Cisco MDS NX-OS Release Notes, 9.4(5a)

Contents

Cisco MDS NX-OS 9.4(5a) 3
IBM FICON Qualification Status 5
New/Enhanced software features 5
New hardware features 6
Behavior changes 6
Resolved issues 6
Open issues 9
Unsupported features 10
Related resources 12
Legal information 12

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

Cisco MDS NX-OS 9.4(5a)

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 Fibre Channel switches and 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
September 01, 2026	Initial Release

About NX-OS 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.

About BIOS updates

Many Cisco MDS 9000 Series switches and modules contain a CPU supported by BIOS (Basic Input/Output System) firmware. The BIOS initializes hardware during the boot process, performs the POST (Power-On Self-Test) and provides the low-level foundation to load the Cisco NX-OS operating system. BIOS updates are contained within the system image, and the installed BIOS is updated, if needed, automatically as part of the ISSU process. The following table lists the BIOS versions in Cisco MDS NX-OS 9.4(5a).

MDS platform BIOS versions

MDS Platform	BIOS Version	Caveats
DS-X97-SF4-K9 Intel(R) Xeon(R) CPU D-1548* Intel(R) Xeon(R) CPU D-1564N*	2.22.0 4.14.0	CVE-2024-38796

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

MDS Platform	BIOS Version	Caveats
DS-X9748-3072K9	1.12.0	CVE-2024-38796
DS-X9334-K9	4.2.2.0	CVE-2024-57258
DS-X9648-1536K9	04.01.05.7	CVE-2024-57258
DS-C9250I-K9-SUP	02.01.20	CVE-2024-57258
DS-C9148S-K9-SUP	02.01.20	CVE-2024-57258
DS-C9396S-K9-SUP	05.02.02(8)	CVE-2024-57258
DS-C9132T-K9-SUP	1.52.0	CVE-2024-38796
DS-C9148T-K9-SUP	1.14.0	CVE-2024-38796
DS-C9396T-K9-SUP	1.14.0	CVE-2024-57258
DS-C9220i-K9-SUP	1.18.0	CVE-2024-38796
DS-C9124V-K9-SUP	1.12.0	CVE-2024-38796
DS-C9148V-K9-SUP	1.12.0	CVE-2024-38796
DS-C9396V-K9-SUP	1.14.0	CVE-2024-38796

* The CPU model is shown in the 'Hardware' section of the **show version** command.

About EPLD images

Cisco MDS 9000 Series Switches contain a few 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, 9.4(5a).

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

Upgrade and downgrade paths

Cisco MDS NX-OS 9.4(5a) 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.

© 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.

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*.

IBM FICON Qualification Status

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

New/Enhanced software features

Product Impact	Feature	Description
Feature Set	Hardware Fabric CRC Monitoring	The 'log-only' action was removed as the default action. The default is now 'hardware fabric crc' which is enabled with a threshold of 3. This proactively disables faulty modules (xbars, linecards, supervisors) to minimize impact of internal faults on traffic. For more information, see *Cisco MDS 9000 High Availability Configuration Guide, Release 9.x*.
	Fabric Error Monitoring	Monitoring of fabric errors on linecards was added and the set of monitored counters was increased. This improves identification of the source of fabric errors for more precise actions. The default action was changed from 'log-only' to 'log-and-out-of-service'. This proactively disables faulty modules to minimize impact of internal faults on traffic. For more information, see *Cisco MDS 9000 High Availability Configuration Guide, Release 9.x*.
	showintstats command	The following fields were added to the output: receive/transmit average frame size in general-stats, SFP firmware version in transceiver-detail-stats and Transmit FC Aborts in link-stats. For more information, see *Cisco MDS 9000 Interfaces Configuration Guide, Release 9.x*.
	DWDM at 32 Gbps	A new configuration command to control TTS at 32 Gbps link speed on 64 Gbps interfaces was added. This allows interoperability with specific DWDM devices at 32 Gbps link speed. For more information, see *Cisco MDS 9000 Interfaces Configuration Guide, Release 9.x*.
	RxWait SNMP OID	A new SNMP OID for the Fibre Channel RxWait counter was added to allow management applications to collect this metric: 1.3.6.1.4.1.9.9.289.1.2.1.1.48 For more information, see *Cisco MDS 9000 System Management Configuration Guide, Release 9.x*.

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

Product Impact	Feature	Description
	File Name Restriction	Starting with MDS NX-OS 9.4(5a), the allowable characters comprising MDS file names on bootflash have been updated to include only alphanumeric and the five special characters '._-+:'. For more information, see *Cisco MDS 9000 Series Fundamentals Configuration Guide, Release 9.x*.

New hardware features

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

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. To see the BIOS version contained in this release reference the BIOS version table in this document.

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 resulting from BIOS updates, 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.

To determine the current BIOS version running in the switch issue the 'show version' command. To determine the current BIOS version on any module issue 'show version module <slot number>'.

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

Resolved issues

Severity 2 (Severe) issues

Bug ID	Headline	Known Impacted Releases
CSCwv47654	MDS 9250i runs out of memory (OOM) and may reboot	9.4(5a), 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), 9.3(2a), 9.3(2), 9.3(1), 9.2(2), 9.2(1a), 9.2(1), 8.5(1), 8.4(2f), 8.4(2e), 8.4(2d), 8.4(2c), 8.4(2b), 8.4(2a), 8.4(2), 8.4(1a), 8.4(1), 8.3(2), 8.3(1), 8.2(2), 8.2(1), 8.1(1b), 8.1(1a), 8.1(1)

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

Severity 3 (Moderate) issues

Bug ID	Headline	Known Impacted Releases
CSCws83802	CSR generation fails with error: 'could not perform certificate request creation'	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), 9.3(2a), 9.3(2), 9.3(1), 9.2(2), 9.2(1a), 9.2(1), 8.5(1), 8.4(2f), 8.4(2e), 8.4(2d), 8.4(2c), 8.4(2b), 8.4(2a), 8.4(2), 8.4(1a), 8.4(1), 8.3(2), 8.3(1), 8.2(2), 8.2(1), 8.1(1b), 8.1(1a), 8.1(1)
CSCwk62905	Include ‘show system internal xbar event-history info’ command to 'show tech-support details’	9.4(5a), 8.2(2)
CSCwu59451	Few FC drop counters are not getting logged to onboard logging	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), 9.3(2a), 9.3(2), 9.3(1), 9.2(2), 9.2(1a), 9.2(1), 8.5(1), 8.4(2f), 8.4(2e), 8.4(2d), 8.4(2c), 8.4(2b), 8.4(2a), 8.4(2), 8.4(1a), 8.4(1), 8.3(2), 8.3(1), 8.2(2), 8.2(1), 8.1(1b), 8.1(1a), 8.1(1)
CSCwt90883	show port-license output missing on MDS 9396S/9396T/9396V after the upgrade	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), 9.3(2a), 9.3(2), 9.3(1), 9.2(2), 9.2(1a), 9.2(1), 8.5(1), 8.4(2f), 8.4(2e), 8.4(2d), 8.4(2c), 8.4(2b), 8.4(2a), 8.4(2), 8.4(1a), 8.4(1), 8.3(2), 8.3(1), 8.2(2), 8.2(1), 8.1(1b), 8.1(1a), 8.1(1)
CSCwv28232	Service " snmpd" crashes with SIGABRT	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), 9.3(2a), 9.3(2), 9.3(1), 9.2(2), 9.2(1a), 9.2(1), 8.5(1), 8.4(2f), 8.4(2e), 8.4(2d), 8.4(2c), 8.4(2b), 8.4(2a), 8.4(2), 8.4(1a), 8.4(1), 8.3(2), 8.3(1), 8.2(2), 8.2(1), 8.1(1b), 8.1(1a), 8.1(1)

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

Bug ID	Headline	Known Impacted Releases
CSCwt42019	Zone modifications performed via snmp fail	8.1(1), 8.1(1a), 8.1(1b), 8.2(1), 8.2(2), 8.3(1), 8.3(2), 8.4(1), 8.4(1a), 8.4(2), 8.4(2a), 8.4(2b), 8.4(2c), 8.4(2d), 8.4(2e), 8.4(2f), 8.5(1), 9.2(1), 9.2(1a), 9.2(2), 9.3(1), 9.3(2), 9.3(2a), 9.4(1), 9.4(1a), 9.4(2), 9.4(2a), 9.4(3), 9.4(3a), 9.4(3b), 9.4(4), 9.4(5)
CSCwq13412	Duplicate warnings and alarms for tx-overutilization and txwait SMA counters	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)
CSCwr75319	Some SMA counters are assigned incorrect action groups when configured with action group ag-default	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)
CSCwt04973	'show fcs ie' + 'show topology' commands show wrong IP address of remote switch, NDFC unable to discover/manage switch	8.1(1), 8.1(1a), 8.1(1b), 8.2(1), 8.2(2), 8.3(1), 8.3(2), 8.4(1), 8.4(1a), 8.4(2), 8.4(2a), 8.4(2b), 8.4(2c), 8.4(2d), 8.4(2e), 8.4(2f), 8.5(1), 9.2(1), 9.2(1a), 9.2(2), 9.3(1), 9.3(2), 9.3(2a), 9.4(1), 9.4(1a), 9.4(2), 9.4(2a), 9.4(3), 9.4(3a), 9.4(3b), 9.4(4), 9.4(5)
CSCwt23512	IVR zone configurations failing after ISSU	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), 9.3(2a), 9.3(2), 9.3(1), 9.2(2), 9.2(1a), 9.2(1), 8.5(1), 8.4(2f), 8.4(2e), 8.4(2d), 8.4(2c), 8.4(2b), 8.4(2a), 8.4(2), 8.4(1a), 8.4(1), 8.3(2), 8.3(1), 8.2(2), 8.2(1), 8.1(1b), 8.1(1a), 8.1(1)
CSCwo81317	False SMA alarm or warning syslogs triggered for counters after policy activation	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)

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

Severity 4 (Minor) issues

Bug ID	Headline	Known Impacted Releases
CSCwt40941	Control characters in JSON output when 'terminal color' configured	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), 9.3(2a), 9.3(2), 9.3(1), 9.2(2), 9.2(1a), 9.2(1), 8.5(1), 8.4(2f), 8.4(2e), 8.4(2d), 8.4(2c), 8.4(2b), 8.4(2a), 8.4(2), 8.4(1a), 8.4(1), 8.3(2), 8.3(1), 8.2(2), 8.2(1), 8.1(1b), 8.1(1a), 8.1(1)
CSCwt08564	IOSlice temperature sensor shows as failed in MDS 9148T/9132T/9396T/9220i switch/MDS 9700 32 Gbps line card after second retry failure	8.1(1), 8.1(1a), 8.1(1b), 8.2(1), 8.2(2), 8.3(1), 8.3(2), 8.4(1), 8.4(1a), 8.4(2), 8.4(2a), 8.4(2b), 8.4(2c), 8.4(2d), 8.4(2e), 8.4(2f), 8.5(1), 9.2(1), 9.2(1a), 9.2(2), 9.3(1), 9.3(2), 9.3(2a), 9.4(1), 9.4(1a), 9.4(2), 9.4(2a), 9.4(3), 9.4(3a), 9.4(3b), 9.4(4), 9.4(5)

Severity 6 (Enhancement) issues

Bug ID	Headline	Known Impacted Releases
CSCwp39726	Enhancement to prevent statsclient, xbar and xbar_client crashes during sync loss b/w xbar and other modules	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), 9.3(2a), 9.3(2), 9.3(1), 9.2(2), 9.2(1a), 9.2(1), 8.5(1), 8.4(2f), 8.4(2e), 8.4(2d), 8.4(2c), 8.4(2b), 8.4(2a), 8.4(2), 8.4(1a), 8.4(1), 8.3(2), 8.3(1), 8.2(2), 8.2(1), 8.1(1b), 8.1(1a), 8.1(1)
CSCwm97073	PhysicalStatus is missing for SFPs and therefore not reflected in the SNMP Entity MIB.	9.4(2)

Open issues

Severity 3 (Moderate) issues

Bug ID	Headline	Known Impacted Releases
CSCws76238	An overutilized device is not isolated after ISSU from MDS NX-OS 9.4(4) to 9.4(5)	9.4(5a), 9.4(5), 9.4(3b), 9.4(3a), 9.4(2a), 9.4(1a)
CSCwt26267	Receiving timeout error during BIOS upgrade	9.4(5a), 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(5a), 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	8.4(2c), 8.1(1)
CSCwk33644	Power Supply status of " Powered-dn" causes Amber System Status LED	9.4(5a), 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), 9.4(1a)

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(5a), 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(5a), 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)
CSCwb13413	A fabric module with a faulty link to a linecard is not powered down	9.4(5a), 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(5a), 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(5a), 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:

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

- DS-X9848-480K9 – MDS 9700 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*.

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. Although DES encryption for SNMP is supported for existing users upgrading to Cisco MDS NX-OS Release 8.5(1), this method is deprecated. As a best practice, you should delete all SNMPv3 users configured with DES encryption before upgrading to Release 8.5(1) or later. 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*.

FCWA, XRC, DMM, SME

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

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

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.

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.