Release Notes for Cisco Intersight Managed Mode Infrastructure Firmware, Release 4.2

First Published: 2023-09-26

Last Modified: 2026-08-05

Overview

Firmware upgrades in Intersight include server firmware upgrades and infrastructure firmware upgrades. Infrastructure firmware upgrades in Intersight Managed mode is supported on Cisco UCS Fabric Interconnects Series 6600, 6500, 6400, and Cisco UCS X-Series Direct Fabric Interconnects. To manage the Cisco UCS infrastructure firmware, see Upgrading Fabric Interconnect Firmware in IMM. This feature is available with a Cisco Intersight Essentials or Advanced license tier.

In Intersight, infrastructure and server firmware upgrades can be done independently. That is, you do not need to upgrade infrastructure firmware to use the latest server firmware and vice versa. For more information on compatibility between infrastructure firmware and server firmware, see Cross Version Firmware Support. For more information on server firmware updates, see Release Notes for Cisco Intersight Managed Mode Server Firmware.

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.

To view the complete matrix in PDF format, click here.

Revision History

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

Revision Date	Description
August 05, 2026	Updated release notes for Infrastructure Firmware Release 4.2(3o). This release includes updates to: • Resolved issues in Release 4.2(3o), on page 7 It does not include any new hardware support, security fixes, or open issues.
May 21, 2026	Cisco UCS X-Series 5.0(4k), B-Series 4.2(3o), and C-Series 4.2(3q) Server Firmware versions have been released. There is no corresponding Infrastructure Firmware release.

Revision Date	Description
September 23, 2025	Updated release notes for Infrastructure Firmware Release 4.2(3n). This release includes updates to: • Security Fixes in Release 4.2(3n), on page 5 It does not include any new hardware support, resolved caveats, or open caveats.
February 21, 2025	Updated release notes for Infrastructure Firmware Release 4.2(3m). This release includes updates to: • Resolved Caveats in Release 4.2(3m), on page 8 • Open Caveats in Release 4.2(3m), on page 16 It does not include any new hardware support or security fixes.
December 19, 2024	Cisco UCS X-Series 5.0(4h), B-Series 4.2(3k), and C-Series 4.2(3n) Server Firmware versions have been released. There is no corresponding Infrastructure Firmware release.
October 01, 2024	Updated release notes for Infrastructure Firmware Release 4.2(3l). This release includes updates to the security fixes and resolved caveats sections. It does not include any new hardware support or open caveats.
August 20, 2024	Updated Resolved Caveats in Release 4.2(3k).
June 17, 2024	Updated release notes for Intersight Infrastructure Firmware Release 4.2(3k).
April 17, 2024	Updated the **Cross Version Firmware Support** table.
February 22, 2024	Intersight Infrastructure Firmware Release 4.2(3j) has been released. This release includes updates to the resolved caveats section. It does not include any new hardware support, security fixes, or open caveats.
September 29, 2023	Updated release notes for Intersight Infrastructure Firmware Release 4.2(3h).
July 24, 2023	Updated release notes for Intersight Infrastructure Firmware Release 4.2(3g).
May 17, 2023	Updated release notes for Intersight Infrastructure Firmware Release 4.2(3e).
March 27, 2023	Updated release notes for Intersight Infrastructure Firmware Release 4.2(3d).
March 16, 2023	Updated release notes to include supported hardware information for every Intersight Infrastructure Firmware release.
January 20, 2023	Updated release notes for Intersight Infrastructure Firmware Release 4.2(2a) and 4.2(1n).

Revision Date	Description
January 12, 2023	Updated release notes for Intersight Infrastructure Firmware Release 4.2(3c).
January 10, 2023	Updated release notes for Intersight Infrastructure Firmware Release 4.2(3b).
August 04, 2022	Updated release notes for Intersight Infrastructure Firmware Release 4.2(2b).
February 15, 2022	Created release notes for Intersight Infrastructure Firmware Release 4.2(1l).

New Software Support

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 Features in Release

New Hardware Features in Infra Firmware Releases

New hardware support in 4.2(3o) — None

New Hardware Support in 4.2(3n) — None

New Hardware Support in 4.2(3m) — None

New Hardware Support in 4.2(3c)

Support for the following IOM in Intersight Managed Mode:

- UCS-IOM-2304
- UCS-IOM-2304V2



Note The above two IOM are supported only with Cisco UCS 6500 series Fabric Interconnect and require CMC Firmware version 4.2(2.30) or above.

For more information, see Supported Hardware for Intersight Managed Mode.

New Hardware Support in 4.2(3b)

Note

- Cisco UCS X210c M7 Compute Node requires Server Firmware Version 5.1(0.230096) and Cisco Intersight Infrastructure Firmware version 4.2(3b) or above.
- Cisco UCS C220 M7 and C240 M7 servers require Server Firmware Version 4.3(1.230097) and Cisco Intersight Infrastructure Firmware version 4.2(3b) or above.

For more information, see Supported Hardware for Intersight Managed Mode.

New Hardware Support in 4.2(2b)

Support for the following:

- Support for Cisco UCS-FI-6536 Fabric Interconnect.
- Support for Cisco UCSX-I-9108-100G Intelligent Fabric Module (IFM).
- Support for Cisco UCSX-440P PCIe Node.

For more information, see Supported Hardware for Intersight Managed Mode.

New Hardware Support in 4.2(1e)

Cisco UCS X9508 Chassis

The Cisco UCS X-Series Modular System begins with the Cisco UCS X9508 Chassis engineered to be adaptable and future ready. With a midplane-free design, I/O connectivity for the X9508 chassis is accomplished with frontloading, vertically oriented compute nodes intersecting with horizontally oriented I/O connectivity modules in the rear of the chassis. A unified Ethernet fabric is supplied with the Cisco UCS 9108 Intelligent Fabric Modules.

- 7-Rack-Unit (7RU) chassis has 8x front-facing flexible slots. These can house a combination of compute nodes and a pool of future I/O resources that may include GPU accelerators, disk storage, and nonvolatile memory.
- 2x Cisco UCS 9108 Intelligent Fabric Modules (IFMs) at the top of the chassis that connect the chassis to upstream Cisco UCS 6400 Series Fabric Interconnects. Each IFM features:
  - Up to 100 Gbps of unified fabric connectivity per compute node
  - 8x 25-Gbps SFP28 uplink ports.
- Six 2800W Power Supply Units (PSUs) provide 54V power to the chassis with N, N+1, and N+N redundancy.
- Efficient, 4x100mm, dual counter-rotating fans deliver industry-leading airflow and power efficiency.

Cross Version Firmware Support

An IMM Server firmware in a domain is supported with a specific IMM Infrastructure firmware version.

The following table shows the supported Server and Infrastructure firmware combinations within an IMM domain. Any additional Infrastructure firmware restrictions are highlighted as a note in the specific New Hardware Support section.

X-Series Server Firmware Version	Infrastructure Firmware Version		
	4.2(1)	4.2(2)	4.2(3)
5.1(1)	No	No	Yes
5.1(0)	No	No	Yes
5.0(4)	Yes	Yes	Yes
5.0(2)	Yes	Yes	Yes
5.0(1)	Yes	Yes	Yes

C-Series Server Firmware Version	Infrastructure Firmware Version		
	4.2(1)	4.2(2)	4.2(3)
4.3(1)	Yes	Yes	Yes
4.2(3)	Yes	Yes	Yes
4.2(2)	Yes	Yes	Yes
4.2(1)	Yes	Yes	Yes
4.1(3)	Yes	Yes	Yes

B-Series Server Firmware Version	Infrastructure Firmware Version		
	4.2(1)	4.2(2)	4.2(3)
5.1(0)	Yes	Yes	Yes
4.2(3)	Yes	Yes	Yes
4.2(2)	Yes	Yes	Yes
4.2(1)	Yes	Yes	Yes
4.1(3)	Yes	Yes	Yes

Security Fixes

Security fixes in Release 4.2(3o) — None

Security Fixes in Release 4.2(3n)

The following security issues are resolved:

Defect ID - CSCwm88173

Cisco NX-OS Software includes a vulnerability in the CLI identified by the following Common Vulnerability and Exposures (CVE) ID:

- **CVE-2025-20292**—A command injection vulnerability due to insufficient validation of user-supplied input allows an authenticated, local attacker with valid credentials to execute commands on the underlying operating system with non-root user privileges. Successful exploitation could allow reading and writing files limited to the attacker's account permissions.

Cisco has released software updates that address this vulnerability. There are no workarounds available. Future versions of the product will not be affected by this issue.

Defect ID - CSCwn06798 and CSCwn23023

Cisco NX-OS Software for Cisco Nexus 3000 Series Switches, Cisco Nexus 9000 Series Switches in standalone NX-OS mode, Cisco UCS 6400 Series Fabric Interconnects, Cisco UCS 6500 Series Fabric Interconnects, and Cisco UCS 9108 100G Fabric Interconnects includes Third-party Software that is affected by the vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) IDs:

- **CVE-2025-20290**—A vulnerability in the logging feature of Cisco NX-OS Software and Cisco UCS Fabric Interconnects could allow a local, authenticated attacker to access sensitive information.

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.For additional information, see the Cisco Security Advisory:Cisco NX-OS Software Sensitive Log Information Disclosure Vulnerability.

Security Fixes in Release 4.2(3m) — None

Security Fixes in Release 4.2(3l)

The following security issues are resolved:

Defect ID - CSCwk62264

Cisco Intersight includes Third-party Software that is affected by the vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) IDs:

- **CVE-2024-6387**—A race condition has been identified in the sshd service related to its signal handler. If a client fails to authenticate within the LoginGraceTime period (default is 120 seconds, previously 600 seconds in older OpenSSH versions), the sshd SIGALRM handler is triggered asynchronously. This handler, however, invokes several functions that are not safe to call from within a signal handler, such as syslog().

  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.

Defect ID - CSCwi59915

Cisco Intersight includes Third-party Software that is affected by the vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) IDs:

- **CVE-2023-48795**—The SSH transport protocol with certain OpenSSH extensions, found in OpenSSH before 9.6 and other products, allows remote attackers to bypass integrity checks, such that some packets are omitted (from the extension negotiation message), and a client and server may consequently end up

with a connection for which some security features have been downgraded or disabled, also known as Terrapin attack.

This occurs because theSSH BinaryPacketProtocol (BPP), implemented by these extensions, mishandles the handshake phase and use ofsequence numbers.For example, when there is an effective attack against SSH's use of ChaCha20-Poly1305 (and CBC with Encrypt-then-MAC), the bypass occurs in chacha20-poly1305@openssh.com, (and if CBC is used, then the -etm@openssh.com MAC algorithms).

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.

Caveats

You can view the open issues, resolved issues, and security fixes using the Cisco Bug Search Tool.

Resolved Caveats

Resolved issues in Release 4.2(3o)

The following caveats are resolved in Release 4.2(3o):

Defect ID	Description	First Version Affected	Resolved in Release
CSCwt48678	On Cisco UCS X-series chassis with UCSX-I-9108-100G Intelligent Fabric Modules (IFM), after running the factory reset command `debug platform software cmcctrl factory` to securely erase the embedded MultiMediaCard (eMMC) of an IFM, the IFM may become non-operational immediately following the reboot. When this condition occurs, the IFM becomes offline and no LED indicators are visible, but the chassis PSU and fans remain operational. There is no workaround after the IFM becomes non-operational. It is recommended to contact Cisco TAC for assistance. This issue is resolved.	Cisco UCS 6500 and 6400 Series FI: 4.2(2c)	4.2(3o)

Defect ID	Description	First Version Affected	Resolved in Release
CSCwt42965	On Cisco UCS X9508 chassis connected to Cisco Intersight Virtual Appliance, chassis profile deployment may fail when a Simple Network Management Protocol (SNMP) policy is attached to the profile. When this condition occurs, the device SNMP policy deployment fails, and the chassis profile does not fully deploy in Cisco Intersight. This issue is resolved.	Cisco UCS 6500 and 6400 Series FI: 4.2(2c)	4.2(3o)

Resolved Caveats in Release 4.2(3n) — None

Resolved Caveats in Release 4.2(3m)

The following caveats are resolved in Release 4.2(3m):

Defect ID	Description	First Version Affected	Resolved in Release
CSCwf61769	After upgrading to firmware 4.2.2c, UCS 64108 FIs encounter random SNMP OID issues: OID ".1.3.6.1.2.1.2.2.1.10.xxxxx" returns "noSuchInstance," and OID ".1.3.6.1.2.1.2.1.0" reports an incorrect value of "1." No workaround is currently available.	4.2(2c)	4.2(3m)
CSCwf63137	On UCS-FI-6454 with firmware 4.2(2c), the NGINX process intermittently crashes with signal 6, potentially causing temporary access loss. The process auto-restarts without user action. Logs capture crash details, and any inventory alerts clear automatically.	4.2(2c)	4.2(3m)

Defect ID	Description	First Version Affected	Resolved in Release
CSCwm80801	Applying the patch KB5040434 to NPS causes RADIUS login failures on Cisco UCS devices due to message authenticator verification issues. Rolling back the patch resolves the problem, and other Cisco devices are not affected.	4.2(3h)	4.2(3m)
CSCwm83085	On UCS-FI 6454 with firmware 4.3, FCoE VLAN changes for a VSAN lead to storage path disruption, while FC interfaces remain active. Connectivity is restored by flapping the FC interfaces.	4.3(4.240074)	4.2(3m)
CSCwn32035	UCS-IOM-2408 boards encounter I2C lockups, marking system fans as faulty due to prolonged SDA line holds. A driver update will extend the I2C channel hold to 5ms, aiding the unlock process and reducing permanent locks. Temporary fan reseating may help, but persistent issues might require IOM replacement.	4.3.5.240021	4.2(3m) 4.3(5.250030)

Resolved Caveats in Release 4.2(3l)

The following caveats are resolved in Release 4.2(3l):

Defect ID	Description	First Bundle Affected
CSCwk28221	When changing the FCoE VLAN from 3121 to 3120 while FI is in FC Switch mode, initiators can FLOGI and obtain FCID but fail to PLOGI to target ports, resulting in indefinite timeouts. Admin down/up of the FC link or port-channel resolves the issue. This change causes path loss in ESXi, with host logs showing successful FLOGI and FCID assignment but PLOGI timeouts.	4.3(2b)A

Defect ID	Description	First Bundle Affected
CSCwj28488	Cisco UCS server is unable to start the PNUOS because BIOS/bt/biosSecureVars/dbx_os file with an invalid certificate prevents PNUOS from operating. The dbx_os file holds certificates added by the operating system and specifies which certificates are prohibited from loading. The cause of the failure is a secure boot violation and following error message is displayed: `Invalid signature detected. Check secure boot policy in setup.`	4.3(3a)A
CSCwk47042	During migration from Cisco UCS 6300 FI Series to Cisco UCS 6500 FI Series, configuring FC storage ports results in errors, indicating that FC Breakout is not supported.	4.2(3i)A

Resolved Caveats in Release 4.2(3k)

The following caveats are resolved in Release 4.2(3k)

Defect ID	Description	First Bundle Affected
CSCwf83491	In Cisco UCSX-I-9108-25G, one I/O Fabric Module (IFM) fails to read temperature sensor data, resulting in the maximum fan speed and non-responsiveness to GUI requests. To ensure that both IFMs correctly identify their slots and come back online, reinsert IFM 2 and wait for it to come back online, then reinsert IFM 1.	4.2(3b)A
CSCwb47181	UCS Manager servers with firmware version 4.2(1f) and Cisco Custom VMWare ESXi OS are missing host inventory annotations. Some key-value pairs are either mismatched or missing in UCSM managed objects, although they are correct in the UCS Tools inventory within ESXi. To resolve this issue, manually initiate the inventory collection from Intersight.	4.2(1f)
CSCwe35644	Several ECCs are observed on a single DIMM with no fault from Cisco UCS Manager in Cisco UCS C-Series and B-Series M5 and M6 servers equipped with 64GB DIMMs (UCS-MR-X64G2RW) and ADDDC enabled.	4.1(3e)B and C
CSCwf03588	In a setup equipped with Cisco UCS 6454 FI, all the IOMs display the following fault: `Critical F1707 time-stamp 6270802 CMCLowMem : Please check the Health tab for more details`	4.2(2d)A
CSCwh65058	Cisco UCS 6454 FI operating on release 4.2(1l) might experience difficulties establishing FC (Fibre Channel) port-channels with 93180YC-FX switches that are on release 10.2(6)M. There is a possibility that the port-channel could enter an error-disabled state as soon as the links are activated.	4.2(1l)A

Defect ID	Description	First Bundle Affected
CSCwe38504	Cisco UCS 6454 FI operating on any 4.2(1) release cause a surge in CPU utilization to 100% for bladeAG, resulting in the process exhausting available memory. As a result, this prevents the peer Fabric Interconnect from being programmed during startup.	4.2(1i)A
CSCwi76042	Upon deletion of a VLAN from the VLAN group that is utilized by both Uplinks and vNICs, the vNICs momentarily lose connection, displaying an ENM Pinning failure error. The vNICs are expected to automatically restore their connection and become operational again. Cisco UCS Manager indicate the vNIC status as **down** and attribute the cause to an ENM pinning source failure.	4.2(3e)A
CSCwj10758	In Cisco UCS Manager release 4.3(3), 4.3(2), and 4.2(3), an issue has been identified where SSH logins for users authenticated through LDAP, RADIUS, or TACACS fail on Cisco UCS 6500 and 6400 series FIs, but not on Cisco UCS 6300 FIs. The SSH login succeeds if there is an active HTTP/HTTPS web session or an existing SSH session for the same user. This issue does not affect GUI or telnet logins for remotely authenticated users, nor does it impact SSH logins using local Cisco UCS Manager credentials.	4.2(3i)
CSCwj28369	Cisco UCS 6454 Fabric Interconnect experiences failures attributed to a High Availability (HA) policy reset, specifically due to Link Layer Discovery Protocol (LLDP) related issues. System logs obtained via show system reset-reason confirm that the device is automatically performing resets due to an HA policy.	4.2(3j)
CSCwd35712	A critical defect has been identified in the Cisco UCS Manager where the Data Management Engine (DME) crashes due to an **instance id not found** error. Additional symptoms include the inability to access the Cisco UCS Manager GUI, non-functionality of cluster management services, and a core dump indicated by the **show pmon state** command via SSH. The problem is not firmware-specific and can impact any Cisco UCS Manager domain. Although the data plane and server operations of the domain remain unaffected, there is no workaround for this issue, and affected environments may require restoration from a backup.	4.2(1d)

Resolved Caveats in Release 4.2(3j)

The following table lists the resolved caveats in release 4.2(3j)

Defect ID	Description	First Bundle Affected
CSCwf93621	During the ComputeRackUnitDiscover:OobStorageConfig process on Cisco UCS C240 M5SX servers, the discovery or association often failed with an error message *Remote-Invocation-Error: Waiting for storage subsystem to initialize*.This issue was observed following the server firmware upgrade to 4.2(3d) and appeared to affect servers using 3.8Tb or 7.6Tb drives.	4.2(3d)C
CSCwe96606	Cisco UCS 6454 Fabric Interconnect displayed *svc_sam_samcproxy* process failure messages.	4.2(3d)A
CSCwh86319	The Cisco UCS 6400 series and 6500 series Fabric Interconnects operating on 4.3(2.230117) version observed persistent issues of storage space exhaustion and firmware upgrade failures.	4.3(2.230117)
CSCwd15750	In a setup equipped with Cisco UCS 6454 Fabric Interconnects, reboots during auto-install, without user acknowledgement. This issue was observed during the upgrade process of the infrastructure firmware from version 4.1(3e)A to version 4.2(1i)A.	4.1(3e)A
CSCwe95417	After upgrading Cisco UCS 6332-16UP Fabric Interconnects to Infrastructure Firmware 4.2(2c)A, chassis power chart shows abnormal readings.	4.2(2c)A
CSCwe88483	Cisco UCS 6454 Fabric Interconnect crash due to Machine Check Exception (MCE) errors.	4.2(2c)A
CSCwi54393	In a setup with Linux OS, some LUNs do not get mounted when the setup is starting boot time with PXE boot along with lot of SAN LUNs.	4.1(3b)

Resolved Caveats in Release 4.2(3h)

The following caveats are resolved in Release 4.2(3h)

Defect ID	Description	First Bundle Affected
CSCwf61835	In a setup equipped with Cisco UCS 15000 Series VIC adapters and ESXi OS, the adapters may become unreachable and be in hung state. Internal PO goes down and the backplane connection link also shows as link down. All the vNICs/vHBAs are also in a down state.	4.2(2a)
CSCwf52054	Cisco UCS 2200/2300/2400 IOMs may go offline after upgrading to release 4.2(3d).	4.2(3d)
CSCwe98053	CRC errors are seen in a setup equipped with Cisco UCS 2408 IOM connected to Cisco UCS B-Series server HIF ports.	4.2(2a)
CSCwh15315	Third-party SFP goes into unsupported state after upgrading to release 4.2(2a) or later.	4.2(2a)

Defect ID	Description	First Bundle Affected
CSCwf92065	SNMP configuration does not restore in NXOS after SNMPD restart.	4.2(2c)
CSCwf73403	On a Cisco UCS 6454 Fabric Interconnect, on initial boot or after an erase configuration, the fabric interconnect did not boot to the initial configuration prompt. After finishing boot, the fabric interconnect showed a login prompt with the default hostname of switch.	4.2(3b)

Resolved Caveats in Release 4.2(3g)

The following table lists the resolved caveats in release 4.2(3g)

Defect ID	Description	First Bundle Affected
CSCwe45912	In a cluster setup with Cisco UCS 6400 series FI or 6536 FI, after a server reboot, if the MAC address is learned through the impacted FI, then the ARP is unable to resolve on any OS. This issue does not impact the servers, which are not rebooted.	4.2(1i)
CSCwf05062	Cisco UCS 6454 FI crashes and recovers due to following error: `%SYSMGR-2-SERVICE_CRASHED: Service "mfdm" (PID 15518) hasn't caught signal 6 (core will be saved). %$ VDC-1 %$ %SYSMGR-2-HAP_FAILURE_SUP_RESET: Service "mfdm" in vdc 1 has had a hap failure`	4.2(1d)
CSCwf44680	In a setup equipped with Cisco UCS 6454 FI, when IP Unicast/Subnet-broadcast packet destined to Link-Layer broadcast is received over Mgmt port of FI, the packet is routed over Mgmt0 Interface. This results in FI sending back the received packet with the Mgmt0 source MAC address leading to upstream device on the network detecting the same destination IP address with a different source MAC address.	4.2(3e)

Resolved Caveats in Release 4.2(3e)

The following table lists the resolved caveats in release 4.2(3e)

Defect ID	Description	First Bundle Affected
CSCwe07549	iSCSI LUN discovery fails for servers in Intersight Managed Mode with CHAP Authentication enabled. A X210c M6 Compute Node was configured with iSCSI profile with Challenge Handshake Authentication Protocol (CHAP) authentication enabled. On rebooting the server, iSCSI boot LUN in BIOS is not found. Even though CHAP is enabled in iSCSI boot profile of Intersight from BIOS in iSCSI configuration, it is observed that Authentication mode appears as none.	4.2(1l)

Resolved Caveats in Release 4.2(3d)

The following table lists the resolved caveats in release 4.2(3d)

Defect ID	Description	First Bundle Affected
CSCwd41247	Multiple instances of hung **Samcproxy** is observed in a setup equipped with Cisco UCS 6400 FI. There may also be other miscellaneous faults on the domain related to **Samcproxy** being in a bad state.	4.2(3c)
CSCwe24011	Unexpected reboot is observed during normal operation in Cisco UCS 6536 FI and Cisco UCS 6400 FI series FIs.	4.2(3c)

CSCwd90187	In a setup equipped with Cisco UCS 6536 FI, port goes to **Link not connected** status when QSFP-100G-DR/FR-S is replaced with QSFP-100G-CUxM under the following conditions:
	• 100G interface
	  • Interface is configured with **FEC Auto**
	  • Interface was using QSFP-100G-FR, QSFP-100G-DR transceivers Interface now uses QSFP-100G-CUxM, where CUxM refers to CU1M, CU2M, and so on.
		4.2(3c)

CSCwe28336	MTS buffer stuck on vsh.bin process. The process crashes and impacts other functionality once the limit is reached.	4.2(3c)
CSCwe28336	In a setup equipped with Cisco UCS 6400 FI, Multicast streams are not accepted by the server.	4.2(3c)

Resolved Caveats in Release 4.2(3c)

The following table lists the resolved caveats in release 4.2(3c)

Defect ID	Description	First Bundle Affected
CSCwd86029	While upgrading the Infrastructure firmware from 4.2(1d) to 4.2(2a), 4.2(3b), or 4.2(3c) release, if there is a time lag between two IFM upgrades, Redfish query fails on one of the IFM during this time interval. It may be seen as a connection failure in IMM.	4.2(2c)

Resolved Caveats in Release 4.2(3b)

The following table lists the resolved caveats in release 4.2(3b)

Defect ID	Description	First Bundle Affected
CSCwd37309	In a UCS X-Series Chassis, using the fan UCSX-9508-FAN, an alert is seen stating "[Chassis fan module] has a critical speed threshold condition". This behavior may be seen on multiple chassis and may occur on different fan modules. A fault gets raised and then gets cleared on its own. The issue is observed during LOW fan speed conditions. If the fault persists and does not clear on its own, physically re-seat the fan. If the fault persists even after re-seating, reach out to Cisco TAC as it could potentially indicate a separate problem.	4.2(1l)

Resolved Caveats in Release 4.2(2d)

The following table lists the resolved caveats in release 4.2(2d)

Defect ID	Description	First Bundle Affected
CSCwd37309	In a UCS X-Series Chassis, using the fan UCSX-9508-FAN, an alert is seen stating "[Chassis fan module] has a critical speed threshold condition". This behavior may be seen on multiple chassis and may occur on different fan modules. A fault gets raised and then gets cleared on its own. The issue is observed during LOW fan speed conditions. If the fault persists and does not clear on its own, physically re-seat the fan. If the fault persists even after re-seating, reach out to Cisco TAC as it could potentially indicate a separate problem.	4.2(1l)

Resolved Caveats in Release 4.2(1n)

The following table lists the resolved caveats in release 4.2(1n)

Defect ID	Description	First Bundle Affected
CSCwb90201	In Cisco UCS 6500 Series FI, extra member port in uplink port fails to forward the broadcast traffic. This happens because the Fibre Channel over Ethernet (FCoE) member port gets incorrectly included in the uplink port.	4.2(1l)

Defect ID	Description	First Bundle Affected
CSCwb00770	In Cisco UCS 6500 Series FI, the fabric port fails to forward the unicast traffic in the UDP port range 100-150	4.2(1l)
CSCwb43580	FI switch link with QSFP-40G-LR4 status appears as Up for more than a minute even after shutting the remote end port or pulling the cable. FI switch is connected to C-Series server with Cisco 1400 Series adapter.	4.2(1l)
CSCwb07198	For Cisco UCS 6500 Series FI, IGMP 16k limit notification is seen on Syslog even on sending only one igmp join from Appliance server to FI.	4.2(1l)
CSCwb73274	A convergence time of more than 100 sec is observed for IP multicast traffic during fabric failover. This is observed when 3K VLAN on FI and N9K with Snoop Enabled are configured on all VLAN. More than 5 querier are configured on N9K on different VLANs. Three groups are joined on different VLAN from different Host/Servers.	4.2(1l)
CSCwb78536	Fiber Channel Storage port is stuck at Init after FI reboot. The port is connected to 32G Netapp and FCoE traffic is sent to it before the reboot of Fabric Interconnect B.	4.2(1l)
CSCwb64509	snmpd_log core is affected when FI is rebooted after enabling FC uplink port and breakout interfaces.	4.2(1l)

Resolved Caveats in Release 4.2(1l)

The following table lists the resolved caveats in release 4.2(1l)

Defect ID	Description	First Bundle Affected
CSCvz92352	The Intelligent Fabric Management (IFM) experiences reboot loop due to a faulty Power Supply Unit in the chassis. A faulty PSU is indicated by non solid green PSU LED.	4.2(2a)

Open Caveats

Open issues in Release 4.2(3o) — None

Open Caveats in Release 4.2(3n) — None

Open Caveats in Release 4.2(3m)

The following caveats are open in Release 4.2(3m):

Defect ID	Symptom	Workaround	First Version Affected
CSCwn65484	The Fabric Interconnect (FI) logs a warning about the missing FCOE_NPV_PKG license, but the FCoE feature continues to operate normally under honor-based licensing.	There is no workaround.	4.3(3a)

Open Caveats in Release 4.2(3l) — None

Open Caveats in Release 4.2(3k) — None

Open Caveats in Release 4.2(3c)

The following caveats are open in Release 4.2(3c):

Defect ID	Symptom	Workaround	First Bundle Affected
CSCwd52370	After upgrading the firmware of the Fabric Interconnect in UCSB-5108-AC2 chassis with UCS-IOM-2408, connection to Intersight is lost. Port flaps cause the CMC to unset its chassis information, which removes the useful information from /var/isconfig. When chassis info is again set, the CMC DC may not re-read the /var/isconfig file after it is again populated with its data, causing the CMC to be disconnected from Intersight.	Restart CMC DC (/etc/init.d/dc restart)	4.2(2c)

Open Caveats in Release 4.2(2a)

The following caveats are open in Release 4.2(2a):

Defect ID	Symptom	Workaround	First Bundle Affected
CSCwd82136	In a setup equipped with Cisco UCS 6400 series FI connected to Cisco UCS C-Series servers using Cisco VIC 1457/1455/1467, ports on the FI may go to error-disabled state with **errDisabledExcessportIn** reason after a link flap.	Flap the FI port connected to the Cisco UCS C-Series servers.	4.2(2a)
CSCwd90187	In a setup equipped with Cisco UCS 6536 FI, port goes to **Link not connected** status when QSFP-100G-DR/FR-S is replaced with QSFP-100G-CUxM under the following conditions: • 100G interface • Interface is configured with **FEC Auto** • Interface was using QSFP-100G-FR, QSFP-100G-DR transceivers Interface now uses QSFP-100G-CUxM, where CUxM refers to CU1M, CU2M, and so on.	There are two workarounds for this issue: • Perform the following steps: 1. Insert an optic or AOC transceiver that does not have FEC capability. For example, QSFP-100G-SR or QSFP-100G-AOC3M on the interface. 2. Remove the transceiver in Step 1. 3. Re-insert passive copper cable. • Reboot the FI.	4.2(2a)

Related Documentation

Release Notes

- Release Notes and Release Bundles for Cisco Intersight
- Release Notes for Cisco UCS Manager
- Release Notes for Cisco Integrated Management Controller