Release Notes for Cisco Intersight Unified Edge eCMC Firmware Release, 6.0

© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Intersight Unified Edge eCMC Firmware Release, 6.0

Overview

Firmware upgrades in Intersight include server firmware upgrades and infrastructure firmware upgrades. Infrastructure firmware upgrades in Intersight Managed mode is supported on Cisco Unified Edge Edge Chassis Management Controller (eCMC). To manage the eCMC infrastructure firmware, see Upgrading Firmware for Unified Edge Chassis. This feature is available with a Cisco Intersight Essentials or Advanced license tier.

In Intersight, infrastructure and compute node firmware upgrades can be done independently. That is, you do not always need to upgrade infrastructure firmware to use the latest compute node firmware and vice versa. For more information on Unified Edge compute node firmware updates, refer to Release Notes for Cisco Intersight Managed Mode Server Firmware and Release Notes for Secure Router Compute Node Firmware.

Revision History

The following table shows the online change history for this document.

Date	Description
November 09, 2026	Updated release notes for Cisco Unified Edge eCMC Infrastructure firmware 6.0(2.261125). This release includes updates to: - Security fixes in Release 6.0(2.261125) - Resolved issues in Release 6.0(2.261125) - Open issues in Release 6.0(2.261125) It does not include any new hardware feature. The Cisco UCS XE-Series M8 Server Firmware release 6.0(2.261125) and Secure Router Node Firmware release 6.0(2.261099) have been released.
June 25, 2026	Updated release notes for Cisco Unified Edge eCMC Infrastructure firmware 6.0(2.260143). This release includes updates to: - Resolved issues in Release 6.0(2.260143) It does not include any new hardware feature, security fixes, or open issues.
April 23, 2026	Updated release notes for Cisco Unified Edge eCMC Infrastructure Firmware 6.0(2.260034). There is no corresponding XE Server Firmware release. This release includes fixes for issues identified internally.
March 16, 2026	Updated release notes for Cisco Unified Edge eCMC Infrastructure firmware 6.0(2.260026). This release includes updates to: - New Hardware Features in Release 6.0(2.260026) - Open issues in Release 6.0(2.260026)

© 2026 Cisco and/or its affiliates. All rights reserved.

Date	Description
	This release includes fixes for issues identified internally.
January 16, 2025	Cisco UCS XE-Series M8 6.0(1.260001) Server Firmware version has been released. There is no corresponding Unified Edge eCMC Firmware release.
December 15, 2025	Updated release notes for Cisco Unified Edge eCMC Infrastructure firmware 6.0(1.251006). This release includes updates to: - Resolved issues in Release 6.0(1.251006) It does not include any new hardware feature, security fixes, or open issues.
December 01, 2025	Updated release notes for Cisco Unified Edge eCMC Infrastructure firmware 6.0(1.251005). This release includes updates to: - New Hardware Features in Release 6.0(1.251005) - Open issues in Release 6.0(1.251005) It does not include any security fixes or resolved caveats.

New software features

Intersight software features may not align with the Intersight firmware release schedule. To know more about the latest software features, see the What's New section in Intersight Help Center.

New hardware features

New Hardware Features in Release 6.0(2.261125)

No new hardware is introduced in this release.

New Hardware Features in Release 6.0(2.260143)

No new hardware is introduced in this release.

New Hardware Features in Release 6.0(2.260034)

No new hardware is introduced in this release.

New Hardware Features in Release 6.0(2.260026)

- Support for 2400W DC power supply unit (PSU)
- Support for 25 Gigabit Ethernet (25G) on eCMC small form-factor pluggable (SFP) ports

New Hardware Features in Release 6.0(1.251006)

No new hardware is introduced in this release.

New Hardware Features in Release 6.0(1.251005)

Cisco UCS XE9305 Chassis

© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Unified Edge brings together computing, storage, routing, switching, and security into a single configurable solution to help IT organizations simplify the deployment, operations, and lifecycle management of edge infrastructure at a global scale.

The foundation of Cisco Unified Edge is the Cisco UCS XE9305 modular system. A 3RU, short-depth, multi-mountable chassis, the Cisco UCS XE9305 provides five front-facing slots that can accommodate modules (nodes) that are easy to service and adaptable to deliver a range of capabilities, from computing to storage and networking to security.

The Cisco UCS XE9305 is designed to operate in an extended range of temperatures (5° to 45° C) while maintaining a quiet noise level (40s dBA with 20% fan load at 25° C) and is protected by an optional locking bezel with an independently replaceable air filter, allowing deployments in a wide range of physical spaces and flexible mounting options. High-bandwidth inter-node connectivity is achieved through active-active 25 Gbps switches embedded on the Cisco UCS Edge Chassis Management Controller

Key Features and Benefits

- **Five slots**: 3 RU-high, 17-inch-wide, and 18-inch-deep chassis with five front-facing flexible slots for compute nodes and future modules that may include networking nodes for routing, switching, and secure access service edge (SASE) capabilities.
- **Compute node support**: Support for 1-CPU single-slot compute nodes. For more information, see Cisco UCS XE130c M8 Compute Node Data Sheet.
- **Hot-swappable controllers**: Two hot-swappable Cisco Edge Chassis Management Controllers (eCMCs), forming a unified fabric that provides connectivity between all nodes within the chassis and with upstream networks, and provides local chassis management and a secure control plane connection with Cisco Intersight.

  Each eCMC features:

  - An embedded 25 Gbps switch with 145 Gbps of switching bandwidth with five rear-facing 25 Gbps switch ports connecting to nodes within the chassis through the chassis mid-plane and two front-panel 10 Gbps SFP+ uplink ports for data traffic.
  - One front-panel 1 Gbps RJ-45 uplink port for management traffic.
  - Two front-panel USB-C ports for management console and external storage connectivity.
- **Two power supplies:** Two hot-swappable 2400W Titanium Power Supply Units (PSUs) providing N+N (Grid mode) redundancy, removable from the front for service via a latching mechanism without special tooling. Non-redundant mode is also supported.
- **Acoustically optimized fans:** Five 80 mm by 56 mm hot-swappable fan modules with acoustically optimized cooling controls, removable from both the top and the rear for service via a latching mechanism without special tooling.
- **Locking bezel:** One optional locking bezel with a separately replaceable air filter covering the entire front of the server, providing protection against physical tampering and filtration against ambient particulate matter.
- **Near Field Communication (NFC) identifier:** NFC capability embedded in the chassis to aid chassis identification, claiming, and troubleshooting when used in conjunction with the Cisco Intersight mobile app.

© 2026 Cisco and/or its affiliates. All rights reserved.

- **Multiple mounting options:** Accessories for flexible server mounting options: sliding rail kit for 4-post racks, static mount kit for 2-post racks, brackets for wall mounting, and brackets for shelf mounting (horizontally or vertically positioned).
- Fabric bandwidth:
  - Data fabric connectivity to compute nodes of 50 Gbps Ethernet speeds per compute node.
  - Modular eCMC design allows for future hardware upgrades.

For more information, see Cisco UCS XE9305 Data Sheet and Release Notes for Cisco Intersight Managed Mode Server Firmware, Release 6.0.

Security fixes

Security fixes in Release 6.0(2.261125)

Defect ID - CSCwu72986

This product includes third-party software that is affected by the vulnerabilities identified by the following Common Vulnerabilities and Exposures (CVE) IDs:

CVE ID	Description
CVE-2026-20898	Improper access control in the Alias Checking Trusted Module firmware on certain Intel Xeon processors may allow a privileged local attacker with startup-code and System Management Mode (SMM) capabilities to escalate privileges, affecting confidentiality and integrity.
CVE-2025-35973	Improper value handling in certain Intel processors within Ring 0, including the kernel, hypervisor, and bare-metal operating system, may allow a privileged local attacker to escalate privileges.
CVE-2026-20713	A control-flow implementation flaw in firmware for certain Intel Xeon processors may allow a privileged local system-software attacker to escalate privileges, potentially compromising the confidentiality and integrity of a subsequent system.
CVE-2026-20775	An uncaught exception in certain Intel Trust Domain Extensions (Intel TDX) modules may allow a privileged local attacker in a trust-domain context to cause a denial of service.
CVE-2026-20885	Improper authentication in the Intel Trust Domain Extensions (Intel TDX) module on certain Intel platforms may allow a privileged local attacker to disclose information and escalate privileges.
CVE-2026-20705	Insecure storage of sensitive information in the Intel Trust Domain Extensions (Intel TDX) module on certain Intel platforms may allow a privileged local attacker to disclose confidential data.
CVE-2025-31936	Improper handling of overlapping protected memory ranges on certain Intel Xeon 6 processors using Intel Trust Domain Extensions (Intel TDX) may allow a privileged local attacker operating in System Management Mode (SMM) to escalate privileges.
CVE-2025-31938	Insufficiently granular access controls in a subsystem of certain Intel Xeon 6 Scalable processors with Intel Trust Domain Extensions (Intel TDX) may allow an authenticated local attacker to disclose information.

© 2026 Cisco and/or its affiliates. All rights reserved.

CVE ID	Description
CVE-2025-31356	Insufficient verification of data authenticity in certain Intel Trust Domain Extensions (Intel TDX) implementations may allow a privileged local attacker in a hypervisor context to disclose information, potentially affecting confidentiality and integrity.
CVE-2026-20716	Improper access control in certain Intel processors in a Ring 3 user-application context may allow an authenticated local attacker with simple hardware capabilities to escalate privileges.

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

Security fixes in Release 6.0(2.260143)

There are no security fixes in this release.

Security fixes in Release 6.0(2.260034)

There are no security fixes in this release.

Security fixes in Release 6.0(2.260026)

There are no security fixes in this release.

Security fixes in Release 6.0(1.251006)

There are no security fixes in this release.

Security fixes in Release 6.0(1.251005)

There are no security fixes in this release.

Resolved issues

Resolved issues in Release 6.0(2.261125)

This section provides a brief description of the resolved issues.

Defect ID	Description	First Version Affected	Resolved in Release
CSCws41320	On Cisco Unified Edge chassis, rebooting an Edge Chassis Management Controller (eCMC), with or without a switch firmware upgrade, may leave a server-facing switch port down. Intersight reports a missing link on the connected server adapter port, and the affected server-facing connection remains unavailable. This issue is resolved.	6.0(1.251006)	6.0(2.261125)
CSCws97818	On Cisco Unified Edge eCMC chassis running CMC version 6.0(2.260026), a critical alarm *EquipmentChassisTempSensorReadFailure* may be reported for each installed sled. Attempts to connect to MTS/eCMC debug shell fail, and CLI commands such as connect ecmc, connect switch, and show	6.0(2.260026)	6.0(2.261125)

© 2026 Cisco and/or its affiliates. All rights reserved.

Defect ID	Description	First Version Affected	Resolved in Release
	firmware-version ecmc <local-eCMC-ID> also fail. The issue can occur at any time with no known external trigger, though it is not expected to be frequent. Cisco Intersight consistently reports the critical alarm during this failure state. Reboot the affected eCMC to clear the critical alarms and restore command functionality. This issue is resolved.		

Resolved issues in Release 6.0(2.260143)

This section provides a brief description of the resolved issues.

Defect ID	Description	First Version Affected	Resolved in Release
CSCws97818	On Unified Edge eCMC chassis running CMC version 6.0(2.260026), a critical alarm *EquipmentChassisTempSensorReadFailure* may be reported for each installed sled. Attempts to connect to MTS/eCMC debug shell fail, and CLI commands such as `connect ecmc`, `connect switch`, and `show firmware-version ecmc <local-eCMC-ID>` also fail. The issue can occur at any time with no known external trigger, though it is not expected to be frequent. Cisco Intersight consistently reports the critical alarm during this failure state. Reboot the affected eCMC to clear the critical alarms and restore command functionality. This issue is resolved.	6.0(2.260026)	6.0(2.260143)

Resolved issues in Release 6.0(2.260034)

There are no resolved issues in this release.

Resolved issues in Release 6.0(2.260026)

There are no resolved issues in this release.

Resolved issues in Release 6.0(1.251006)

This section provides a brief description of the resolved issues.

Defect ID	Description	First Version Affected	Resolved in Release
CSCws30566	Unified Edge Chassis Management Controllers may experience unexpected reboots when the MTS	6.0(1.251005)	6.0(1.251006)

© 2026 Cisco and/or its affiliates. All rights reserved.

Defect ID	Description	First Version Affected	Resolved in Release
	watchdog heartbeat times out. This is caused by mismatched polling intervals between mtsmanager and mtswdwatcher, which can result in incorrect detection of a system reset and a **NetworkInterClusterLinkStateDown** alarm in Intersight. There is no workaround for this issue. Please contact Cisco TAC for support.		

Resolved issues in Release 6.0(1.251005)

There are no resolved issues in this release.

Open issues

Open issues in Release 6.0(2.261125)

This section provides a brief description of the open issues.

Defect ID	Description	Workaround	First Version Affected
CSCww54681	On Cisco Unified Edge chassis, deployment of a Unified Edge Profile may fail when a Virtual Local Area Network (VLAN) policy contains 113 active VLANs configured across uplinks and Secure Router roles. In the reported case, the failure occurred while detaching the associated policy from the Secure Router roles, preventing the profile deployment from completing.	Reduce the number of VLANs configured for uplink switches in the VLAN policy.	6.0(2.261125)
CSCww10428	On Cisco Unified Edge chassis, host traffic on a Virtual Local Area Network (VLAN) may intermittently fail when Spanning Tree Protocol (STP) is disabled. In this state, Media Access Control (MAC) addresses are not learned on some ports, and Address Resolution Protocol (ARP) broadcast traffic is not flooded to other ports, preventing traffic from being forwarded between hosts.	Reboot the affected host. If traffic still fails, reboot the Edge Chassis Management Controller (eCMC).	6.0(2.261125)
CSCww63266	On Cisco Unified Edge chassis, untagged traffic on a native Virtual Local Area Network (VLAN) may be assigned to an incorrect queue after the active path changes from a secure-router link to an interchassis link (ICL). This occurs when class-of-service (CoS)-to-queue mappings are configured through an ingress Quality of Service (QoS) service policy. Queue mapping is correct before	There is no known workaround.	6.0(2.261125)

© 2026 Cisco and/or its affiliates. All rights reserved.

Defect ID	Description	Workaround	First Version Affected
	the path change but may become incorrect after traffic begins using the ICL. Under congestion, affected traffic may not receive the expected prioritization, which can affect latency or packet delivery.		
CSCwu60225	On a Cisco Unified Edge Chassis Management Controller (eCMC), Spanning Tree Protocol (STP) may intermittently remain disabled on a link-up port after allowed Virtual Local Area Networks (VLANs) are changed on a secure port link or uplink. The affected port does not participate in STP calculations, which can cause an incorrect STP root bridge selection and potentially create a Layer 2 loop.	Disable and then re-enable the affected ports that are in an error state.	6.0(2.261125)

Open issues in Release 6.0(2.260143)

There are no open issues in this release.

Open issues in Release 6.0(2.260034)

There are no open issues in this release.

Open issues in Release 6.0(2.260026)

This section provides a brief description of the open issues.

Defect ID	Description	Workaround	First Version Affected
CSCws97818	On Unified Edge eCMC chassis running CMC version 6.0(2.260026), a critical alarm *EquipmentChassisTempSensorReadFailure* may be reported for each installed sled. Attempts to connect to MTS/eCMC debug shell fail, and CLI commands such as `connect ecmc`, `connect switch`, and `show firmware-version ecmc <local-eCMC-ID>` also fail. The issue can occur at any time with no known external trigger, though it is not expected to be frequent. Cisco Intersight consistently reports the critical alarm during this failure state.	Reboot the affected eCMC to clear the critical alarms and restore command functionality.	6.0(2.260026)

Open issues in Release 6.0(1.251006)

There are no open issues in this release.

Open issues in Release 6.0(1.251005)

This section provides a brief description of the open issues.

© 2026 Cisco and/or its affiliates. All rights reserved.

Defect ID	Description	Workaround	First Version Affected
CSCwr78089	After replacing an eCMC (controller module hardware), the new unit does not automatically match its firmware version with the other eCMC when that unit is already connected to Intersight. This causes the two controllers to have different firmware versions, leading to a mismatch alarm in Intersight. This issue happens after replacing a single eCMC.	To fix the mismatch, upgrade the controller modules from Intersight (only the one with older software will update), or update the replaced module manually using the command-line interface (CLI), which is a text-based management tool.	6.0(1.251005)

Compatibility

Cross-Version Firmware Support

XE-Series Server Firmware Version	eCMC Infrastructure Firmware Version	
	6.0(1)	6.0(2)
6.0(2)	Yes	Yes
6.0(1)	Yes	Yes

Related resources

- Release Notes for Cisco Intersight Unified Edge Server Firmware, Release 6.0
- Release Notes for Cisco Intersight Unified Edge eCMC Infrastructure Firmware Release, 6.0
- Release Notes and Release Bundles for Unified Edge
- Managing Firmware in Unified Edge

© 2026 Cisco and/or its affiliates. All rights reserved.