Release Notes for Cisco NCS 560 Series Routers, Cisco IOS XR Release 25.4.1

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

Contents

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

Cisco NCS 560 Series Routers, Release 25.4.1

Cisco IOS XR Release 25.4.1 is a new feature release for Cisco NCS 560 Series routers.

For more details on the Cisco IOS XR release model and associated support, see Software Lifecycle Support Statement - IOS XR.

New software features

Table 1. New software features for NCS 560 Series Routers, Release 25.4.1

Product impact	Feature	Description
Interface and Hardware Component		
Software Reliability	Restore timer configuration	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		
Ease of Use	Layer 3 EVPN IGMP and MLD state synchronization	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.
Licensing		
Licensing Process	Smart Licensing Perpetual Mode	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.
MPLS		
Software Reliability	MPLS-TE IPv6-only autoroute announce	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.
System Monitoring		
Software Reliability	Insecure features warning syslog messages	The Cisco IOS XR software displays a warning syslog message when you run an insecure command. The warning syslog appears each time when you execute an insecure command, alerting you to potential security risks and suggesting safer alternatives so you can take action to improve your router and network security. Cisco will systematically deprecate the insecure features and protocols from the IOS XR software and will eventually remove them in future releases.

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

Product impact	Feature	Description
System Security		
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 (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.

New hardware

This section provides a brief description of the new hardware features introduced in this release.

Table 2. New hardware features for NCS 560 Series Routers, Release 25.4.1

Hardware	Description
Optics	*Note*: Optics support varies across devices (routers, line cards, RPs, and so on). To know if an optics is compatible with a specific Cisco device, refer to the Transceiver Module Group (TMG) Compatibility Matrix. This release introduces the following optic: • DP01QS28-E20 (C-Temp) • DP01QS28-E25 (I-Temp)

Changes in behavior

- Starting with Release 25.3.1, IOS XR software no longer supports Call Home transport mode for Licensing. Please configure CSLU or Smart Transport to ensure seamless operation of the licensing solution.
- Type6 server output enhancements: The show type6 server command now includes two new outputs that provides additional details for enhanced server management and troubleshooting:
  - Masterkey Length
  - Masterkey Hash
- gRPC remote-connection disable command: A new command, **grpc remote-connection disable**, has been introduced. This command allows users to disable TCP connections on the router, providing greater control over network configurations.

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

- The **Cisco-IOS-XR-pmengine-oper.yang** data model has been updated to ensure consistency. The naming convention has been standardized by renaming elements such as **hour24fec** to **hour24-fec**, **minute15pcs** to **minute15-pcs**, and **second30pcs** to **second30-pcs** across all layers, including OTN, OTNSEC, PCS, FEC, PRBS, Ether, and GFP. For more details on the sensor paths or the updated 25.2.1 YANG models, refer to the GitHub repository.
- **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.
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.

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

If you are using the following insecure features...	Then follow these secure alternatives...
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

Table 4. Open issues for Cisco NCS 560 Series Routers, Release 25.4.1

Bug ID	Description
CSCwr03926	NTP warning when you enable no authentication or MD5 authentication

Known Issues

- During the software upgrade to 25.4.1, the system may not complete the Auto-FPD upgrade as expected. After the software upgrade, the FPD status shows 'RLOAD REQ', indicating that you must perform an additional reload to activate the updated FPD.
- Telemetry data collection may timeout due to CPU overload during route churn. In such scenarios, telemetry will resume when the CPU becomes available after the route churn is complete.
- The standby RP may get into 'NOT READY' state intermittently due to some network churn, though the corresponding VM is up and running. But this is a transient state and shows that some data aren't in sync between active and standby due to the network churn. After both active and standby are in sync with respect to all the parameters, then the standby RP comes into 'READY' state.

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

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 5. Compatibility matrix for Cisco NCS 560 Series Routers, Release 25.4.1

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 14:13:15 PST 2025
 Built Host   : iox-lnx-125
 Workspace    : /auto/srcarchive12/prod/25.4.1/ncs560/ws
 Version      : 25.4.1
 Location     : /opt/cisco/XR/packages/
 Label        : 25.4.1

cisco NCS-560 () processor
System uptime is 4 hours 47 minutes
```

Supported software packages

This table 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.

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

Feature Set	Filename	Description
Cisco IOS XR IP Unicast Routing Core Bundle	ncs560-mini-x-25.4.1.iso	Contains base image contents that includes: Host operating system System Admin boot image IOS XR boot image BGP packages OS Admin Base Forwarding Modular Services Card Routing SNMP Agent Alarm Correlation
Cisco IOS XR Manageability Package	ncs560-mgbl-1.0.0.0-r2541.x86_64.rpm	Telemetry, Extensible Markup Language (XML), Parser, and HTTP server packages, NETCONF, YANG Models, gRPC.
Cisco IOS XR OSPF package	ncs560-ospf-1.0.0.0-r2541.x86_64.rpm	Supports OSPF
Cisco IOS XR Security Package	ncs560-k9sec-1.0.0.0-r2541.x86_64.rpm	k9sec is needed for IPsec or MACsec and Dot1x and for basic crypto services such as Decryption, Secure Shell (SSH), Secure Socket Layer (SSL), and Public-key infrastructure (PKI).
Multicast Package	ncs560-mcast-1.0.0.0-r2541.x86_64.rpm	Supports Multicast Supports Automatic Multicast Tunneling (AMT), IGMP Multicast Listener Discovery (MLD), Multicast Label Distribution Protocol (MLDP), Multicast Source Discovery Protocol (MSDP) and PIM.
Cisco IOS XR ISIS package	ncs560-isis-1.0.0.0-r2541.x86_64.rpm	Supports Intermediate System to Intermediate System (IS-IS).
Cisco IOS XR USB Boot Package	ncs560-usb_boot-25.4.1.zip	Supports Cisco IOS XR USB Boot Package
Cisco IOS XR MPLS Package	ncs560-mpls-1.0.0.0-r2541.x86_64.rpm ncs560-mpls-te-rsvp-1.0.0.0-r2541.x86_64.rpm	Supports MPLS and MPLS Traffic Engineering (MPLS-TE) RPM. Label Distribution Protocol (LDP), MPLS Forwarding, MPLS Operations, Administration, and Maintenance (OAM), Link Manager Protocol (LMP), Optical User Network Interface (OUNI) and Layer-3 VPN. Cisco IOS XR MPLS-TE and RSVP Package MPLS Traffic Engineering (MPLS-TE) and Resource Reservation Protocol (RSVP).
Cisco IOS XR LI Package	ncs560-li-1.0.0.0-r2541.x86_64.rpm	Lawful Intercept
Cisco IOS XR EIGRP Package	ncs560-eigrp-1.0.0.0-r2541.x86_64.rpm	(Optional) Includes EIGRP protocol support softwar

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

Related resources

Table 6. Related resources

Document	Description
Cisco feature finder	An interactive tool that assists in locating features introduced across Cisco IOS XR releases and platforms.
Smart licensing	Information about Smart Licensing Using Policy solutions and their deployment on IOS XR Routers.
Cisco NCS 560 documentation	CCO Documentation for Cisco NCS 560 Series Routers
Transceiver Module Group (TMG) compatibility matrix	Search 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	Search by release number, error strings, or compare release numbers to view a detailed repository of error messages and descriptions.
Cisco IOS XR MIBs	Select the MIB of your choice from a drop-down to explore an extensive repository of MIB information.
YANG data models	A user-friendly reference designed to easily explore and understand the various data models supported in Cisco IOS XR platforms and releases.
Yang data models in Github	Repository containing the folders with yang data models introduced and enhanced in every IOS XR release.

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.