Cisco MDS 9000 Series Release Notes

Release 9.4(5)

Contents

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

Cisco MDS 9000 Series Switches, Release 9.4(5)

This document describes the features, issues, and deployment guidelines for the Cisco MDS NX-OS software for use on the Cisco MDS 9000 Series Switches.

The Cisco MDS 9000 Series of Multilayer Directors provide best-in-class high availability, scalability, security, and management that enables you to deploy high-performance storage area networks. Layering a rich set of intelligent features onto a high-performance switch fabric, the Cisco MDS 9000 Series has the flexibility to fit small deployments and to address the stringent requirements of large data center storage environments: high availability, security, scalability, sustainability, ease of management, and seamless integration of new technologies.

Note: Release notes are updated on an as needed basis with new information on restrictions and issues.

See the following website for the most recent version of the Cisco MDS 9000 Series Release Notes: https://www.cisco.com/c/en/us/support/storage-networking/mds-9000-nx-os-san-os-software/products-release-notes-list.html.

Date	Description
March 4, 2026	Initial Release

About software images

The Cisco MDS NX-OS operating system is shipped with the Cisco MDS 9000 Series Switches. The Cisco MDS NX-OS software consists of two images: the kickstart image and the system image. These images can be upgraded or downgraded to different versions. The versions of both images must match for the system to boot.

Each model of the Cisco MDS switch has unique kickstart and system images. To download the new Cisco MDS 9000 Series Switches NX-OS software, go to the Storage Networking Software download website at https://software.cisco.com/download/find/MDS.

Upgrade and downgrade paths

Cisco MDS NX-OS Release 9.4(5) supports non-disruptive upgrade and downgrade to other Cisco MDS NX-OS Releases. For upgrade and downgrade paths, and guidelines that are recommended for upgrading or downgrading Cisco MDS NX-OS software images, see Cisco MDS 9000 NX-OS Software Upgrade and Downgrade Guide, Release 9.x.

About firmware images

Cisco MDS 9000 Series Switches contain a number of hardware components with updatable firmware. The Transceiver Firmware bundle contains updates for various port transceivers. The EPLD Firmware bundle contains updates for programmable logic devices in the system.

These updates can be disruptive and so are not part of the Cisco NX-OS software image. They are released with every Cisco NX-OS release but do not frequently contain changes. Refer to the specific Release Notes for any recommended versions.

For more information on Transceiver Firmware, see the Cisco MDS 9000 Series Transceiver Firmware Release Notes, Release 9.4(5).

For more information on EPLD bundles, see the Cisco MDS 9000 Series EPLD Release Notes, Release 9.4(5).

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

Components supported

For information on supported software and hardware components, see Cisco MDS 9000 Series Compatibility Matrix.

IBM FICON qualification status

Cisco MDS NX-OS Release 9.4(5) is not IBM FICON qualified.

Cisco TrustSec FC Link encryption

For more information about which set of interfaces on each module support Trustsec FC link encryption, see the Configuring Cisco TrustSec Fibre Channel Link Encryption chapter of the *Cisco MDS 9000 Series Security Configuration Guide, Release 9.x*.

New software features

Product Impact	Feature	Description
Feature Set	Transmit FC abort counter	Support has been introduced for per-interface transmit FC Abort Sequence (ABTS) frame counters. This allows monitoring of health and performance of Cisco MDS FC fabrics. For more information, refer to *Cisco MDS 9000 Series Interfaces Configuration Guide, Release 9.x*.
	Link Negotiation Early Training Complete	Support has been introduced for enhanced Fibre Channel link negotiation capability for simultaneous TC signaling and LSN completion during Fibre Channel link negotiation at 32 Gbps to interoperate with non-compliant devices. For more information, refer to *Cisco MDS 9000 Series Interfaces Configuration Guide, Release 9.x*.
	System Health	Support has been introduced for new error counters by default in Fabric Module Error Monitoring feature. They are the "HIGH_NULL_POE_DROP_CNT" counter for Fabric 1 Modules and the "null FPOE port" counter for Fabric 3 Modules. The default error threshold has been changed from 50 to 10 errors per monitoring interval. For more information, see *Cisco MDS 9000 High Availability Configuration Guide, Release 9.x*.
	Congestion Isolation for non FPIN devices	Support has been introduced to move congesting flows for devices that have not registered for FPINs instead into the slow virtual lane at ISLs on adjacent switches. This is an enhancement in both Port Monitor (PMon) and Smart Monitoring and Alerting (SMA) of the portguard FPIN action for the tx-overutilization counter. For more information, refer to *Cisco MDS 9000 Series Interfaces Configuration Guide, Release 9.x*.
	Peer notification when FPM is disabled	Support has been introduced for the switches to notify all registered hosts when FPM is disabled. For more information, refer to *Cisco MDS 9000 Series Fabric Configuration Guide, Release 9.x*.

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

Product Impact	Feature	Description
	FPIN without PLOGI	Support has been introduced to send FPIN notifications to the target port by the Fabric Controller even if PLOGI (Port Login) has not occurred. For more information, refer to *Cisco MDS 9000 Series Fabric Configuration Guide, Release 9.x*.
	PMON tx-overutilization counter support for NPV mode	Support has been introduced for tx-overutilization counter in NPV mode. For more information, refer to *Cisco MDS 9000 Series Interfaces Configuration Guide, Release 9.x*.
	Test SMA	Support has been introduced for generating test syslogs and SNMP traps for SMA. This allows testing of remote automation that processes these alerts. For more information, refer to *Cisco MDS 9000 Series Interfaces Configuration Guide, Release 9.x*.
Security	AAA	Support has been introduced for user authentication by OAuth2/OIDC. This enhances switch access security by integrating with centralized identity providers and supporting MFA and SSO. For more information, refer to *Cisco MDS 9000 Series Security Configuration Guide, Release 9.x*.
	PKI Certificate Management	Support has been introduced for Enrollment over Secure Transport (EST) X.509 certificate management. This allows secure and automated certificate provisioning and renewal on switches. For more information, refer to *Cisco MDS 9000 Series Security Configuration Guide, Release 9.x*.
	TACACS	Support has been introduced for CFS distribution of TACACS over TLS configuration. For more information, refer to *Cisco MDS 9000 Series Security Configuration Guide, Release 9.x*.

New hardware features

There are no new hardware features in Cisco MDS NX-OS Release 9.4(5).

Behavior changes

The mechanism of upgrading Fabric Switches has been changed. This makes Cisco NX-OS software updates more reliable. When a Cisco NX-OS update includes a Supervisor BIOS update then the Supervisor CPU now will need to be reset for the new BIOS version to be used by the CPU.

For 32 Gbps Fabric Switches the reset is disruptive and the option exists to do so at the time of the Cisco NX-OS update or later.

For deployed 64 Gbps Fabric Switches, a one-time disruptive EPLD update is required to make future CPU resets nondisruptive. For 64 Gbps Fabric Switches shipped with MDS Release 9.4(5) or later preinstalled, the EPLD update will already be installed and no user action is required.

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

For more information, refer to *Cisco MDS 9000 NX-OS Software and Firmware Upgrade and Downgrade Guide, Release 9.x*.

Resolved issues

Severity 1 (Catastrophic) issues

Bug ID	Headline	Known Impacted Releases
CSCws09730	Fabric Switches reboot after the mgmt0 interface link goes down.	9.4(4)

Severity 2 (Severe) issues

Bug ID	Headline	Known Impacted Releases
CSCvz09012	End devices encounter errors or do not respond after MDS Fabric switch ISSU	8.4(1a), 8.4(1)
CSCwp10980	A 32 Gbps Fabric switch hangs during nondisruptive reload or upgrade	9.4(1) 9.3(1) 9.2(1) 8.5(1), 8.4(1), 8.3(1), 8.2(1), 8.1(1)
CSCwq59485	'nginx_f' process crash on MDS switch	9.4(2a)
CSCwq70630	sm15_usd service crash with signal 6 on 32 Gbps linecard after hardware failure	8.4(2a)
CSCwq74784	Random rlir service crash with type signal 6 after thousands of link flaps in fabric	8.4(2d)
CSCwr10710	Configuring Callhome Destination Profile "short_txt" with format "XML" may result in switch crash	8.4(2f)
CSCwr78631	Devices unable to communicate over an F Port-Channel after a supervisor switchover	9.4(2a) 8.4(1a)
CSCws34408	32 Gbps fabric switches: change ISSU reload behavior and add 'disruptive' option to 'install all' command	8.4(2f)
CSCws52730	FC-SP Authentication Failure During ISSU	9.4(3b)
CSCws59983	Random end devices on an F port lose connectivity	9.4(2a)

Severity 3 (Moderate) issues

Bug ID	Headline	Known Impacted Releases
CSCwo33652	IOA interface goes down after after IPS goes into (Port software failure) state	9.4(1a)
CSCwq37276	'fpm' service crash when invalid words crosses rising or falling threshold	9.3(2a)

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

Bug ID	Headline	Known Impacted Releases
CSCwq42523	'licmgr' service crashes after 345 days with signal 6	9.4(2a) 9.4(1a)
CSCwq48366	'pixm_vl' service crash following many flaps of port channel members	9.4(2a)
CSCwq54982	SNMP service crash with type 'signal 6'	9.4(1), 9.3(1), 9.2(1) 8.4(1)
CSCwq70809	MDS fabric switch hangs after reboot by a system panic	9.3(2a)
CSCwq74996	Device Manager 12.2.2.15 authentication fails with unknown snmp user with remote authentication	9.4(2a)
CSCwq83432	Xbar internal disparity errors not logged to OBFL	9.4(2a)
CSCwq86568	TCAM write failure, zone switches to 'soft' mode due to duplicate entries	9.4(4), 9.4(3a)
CSCwr22545	External Port Loopback test fails on all MDS platforms	9.4(4)
CSCwr46750	The message " LICMGR-2-LOG_LIC_AUTH_MISSING_WARNING: An authorization code is not installed for the enabled ports" is logged every 7 days	9.4(2a)
CSCwr85084	Inconsistent Sensor Naming Between entPhysicalDescr and entity_sensor OIDs	9.4(2a)
CSCwr98019	MDS rmon Falling alarm occur incorrectly even though didn't reach falling-threshold	9.4(2a)
CSCws33340	acltcam process crashed during zone member addition after ISSU from 842d to 945	

Severity 4 (Minor) issues

Bug ID	Headline	Known Impacted Releases
CSCwq27256	'clear logging onboard txwait' also clears unrelated OBFL logs	9.4(4), 9.4(3a), 9.4(2a), 9.4(1a), 9.4(1) 9.3(2a) 9.2(1a), 9.2(1)
CSCws09946	Continuous " ERROR: I2C Nack" messages every three seconds	8.4(2d)
CSCws44964	'show tech-support xbar' missing instance 0 driver_info commands	9.4(4)
CSCws45134	tac-pac filename not cross-platfom compatible	

Severity 6 (Enhancement) issues

Bug ID	Headline	Known Impacted Releases
CSCwm35450	Standby supervisor CPU MAC logs not collected in 'show tech-support details'	9.4(2)

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

Bug ID	Headline	Known Impacted Releases
CSCwo55010	make early tc=1 debug for noncompliant 32 gbps links into a supported configuration command	
CSCwo81224	Add fabric module channel info to 'show tech-support xbar'	9.4(3a)
CSCwq08076	Enhance showanalytics to better evaluate system resources involved with a deployment	9.4(2a)
CSCwq38481	Add NULL_POE monitoring to xBarErrorMonitor	9.4(3b)
CSCwq56537	Update 'factory-reset' warning message	9.4(3b)
CSCwq90146	Create the equivalent of OID zoneEnforcedZoneSetActivateTime in seconds	9.4(4)

Open issues

Severity 3 (Moderate) issues

Bug ID	Headline	Known Impacted Releases
CSCwo81317	False SMA alarm or warning syslogs triggered for counters after policy activation	9.4(5) 9.4(4)
CSCwq13412	Duplicate warnings and alarms for tx-overutilization and txwait SMA counters	9.4(5) 9.4(4)
CSCwr75319	Some SMA counters are assigned incorrect action groups when configured with action group ag-default	9.4(5)
CSCws76238	An overutilized device is not isolated after ISSU from MDS NX-OS 9.4(4) to 9.4(5)	9.4(5)
CSCwt04973	'show fcs ie' + 'show topology' commands show wrong IP address of remote switch, NDFC unable to discover/manage switch	9.4(5)
CSCwt15775	Restoration of missing WKA ACL entries for the F-Port Channel during switchover or ISSU	9.4(5)
CSCwt23512	IVR zone configurations failing after ISSU	9.4(5)
CSCwt26267	Receiving HMRFPO_MERESET_CMD_ID response – timeout error during BIOS upgrade on apex switches.	9.4(5)

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

Severity 4 (Minor) issues

Bug ID	Headline	Known Impacted Releases
CSCvv00538	Remove misleading ficon stat 'merge failed' message in non-FICON VSAN	9.4(5) 9.4(4) 9.4(3b), 9.4(3a), 9.4(3), 9.4(2a), 9.4(2), 9.4(1a) 8.5(1) 8.4(2b), 8.4(2c), 8.4(2d), 8.4(2e)
CSCwc61263	Linecard fails to boot up with '%PORT-5-MODULE_BRINGUP_NOT_ALLOWED' error	9.4(5) 9.4(4) 9.4(3b), 9.4(3a), 9.4(3), 9.4(2a), 9.4(2), 9.4(1a) 8.4(2e), 8.4(2c) 8.1(1)
CSCwk33644	Power Supply status of " Powered-dn" causes Amber System Status LED	9.4(5) 9.4(4) 9.4(3b), 9.4(3a), 9.4(3), 9.4(2a), 9.4(2), 9.4(1a), 9.4(1)

Severity 6 (Enhancement) issues

Bug ID	Headline	Known Impacted Releases
CSCvw77444	Need to automatically sync bootflash:/scripts directory between active and standby sups	9.4(5) 9.4(4) 9.4(3b), 9.4(3a), 9.4(3), 9.4(2a), 9.4(2), 9.4(1a), 9.4(1) 8.1(1a)
CSCvx37657	Need to save nonvolatile logs about BIOS programming errors	9.4(5) 9.4(4) 9.4(3b), 9.4(3a), 9.4(3), 9.4(2a), 9.4(2), 9.4(1a) 8.5(1) 8.4(2c), 8.4(2d), 8.4(2e) 8.3(2)

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

Bug ID	Headline	Known Impacted Releases
CSCwb13413	A fabric module with a faulty link to a linecard is not powered down	9.4(5) 9.4(4) 9.4(3b), 9.4(3a), 9.4(3), 9.4(2a), 9.4(2), 9.4(1a) 8.4(1)
CSCwe86920	Add option to 'show tech-support' to exclude and include subcommands	9.4(5) 9.4(4) 9.4(3b), 9.4(3a), 9.4(3), 9.4(2a), 9.4(2), 9.4(1a), 9.4(1) 8.1(1)
CSCwf66251	Need a syslog warning when number of zone members exceeds maximum supported	9.4(5) 9.4(4) 9.4(3b), 9.4(3a), 9.4(3), 9.4(2a), 9.4(2), 9.4(1a) 8.4(2d)

Unsupported features

MD5 hash in FCSP

Cisco MDS NX-OS Release 9.4(2) and later releases do not support the MD5 hash algorithm in Fibre Channel Security Protocol (FC-SP) as it is no longer considered secure. The default hash algorithm has been changed to SHA1.

10G and 40G FCoE linecards

Cisco MDS NX-OS Release 9.4(2) and later releases do not support the following FCoE linecards:

- DS-X9848-480K9 – 48-port 10-Gbps FCoE Switching Module
- DS-X9824-960K9 – MDS 9700 24-port 40-Gbps FCoE Switching Module

For more information, see the Cisco MDS 9700 Series Multilayer Directors Hardware Installation Guide.

SDV feature

Cisco MDS NX-OS Release 9.3(2) and later releases do not support Cisco SAN device virtualization (SDV).

Traditional and smart licensing version 1.0 licenses

Cisco MDS NX-OS Release 9.2(2) and later releases does not support installation of Product Authorization Key (PAK) or Smart Licensing version 1.0 licenses. Licenses are now managed through Smart License using Policy (SLP).

For more information such as how to migrate licenses, see Smart Licensing Using Policy chapter in *Cisco MDS 9000 Series Licensing Guide, Release 9.x*.

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

Python 2

Support for Python 2 is deprecated from Cisco MDS NX-OS Release 9.2(2). Python 3 remains supported instead. Python 2 scripts should be checked for compatibility with Python 3 to ensure they continue to function as expected.

For more information, see the Python API chapter in the *Cisco MDS 9000 Series Programmability Guide, Release 9.x*.

Zoning features

LUN zoning, read-only zones, and broadcast zones are no longer supported.

If these features are already configured, completely remove all the configurations that include these features before attempting to boot any module. In addition, you cannot configure these features after you bring up any module.

XRC acceleration license

From Cisco MDS NX-OS Release 8.1(1a), the Cisco Extended Remote Copy (XRC) acceleration license is obsoleted on Cisco MDS 9000 Series Switches due to improvements in the mainframe XRC feature.

Virtual Router Redundancy Protocol (VRRP)

Cisco MDS NX-OS Release 8.3(1) and later releases do not support the VRRP feature on Cisco MDS 9000 Series Switches.

Data Encryption Standard (DES) for SNMP

From Cisco MDS NX-OS Release 8.5(1), AES-128 is the default encryption mechanism for SNMPv3. DES encryption for SNMP is supported only for DES users who upgrade from previous releases to Cisco MDS NX-OS Release 8.5(1). Ensure that you delete all the SNMPv3 users configured with DES encryption before upgrading to Cisco MDS NX-OS Release 8.5(1) and later releases. Any downgrades from Cisco MDS NX-OS Release 8.5(1) will be restricted if any of the SNMPv3 users have DES encryption configured as the privacy protocol. All such users will either need to be deleted or reconfigured to use no privacy protocol or AES128 encryption before downgrading.

For more information, see *Cisco MDS 9000 Series System Management Configuration Guide, Release 9.x*.

Fabric Performance Impact Notifications (FPIN)

FPIN is not supported on switches that are operating in NPV mode.

FCWA, XRC, DMM, SME

Cisco MDS NX-OS Release 8.1(1) and later releases do not support FCWA, XRC, DMM and SME features.

SAN extension tuner

SAN Extension Tuner (SET) is not supported on Cisco MDS 9220i switches in Cisco MDS NX-OS Release 8.5(1) or later.

Fibre channel read diagnostic parameters

Fibre Channel RDP querying is not supported on NP, Port Channel, or FCoE links.

Slow drain detection and congestion isolation

ER_RDY is not supported on FC interfaces running at 10 Gbps.

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

FCIP support

- In Cisco MDS NX-OS Release 9.2(2) and later releases, simultaneous use of IVR and FCIP Write Acceleration features is not supported on FCIP tunnels configured on Cisco MDS 9700 Director switches.
- On Cisco MDS 24/10 Port SAN Extension Module, configuring multiple FSPF equal cost paths (ECMP) via port channels or non-port channel interfaces with FCIP members in the same VSAN is not a valid configuration. If this is configured, then the traffic flows through only one of the port channels or non-port channel interfaces.

iSCSI support

iSCSI is not supported on Cisco MDS 9700 Directors with Cisco MDS 24/10 port SAN Extension Modules and Cisco MDS 9220i multiservice fabric switch.

Related resources

The documentation set for the Cisco MDS 9000 Series includes the documents that are listed in this section. To find a document online, access the following URL:

https://www.cisco.com/en/US/products/ps5989/tsd_products_support_series_home.html

Release Notes

https://www.cisco.com/c/en/us/support/storage-networking/mds-9000-nx-os-san-os-software/products-release-notes-list.html

Documentation Suite

https://www.cisco.com/c/en/us/td/docs/storage/san_switches/mds9000/roadmaps/rel90.html

Statement of Volatility

https://trustportal.cisco.com/c/r/ctp/trust-portal.html?search_keyword=mds%209000&solutioncategory=Data%20Center#/1646059028492371

Cisco Nexus Dashboard Fabric Controller (Formerly DCNM)

https://www.cisco.com/en/US/products/ps9369/tsd_products_support_series_home.html

Legal information

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2026 Cisco Systems, Inc. All rights reserved.