Release Notes for Cisco NCS 5500 Series Routers, IOS XR Release 25.4.1

© 2025 Cisco and/or its affiliates. All rights reserved.

Contents

Cisco NCS 5500 Series Routers, IOS XR Release 25.4.1 3
New software features 3
New hardware 7
Changes in behavior 8
Open issues 9
Known issues 10
Compatibility 10
Supported software packages 11
Related resources 12
Legal information 14

© 2025 Cisco and/or its affiliates. All rights reserved.

Cisco NCS 5500 Series Routers, IOS XR Release 25.4.1

Cisco IOS XR Release 25.4.1 is a new feature and hardware release for Cisco NCS 5500 Series routers. Key highlights include automated ISIS metric provisioning, DHCPv6 relay subscriber ID support, L3 EVPN IGMP and MLD state synchronization for improved multicast delivery, modular QoS scale enhancements, and configurable restore timers. The release also introduces MACSec support, TLS RFC 5289 compliance, centralized security template framework, enhanced programmability with gRPC RemoveContainer RPC, streamlined smart licensing, and robust timing with SyncE and PTP support

New software features

Table 1. New software features for Network Convergence System 5500 Series, Release 25.4.1

Product impact	Feature	Description
IP Addresses and Services		
Ease of use	DHCPv6 relay subscriber ID	Introduced in this release on: NCS 5500 fixed port routers; NCS 5700 fixed port routers; NCS 5500 modular routers (NCS 5500 line cards; NCS 5700 line cards [Mode: Native; Compatibility] You can now configure DHCPv6 relay subscriber ID option 38 in the DHCPv6 replay profile. This feature allows DHCPv6 relay agents to send a relay subscriber ID, also known as option 38, to the DHCPv6 server. You can configure unique IDs on L2 sub-interfaces. When a client request arrives on a DHCPv6 relay, the relay agent adds option 38 into the relay-forward message, providing the server with the client's originating interface for efficient address assignment.
Interface and Hardware Component		
Hardware Reliability	Extended support for 1x100G breakout mode on NC57-36H6D-S line card using DP04QSDD-HE0 and QDD-400G-ZRP-S	You can now configure 1x100G breakout mode on NC57-36H6D-S line card using the DP04QSDD-HE0 and QDD-400G-ZRP-S optics.
Software reliability	Restore timer configuration	Introduced in this release on: NCS 5500 fixed port routers; NCS 5500 modular routers (NCS 5500 line cards) This feature stabilizes your network performance by allowing you to configure the restore timer per service individually. The default value is 3.5 times of the CCM packet interval.
L2VPN		

© 2025 Cisco and/or its affiliates. All rights reserved.

Product impact	Feature	Description
Ease of Use	Layer 3 EVPN IGMP and MLD state synchronization	Introduced in this release on: NCS 5500 fixed port routers; NCS 5700 fixed port routers; NCS 5500 modular routers (NCS 5500 line cards; NCS 5700 line cards [Mode: Compatibility; Native]) You can ensure seamless and reliable multicast delivery in residential FTTH networks with IGMP and MLD state synchronization for L3 using EVPN. This feature synchronizes IPv4 IGMP and IPv6 Multicast Listener Discovery (MLD) states across multiple PE devices using L3 sub-interfaces, eliminating the need for complex L2 or IRB configurations. It supports both VRF and global routing table deployments, providing flexibility for various network designs.
Software Reliability	EVPN IRB over SRv6 core	EVPN IRB enhances network flexibility by enabling seamless Layer 3 connectivity between hosts on different subnets over an SRv6 network. This feature allows Layer 3 forwarding among hosts across IP subnets, maintains EVPN's multi-homing capabilities, and facilitates communication between EVPN hosts or subnets and IP VPNs. Leveraging SRv6's programmable and flexible transport, this solution streamlines the integration and management of modern, diverse network environments.
Licensing		
Licensing Process	Smart Licensing Perpetual Mode	Introduced in this release on: NCS 5500 fixed port routers; NCS 5700 fixed port routers; NCS 5500 modular routers (NCS 5500 line cards; NCS 5700 line cards [Mode: Native]) Smart Licensing Perpetual Mode simplifies licensing operations for customers with full-capacity perpetual licenses that cover the entire chassis or all line cards. These customers do not need to enable Smart Licensing Using Policy or report usage, which reduces administrative overhead across these deployments.
Licensing process	Support for Smart Licensing using Policy on NCS-57C3-MOD-HX	Introduced in this release on: NCS 5500 modular routers (NCS 5700 line cards [Mode: Compatibility; Native]) Cisco Smart Licensing Using Policy streamlines the licensing process for Cisco IOS XR products. You no longer need to register your device during installation, and there is no evaluation license state or period. Support for Smart Licensing using Policy is now extended to NCS-57C3-MOD-HX.
MPLS		
Software Reliability	Event history for MPLS-TE headend tunnels	Introduced in this release on: NCS 5500 fixed port routers; NCS 5700 fixed port routers; NCS 5500 modular routers (NCS 5500 line cards; NCS 5700 line cards [Mode: Compatibility; Native]) This feature introduces a granular and configurable

© 2025 Cisco and/or its affiliates. All rights reserved.

Product impact	Feature	Description
		event tracking mechanism for operational visibility into MPLS-TE tunnels. You can enable event history with the **mpls traffic-eng event-history tunnel** command and set the number of tracked events with the **mpls traffic-eng event-history tunnel event-count** command.
API experience	MPLS-TE IPv6-only autoroute announce	Introduced in this release on: NCS 5500 fixed port routers; NCS 5700 fixed port routers; NCS 5500 modular routers (NCS 5500 line cards; NCS 5700 line cards [Mode: Compatibility; Native]) This feature allows you to disable IPv4 autoroute announce without turning off autoroute announce entirely. To achieve IPv6-only announcements over MPLS-TE tunnels, use the new exclude-ipv4 option along with the include-ipv6 option in the autoroute announce configuration.
Programmability		
API Experience	gNOI RemoveContainer RPC	Introduced in this release on: NCS 5500 fixed port routers; NCS 5700 fixed port routers; NCS 5500 modular routers (NCS 5500 line cards; NCS 5700 line cards [Mode: Native]) We have introduced support for RemoveContainer RPC to give you direct, automated control over the removal of application containers managed by App Manager, allowing you to efficiently decommission unneeded or malfunctioning containers and maintain a clean, resource-optimized system.
API Experience	Multiple gRPC servers	Introduced in this release on: NCS 5500 fixed port routers; NCS 5500 modular routers (NCS 5500 line cards) You can now address diverse operational requirements and overcome the single-server limitation. The re-architected Extensible Manageability Services Daemon (EMSd) now supports multiple gRPC servers within a single process. This enables granular control and isolation. Each server can be independently configured with distinct settings for parameters that include listening ports, TLS profiles, network instances (VRFs), and DSCP values. Use this enhancement to support both OpenConfig and proprietary gRPC services.
Routing		
Ease of use	IS-IS auto-cost reference bandwidth	Introduced in this release on: NCS 5500 fixed port routers; NCS 5700 fixed port routers; NCS 5500 modular routers (NCS 5500 line cards; NCS 5700 line cards [Mode: Compatibility; Native]) The IS-IS auto-cost reference bandwidth feature automates IS-IS metric provisioning based on physical link bandwidth, optimizing path selection and reducing operational overhead. This feature allows you to configure a reference bandwidth, which IS-IS then uses to automatically calculate interface metrics. It also

© 2025 Cisco and/or its affiliates. All rights reserved.

Product impact	Feature	Description
		dynamically adjusts metrics for bundle interfaces when member links change, ensuring accurate and efficient routing without manual intervention.
Segment Routing		
Software Reliability	Hardware offload of MPLS liveness monitoring	Introduced in this release on: NCS 5700 fixed port routers; NCS 5500 modular routers (NCS 5700 line cards [Mode: Compatibility; Native]) You can now offload MPLS liveness monitoring for performance measurement to the router's hardware, which is the Network Processing Unit (NPU). This hardware-based approach improves efficiency and scalability, helping you meet delay-sensitive Service Level Agreements (SLAs). Previously, this monitoring was handled in software. The feature introduces a new keyword **npu-offload** under the **performance-measurement liveness-profile name** liveness profile command.
System Monitoring		
Software reliability	Insecure features warning syslog messages	Introduced in this release on: NCS 5500 fixed port routers; NCS 5700 fixed port routers; NCS 5500 modular routers (NCS 5500 line cards; NCS 5700 line cards [Mode: Compatibility; Native]) Cisco IOS XR software warns you with a syslog message each time you use an insecure command and repeats the warning every 30 days until you remove the command. This helps you identify potential security risks and suggests safer alternatives to improve your network security. Cisco will systematically deprecate and eventually remove these insecure features and protocols in future IOS XR releases. For more information on insecure commands and their alternatives, see Feature deprecation phasing out insecure capabilities.
System Security		
Software Reliability	Netconf access controls	Introduced in this release on: NCS 5500 fixed port routers; NCS 5700 fixed port routers; NCS 5500 modular routers (NCS 5500 line cards; NCS 5700 line cards [Mode: Compatibility; Native]) When this feature is enabled, NETCONF sessions will be blocked on the SSH port. However, SCP and SFTP will continue to function on the SSH port.
Ease of Setup	TLS RFC 5289 compliance for security template framework	The security template framework is based on RFC 5289 , which specifies new cipher suites for the Transport Layer Security (TLS) protocol. This feature supports Common Criteria (CC) mode which is an enhanced security mode that enforces stricter compliance-focused behavior. It enhances TLS security by introducing stronger Elliptic Curve Cryptography

© 2025 Cisco and/or its affiliates. All rights reserved.

Product impact	Feature	Description
		(ECC) algorithms.
Ease of Setup	Security template framework for TLS enabled applications	Security templates reduce misconfiguration risks and operational overhead by centralizing and standardizing security policy configuration for TLS-enabled applications. A security template bundles certificate authentication policy, TLS controls, and compliance mode settings. It acts as a single source of truth that applications reference, avoiding local embedding of security settings. This template defines how certificates are handled and controls various aspects of the TLS handshake.
Software Reliability	MACSec support on NCS-57C3-MOD-HX Router	MACsec, the Layer 2 encryption protocol, secures data on physical media and provides data integrity and confidentiality. We now support MACsec encryption on all ports of Cisco NCS-57C3-MOD-HX Router.
Timing		
Software Reliability	Synchronous Ethernet ESMC and SSM on Cisco NCS-57C3-MOD-HX Router	Introduced in this release on: NCS 5700 fixed port routers [Mode: Native] SyncE provides synchronization signals transmitted over the Ethernet physical layer to downstream devices, while the Synchronization Status Message (SSM) indicates the quality level of the transmitting clock to the neighboring nodes, informing the nodes about the level of the network's reliability. Ethernet Synchronization Message Channel (ESMC) is the logical channel that uses an Ethernet PDU (protocol data unit) to exchange SSM information over the SyncE link. This feature is supported on Cisco NCS-57C3-MOD-HX Router.
Software Reliability	PTP profiles support on Cisco NCS-57C3-MOD-HX Router	Introduced in this release on: NCS 5700 fixed port routers [Mode: Native] Based on the IEEE 1588-2008 standard, Precision Time Protocol (PTP) is a protocol that defines a method to synchronize clocks in a network for networked measurement and control systems. Supported PTP profiles: * G.8265.1 * G.8273.2 Class C * G.8275.1 * G.8275.2 This feature is supported on Cisco NCS-57C3-MOD-HX Router.

New hardware

Table 2. New hardware for Cisco NCS 5500 Series Routers, Release 25.4.1

© 2025 Cisco and/or its affiliates. All rights reserved.

Hardware	Description
Optics	This release introduces the following new optics for that are available on supported hardware in the product portfolio. For details refer to the Transceiver Module Group (TMG) Compatibility Matrix. Cisco QSFP28 100G ZR modules * DP01QS28-E20 * DP01QS28-E25 Cisco 100GBASE Quad Small Form-Factor Pluggable (QSFP) * QSFP-100G-ERL-S Cisco 400GBASE Quad Small Form-Factor Pluggable Double Density (QSFP-DD) * QDD-400G-SR4.2-BD (400, 4x100 modes) Cisco 400G QSFP-DD Ultra Long-Haul Coherent * DP04QSDD-ULH-A1 Cisco Small Form-Factor Pluggable (SFP) Modules * SFP-1G-LH * SFP-1G-SX
NCS-57C3-MOD-HX Router	The NCS-57C3-MOD-HX router is an environmental-hardened variant of the NCS-57C3-MOD-S router, specifically designed for deployment in outside plant environments within cabinet enclosures. It operates with the NC57-MOD-RP2-E-HX route processor and can be paired with either the NC57-C3-FAN1-HX or NC57-C3-FAN2-HX fan tray, along with the NC57-MPA-2D4H-H-S MPA. This router supports 56 ports in total (48 25GbE SFP28 and 8 100GbE QSFP28) and includes three Modular Port Adapter (MPA) slots for enhanced flexibility and future scalability.

Changes in behavior

- **Deprecation and phasing out features with insecure capabilities and its secure alternatives**
  From Release 25.4.1, Cisco IOS XR software displays warning messages when you configure features or protocols that lack sufficient security, such as those that transmit sensitive data without encryption or use outdated encryption mechanisms. The software also shows warnings when you do not follow security best practices, and it provides suggestions for secure alternatives.

  This list may change, but Cisco plans to generate warnings for the following features and protocols from Release 25.4.1. Each Release Notes will describe the exact changes for that version.
  These documents list all features planned for removal, including insecure commands, and provide recommended secure alternatives to help you maintain network security and compliance.

  - **Feature deprecation phasing out insecure capabilities**
  - **Feature deprecation and removal details**
  - **Feature removal and suggested alternatives**

Table 3. Deprecation and phasing out features with insecure capabilities and its secure alternatives

If you are using the following insecure features...	Then follow these secure alternatives...
HTTP	Use HTTPS.
FTP client install FTP install TFTP	Use SFTP.

© 2025 Cisco and/or its affiliates. All rights reserved.

If you are using the following insecure features...	Then follow these secure alternatives...
IPV4 source route	There is no alternative. Do not enable IPv4 source routing.
Telnet client Telnet dscp	There is no alternative. Do not use Telnet client.
Telnet server	Use SSH.
TFTP client	Use SFTP.
TFTP server	Use SSH.
copy ftp copy ftp running-config copy running-config ftp copy running-config tftp copy tftp copy tftp running-config copy xml-schema tftp	Use SFTP or SCP.
install FTP install TFTP	Use SFTP.
TCP or UDP small_servers	There is no alternative. Do not use TCP or UDP small_servers.
SSHv1	Use ssh server v2.
SSH host-key DSA algorithm	Use ECDSA, ED25519, or RSA and so on.
Syslog TLS Version 1.1 (server1)	Configure TLS Version 1.2 or higher.
TLS 1.0 TLS 1.1	Use TLS 1.2 or TLS 1.3.
utility mv ftp utility mv tftp	There is no alternative. Do not use utility mv ftp and utility mv tftp.
load ftp load tftp load script ftp load script tftp load diff ftp load diff tftp load diff reverse ftp load diff reverse tftp	Use scp or sftp.
tacacs and radius server with type-7 shared secret	Use type 6 secret.
NTPv2 NTPv3	Use NTPv4.

Open issues

There are no open issues in this release.

© 2025 Cisco and/or its affiliates. All rights reserved.

Known issues

- The Cisco NCS 5500 series modular routers with Cisco NCS 5700 line cards no longer support new features in compatibility mode. All Cisco IOS XR releases will continue to support features that were already enabled in compatibility mode until release 25.1.1. However, no new features will be added to compatibility mode. To take advantage of new features in current and subsequent releases, enable native mode by using the hw-module profile npu native-mode-enable command.
- During a software upgrade to IOS XR Release 25.4.1, the system may not complete the Auto-FPD upgrade as expected. After the upgrade, the FPD status shows 'RLOAD REQ', indicating that you must perform an additional reload to activate the updated FPD.

Compatibility

Compatibility matrix for EPNM and Crosswork with Cisco IOS XR software

The compatibility matrix lists the version of EPNM and Crosswork that are supported with Cisco IOS XR Release in this release.

Table 4. Compatibility Matrix for EPNM and Crosswork with Cisco IOS XR Software

Cisco IOS XR	Crosswork	EPNM
Release 25.4.1	Crosswork Optimization Engine 6.0	Evolved Programmable Network Manager 8.1.1

System requirements

Use the **show hw-module fpd** command in EXEC and Admin mode to view the hardware components with their current FPD version and status. The status of the hardware must be CURRENT; Running and Programed version must be the same. You can also use the **show fpd package** command in Admin mode to check the fpd versions.

Software version

To verify the software version running on the router, use **show version** command in the EXEC mode.

```
Router# show version
Cisco IOS XR Software, Version 25.4.1
Copyright (c) 2013-2025 by Cisco Systems, Inc.

Build Information:
 Built By     : swtools
 Built On     : Mon Dec 15 14:19:28 PST 2025
 Built Host   : iox-lnx-124
 Workspace    : /auto/srcarchive12/prod/25.4.1/ncs5500/ws
 Version      : 25.4.1
 Location     : /opt/cisco/XR/packages/
 Label        : 25.4.1

cisco NCS-5500 () processor
System uptime is 3 hours 14 minutes
```

© 2025 Cisco and/or its affiliates. All rights reserved.

Supported software packages

The following tables lists the Cisco IOS XR Software feature set matrix (packages) with associated filenames. Visit the Cisco Software Download page to download the Cisco IOS XR software images.

Table 5. Supported software for NCS 5500 Series Routers, Release 25.4.1

Feature Set	Filename	Description
Composite Package		
Cisco IOS XR IP Unicast Routing Core Bundle	ncs5500-mini-x.iso	Contains base image contents that includes: Host operating system System Admin boot image IOS XR boot image BGP packages
Individually-Installable Optional Packages		
Cisco IOS XR Manageability Package	ncs5500-mgbl-3.0.0.0-r2541.x86_64.rpm	Extensible Markup Language (XML) Parser, Telemetry, Netconf, gRPC and HTTP server packages.
Cisco IOS XR MPLS Package	ncs5500-mpls-2.1.0.0-r2541.x86_64.rpm ncs5500-mpls-te-rsvp-2.2.0.0-r2541.x86_64.rpm	MPLS and MPLS Traffic Engineering (MPLS-TE) RPM.
Cisco IOS XR Security Package	ncs5500-k9sec-3.1.0.0-r2541.x86_64.rpm	Support for Encryption, Decryption, Secure Shell (SSH), Secure Socket Layer (SSL), and Public-key infrastructure (PKI)
Cisco IOS XR ISIS package	ncs5500-isis-1.2.0.0-r2541.x86_64.rpm	Support ISIS
Cisco IOS XR OSPF package	ncs5500-ospf-2.0.0.0-r2541.x86_64.rpm	Support OSPF
Lawful Intercept (LI) Package	ncs5500-li-1.0.0.0-r2541.x86_64.rpm	Includes LI software images
Multicast Package	ncs5500-mcast-1.0.0.0-r2541.x86_64rpm	Support Multicast
EIGRP	ncs5500-eigrp-1.0.0.0-r2541.x86_64.rpm	Supports Enhanced Interior Gateway Routing Protocol
Lawful Intercept Control	ncs5500-lictrl-1.0.0.0-r2541x86_64.rpm	Supports Lawful Intercept Control
Healthcheck	ncs5500-healthcheck-1.0.0.0-r2541.x86_64.rpm	Supports System Health Check

Table 6. TAR files for Cisco NCS 5500 Series Router, Release 25.4.1

© 2025 Cisco and/or its affiliates. All rights reserved.

Feature Set	Filename
NCS 5500 IOS XR Software 3DES	NCS5500-iosxr-k9-25.4.1.tar
NCS 5500 IOS XR Software	NCS5500-iosxr-25.4.1.tar
NCS 5500 IOS XR Software	NCS5500-docs-25.4.1.tar
NCS 5500 IOS XR Software 3DES	NCS5500-iosxr-k9-25.4.1.tar
NCS 5500 IOS XR Software	NCS5500-iosxr-25.4.1.tar

Table 7. Packages for Cisco NCS 5700 Series Router, Release 25.4.1

Feature Set	Filename
NCS 5700 IOS XR Software	ncs5700-x64-25.4.1.iso
NCS 5700 IOS XR Software (only k9 RPMs)	ncs5700-k9sec-rpms.25.4.1.tar
NCS 5700 IOS XR Software Optional Package	NCS5700-optional-rpms.25.4.1.tar This TAR file contains the following RPMS: optional-rpms/cdp/* optional-rpms/eigrp/* optional-rpms/telnet/*

Related resources

Table 8. Related resources

Resource	Description
Cisco feature finder	Assists in locating features introduced across Cisco IOS XR releases and platforms.
Smart licensing	Provides information about Smart Licensing Using Policy solutions and their deployment on IOS XR routers.
Cisco NCS 5500 documentation	Provides CDC documentation for Cisco NCS 5500 series routers.
Transceiver Module Group (TMG) compatibility matrix	Allows searching by product family, product ID, data rate, reach, cable type, or form factor to determine the transceivers that Cisco hardware device supports.
Cisco IOS XR Error messages	Allows searching by release number, error strings, or comparing release numbers to view a detailed repository of error messages and descriptions.
Cisco IOS XR MIBs	Allows selecting the MIB of your choice from a drop-down to explore an extensive repository of MIB information.
Yang data models in GitHub	Provides yang data models introduced and enhanced in every IOS XR release.
Recommended release	Provides a general guide in case of upgrading IOS XR routers or new deployments that involve IOS XR routers.

© 2025 Cisco and/or its affiliates. All rights reserved.

© 2025 Cisco and/or its affiliates. All rights reserved.

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: www.cisco.com/go/trademarks. 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. (1110R)

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 included 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.

© 2025 Cisco Systems, Inc. All rights reserved.