4.2(1j)	4.2(1n)	Cisco UCS C220 M6, C225 M6, C240 M6, and C245 M6 servers
4.2(1i)	4.2(1m)	Cisco UCS C220 M6, C225 M6, C240 M6, and C245 M6 servers
4.2(1g)	No Support	Cisco UCS C225 M6 and C245 M6 servers
4.2(1f)	4.2(1k)	Cisco UCS C220 M6, C225 M6, C240 M6, and C245 M6 servers
4.2(1e)	4.2(1i)	Cisco UCS C220 M6, C225 M6, C240 M6, and C245 M6 servers
4.2(1c)	No Support	Cisco UCS C225 M6 and C245 M6 servers
4.2(1b)	4.2(1f)	Cisco UCS C220 M6 and C240 M6 servers

Cisco IMC Release	Cisco UCS Manager Release	Rack Mount Servers
4.2(1a)	4.2(1d)	Cisco UCS C220 M6, C240 M6, and C245 M6 servers **Note** Cisco UCS Manager does not support Cisco UCS C245 M6 servers.

Table 11: Cisco IMC and UCS Manager Software Releases for Rack Mount Servers for Cisco IMC 4.1(3) Release

Cisco IMC Release	Cisco UCS Manager Release	Rack Mount Servers
4.1(3n)	NA	Cisco UCS C220 M5, C240 M5, C480 M5, S3260 M5 and S3260 M4 servers
4.1(3m)	4.1(3m)	Cisco UCS C220 M5, C240 M5, C480 M5, S3260 M5 and S3260 M4 servers
4.1(3l)	4.1(3k)	Cisco UCS C480 M5, C220 M5, C240 M5 servers
4.1(3i)	4.1(3j)	Cisco UCS C220 M5, C240 M5, C480 M5, S3260 M4, S3260 M5, C125 M5 servers
4.1(3h)	4.1(3i)	Cisco UCS C220 M5, C240 M5, C480 M5, S3260 M4, S3260 M5, C125 M5 servers
4.1(3g)	No Support	Cisco UCS S3260 M4 and S3260 M5 servers
4.1(3f)	4.1(3h)	Cisco UCS C220 M5, C240 M5, C480 M5, S3260 M4, S3260 M4, S3260 M5, and C125 M5 servers
4.1(3d)	4.1(3e)	Cisco UCS C220 M5, C240 SD M5, C240 M5, C480 M5, C480 ML M5, S3260 M4, S3260 M5, and C125 M5 servers
4.1(3c)	4.1(3d)	Cisco UCS C220 M5, C240 SD M5, C240 M5, C480 M5, C480 ML M5, S3260 M4, S3260 M5 and C125 M5 servers

Cisco IMC Release	Cisco UCS Manager Release	Rack Mount Servers
4.1(3b)	4.1(3a)	Cisco UCS C220 M5, C240 SD M5, C240 M5, C480 M5, C480 ML M5, S3260 M4, S3260 M5 and C125 M5 servers

Table 12: Cisco IMC and UCS Manager Software Releases for Rack Mount Servers for Cisco IMC 4.1(2) Release

Cisco IMC Release	Cisco UCS Manager Release	Rack Mount Servers
4.1(2m)	No Support	Cisco UCS C220 M4, C240 M4 and C460 M4 servers.
4.1(2l)	No Support	Cisco UCS C220 M4 and C240 M4 servers.
4.1(2k)	No Support	Cisco UCS C220 M4, C240 M4, and C460 M4 servers
4.1(2j)	No Support	Cisco UCS C220 M4, C240 M4, and C460 M4 servers
4.1(2h)	No Support	Cisco UCS C220 M4, C240 M4, and C460 M4 servers
4.1(2g)	No Support	Cisco UCS C220 M4, C240 M4, and C460 M4 servers
4.1(2f)	4.1(2c)	Cisco UCS C220 M5, C240 SD M5, C240 M5, C480 M5, C480 ML M5, S3260 M5, C220 M4, C240 M4, C460 M4, and S3260 M4 servers
4.1(2e)	No Support	Cisco UCS C125 M5 servers
4.1(2d)	No Support	Cisco UCS C240 M5 and C240 SD M5 servers
4.1(2b)	4.1(2b)	Cisco UCS C220 M5, C240 SD M5, C240 M5, C480 M5, C480 ML M5, S3260 M5, C125 M5, C220 M4, C240 M4, C460 M4, and S3260 M4 servers
4.1(2a)	4.1(2a)	Cisco UCS C220 M5, C240 SD M5, C240 M5, C480 M5, C480 ML M5, S3260 M5, C125 M5, C220 M4, C240 M4, C460 M4, and S3260 M4 servers

Table 13: 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

Firmware Files

Firmware Files

The C-Series software release includes the following software files:

CCO Software Type	File name(s)	Comment
Unified Computing System (UCS) Server Firmware	For release specific ISO versions, see Cisco UCS C-Series Integrated Management Controller Firmware Files, Release 6.0.	Host Upgrade Utility
Unified Computing System (UCS) Drivers	ucs-cxxx-drivers.6.0(1.250130).iso ucs-cxxx-drivers.6.0(1.250127).iso	Drivers

Unified Computing System (UCS) Utilities	ucs-cxxx-utils-efi.6.0(1.250130).iso ucs-cxxx-utils-linux.6.0(1.250130).iso ucs-cxxx-utils-vmware.6.0(1.250130).iso ucs-cxxx-utils-windows.6.0(1.250130).iso ucs-cxxx-utils-efi.6.0(1.250127).iso ucs-cxxx-utils-linux.6.0(1.250127).iso ucs-cxxx-utils-vmware.6.0(1.250127).iso ucs-cxxx-utils-windows.6.0(1.250127).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 6.0.

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
- PCI Gen5 retimer

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



Note We recommend that you use the select all and **Update** or **Update & Activate 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

Supported Hardware and Software

Operating System and Browser Requirements

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

Cisco recommends the following browsers for Cisco UCS Rack Server Software, Release 6.0(1):

Recommended Browser	Minimum Recommended Browser Version	Minimum Recommended Operating System
Google Chrome	Version 138.0.7204.169 (Official Build) (arm64)	Mac OS 15.5
	Version 138.0.7204.169 (Official Build) (64-bit)	Microsoft Windows 11 Enterprise
	Version 138.0.7204.158	Microsoft Windows 11 Enterprise
Safari	18.5 (20621.2.5.11.8)	Mac OS 15.5
Mozilla Firefox	140.0.4 (aarch64)	
	Version 140.0.4	Microsoft Windows 11 Enterprise
Microsoft Edge	Version 138.0.3351.109 (Official build) (64-bit)	
	Version 138.0.3351.95 (Official build) (64-bit	

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.

Transport Layer Security (TLS) version 1.2.

Default Ports

Following is a list of server ports and their default port numbers:

Table 14: Server Ports

Port Name	Port Number
LDAP Port 1	389
LDAP Port 2	389
LDAP Port 3	389
LDAP Port 4	3268
LDAP Port 5	3268
LDAP Port 6	3268
SSH Port	22
HTTP Port	80
HTTPS Port	443
SMTP Port	25
KVM Port	2068
Intersight Management Port	8889
Intersight Cloud Port	8888
SOL SSH Port	2400
SNMP Port	161
SNMP Traps	162
External Syslog	514

Upgrade Paths to Release 6.0

To get a complete overview of all the possible upgrade paths in Cisco IMC, see Cisco UCS Rack Server Upgrade Support Matrix.

SNMP

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

https://cisco.github.io/cisco-mibs/

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.

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:

- 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

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