



Release Notes for Cisco NCS 5500 Series Routers, IOS XR Release 26.3.1



Contents

- Cisco NCS 5500 Series Routers, IOS XR Release 26.3.1 3
- New software features 3
- New hardware 7
- Changes in behavior 7
- Open issues..... 10
- Known issues..... 10
- Compatibility..... 10
- Supported software packages 11
- Related resources..... 12
- Legal information 14

Cisco NCS 5500 Series Routers, IOS XR Release 26.3.1

Cisco IOS XR Release 26.3.1 for Cisco NCS 5500 Series Routers delivers robust advancements across architecture, IP/QoS, routing, programmability, security, and operational simplification. This release strengthens software reliability with features such as eBGP RT-constraint multipath, Y.1731 measurements for CFM over GRE single pass, admin sleep mode for optical transceivers, and inter-area route propagation limits in IS-IS. Enhanced programmability and telemetry are realized through gNMI Internal Path sharing and high-availability gNOI Containerz on active and standby route processors. Security is elevated with PQC-enabled MACsec with EAP-TLS, IPsec for management traffic, AuditD process keepalive, gated shell access, SSH client strict host key check, upgraded CURL libraries, and SNMP secure-v3. Operational efficiency is furthered by persistent logging, performance monitoring, dynamic configuration in Bootz, XR version formats for service packs and special releases, and Smart Licensing Using Policy for FCM platforms, collectively driving reliability, security, and simplified management.

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 Network Convergence System 5500 Series, Release 26.3.1

Product impact	Feature	Description
BGP		
Software reliability	eBGP RT-constraint multipath	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 enables more complete and resilient VPN route propagation in environments with redundant external peers, while preserving existing best-path behavior and operational consistency by extending RTC (route target constraint) processing on ASBRs (autonomous systems border routers). This is achieved by installing RT membership state on all qualified eBGP multipath neighbors instead of only the best-path neighbor.
Interface and Hardware Component		
Software reliability	Y.1731 measurements for CFM over GRE single pass	You can now monitor delay and frame loss for Layer 2 pseudowire services over MPLS Single-Pass GRE tunnels using Y.1731 Delay Measurement and Synthetic Loss Measurement between CFM UP MEPs, enabling accurate SLA measurements and improved fault detection without changes to your existing service protocols. This feature is supported on: • NCS-55A1-24H • NCS-55A1-36H-S • NCS-55A1-36H-SE-S • NCS-55A2-MOD-HD-S • NCS-55A2-MOD-S • NCS-55A2-MOD-HX-S • NCS-55A2-MOD-SE-H-S • NCS-55A2-MOD-SE-S • NCS-55A1-24Q6H-S

Product impact	Feature	Description
		• NCS-55A1-24Q6H-SS • NC55-24x100G-SE • NC55-24H12F-SE • NC55-36x100G-S • NC55-36x100G-A-SE • NC55-MOD-A-S • NC55-MOD-A-SE-S • NC55-32T16Q4H
Software reliability	Admin sleep mode for optical transceivers	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 provides a controlled way to reduce transceiver power consumption while keeping the optics accessible by adding an admin sleep mode or low power mode for optical transceivers on NCS 5500 routers. When a user applies shutdown under controller optics, the router places the corresponding optical module into a low power state.
MACsec		
Software reliability	PQC-enabled MACsec with EAP-TLS	This feature is supported on all MACsec-supported IOS XR platforms. Introduces PQC-capable TLS key exchange support for EAP-TLS and configurable 128-bit or 256-bit EAP-derived MACsec CAK length.
Routing		
Software reliability	Inter-area route propagation limits in IS-IS	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 helps protect the network from excessive inter-area route propagation caused by misconfiguration or unexpected route growth by limiting the number of prefixes propagated between IS-IS levels. This feature, using the new maximum-propagated-prefixes command, allows operators to define propagation thresholds, receive early warnings, and optionally stop advertising additional prefixes when limits are exceeded.
Setup and Upgrade		
Upgrade	XR version formats for service packs and special releases	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 enhancement introduces support for new XR release version formats for service pack (SP) and special release (SR) in the install infrastructure so that XR software can correctly recognize, compare, display, and validate SP and SR versions.
Ease of setup	Dynamic configuration in Bootz	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])

Product impact	Feature	Description
		You can now set initial device configuration at first boot that remains flexible for future changes. This feature allows you to modify or overwrite dynamic boot-time settings through standard CLI or GNMI Set RPC calls without requiring a factory reset.
System Management		
Ease of use	Configure device data privacy for Smart Licensing	Introduced in this release on: NCS 5500 fixed port routers; NCS 5500 modular routers Provides controls to suppress the device hostname and smart agent version in smart licensing usage reports.
Software reliability	Performance monitoring	Introduced in this release on: NCS 5500 modular routers You can enable or disable performance-data collection globally and use operational commands to verify current and historical clock and port performance records.
Upgrade	Configure SNMP secure-v3	Introduced in this release on: NCS 5500 modular routers; NCS 5700 modular routers This feature enhances the SNMP security by configuring only SNMPv3 with SHA-2 authentication and AES-based privacy using the secure-v3 CLI. The router continues to support SNMPv1, SNMPv2c, and legacy SNMPv3 configurations, but these configurations are deprecated. If a legacy SNMP configuration remains active, the router logs a deprecation warning every 30 days. The router rejects the commit if the same group, user, or notification host user is configured through both legacy SNMP and SNMP secure-v3.
System Monitoring		
Software reliability	Persistent logging	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 preserves the contents of the IOS XR logging buffer across node reloads, router reloads, and RP failovers. Syslog messages are written to both the in-memory logging buffer and a persistent file on local storage. After a reload or failover, the system restores the logging buffer from persistent storage so that retained log messages before the event and current logs, are displayed.
System Security		
Software reliability	IPSec for management traffic	Introduced in this release on: NCS5500 modular routers; NCS 5700 routers. IPSec for management traffic protects eligible management traffic generated by or destined for the router. The feature uses IKEv2, IPSec, Tunnel MA, and associated virtual tunnel interfaces. *This feature is supported on NCS-57C3-MOD-S.
Software reliability	Upgrade CURL libraries for HTTP client	Introduced in this release on: NCS 5500 fixed routers You gain enhanced security and improved reliability through an upgraded embedded libcurl library. This transparent update

Product impact	Feature	Description
		preserves existing functionality and continues to support HTTP/1.0 and HTTP/1.1.
Software reliability	AuditD process keepalive	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]) AuditD process keepalive improves compliance verification and helps detect silent AuditD failures earlier by periodically generating identifiable AuditD keepalive events at a configurable interval to confirm that the AuditD service is running and that the audit logging path remains operational.
Software reliability	Gated shell access	Introduced in this release on: NCS 5500 fixed port routers; NCS 5700 fixed port routers Gated shell access requires consent token authorization for direct root shell access initiated through supported shell commands.
Software reliability	SSH client strict host key check	Introduced in this release on: NCS 5500 fixed port routers; NCS 5700 fixed port routers You enhance SSH security by enforcing strict host key checking, allowing you to control how the SSH client handles new or changed server keys - accept, reject, or prompt for approval. Trusted host keys are stored system-wide and persist across reloads, ensuring consistent validation for your outbound SSH connections.
Telemetry		
Software reliability	gNMI Internal Path sharing	You can now reduce redundant processing and ensure that collectors receive synchronized, reliable data. With Internal Path sharing, the router automatically detects duplicate Internal Paths across different gNMI subscription lists and consolidates data collection for those paths. This optimization provides consistent data snapshots to collectors without requiring any user configuration. This feature introduces these changes: CLI: • show telemetry subscriptions [id <id>] • show telemetry destination endpoints [id <id>] • show telemetry collections [id <id>]
Programmability		
Software reliability	gNOI Containerz on active and standby route processors	You can now reduce downtime and maintain uninterrupted operation of the gNOI Containerz services. With high availability enabled for Containerz on both active and standby Route Processors (RPs), switchover occurs without the need to reset or reload line cards. This high availability facilitates smooth onboarding and management of third-party applications without disrupting service. For the specification on gNOI.containerz, see the GitHub repository.

New hardware

Hardware	Description
Immediate MPA Reinsertion	Introduced in this release on: NCS 5500 fixed port routers; NCS 5700 fixed port routers The MPA replacement process is now faster and more efficient. Starting with this release, you can reinsert or replace an MPA immediately after removing it from the slot, without waiting for the previously required 60-second interval. This enhancement reduces maintenance time and simplifies field replacement procedures. • This feature support is extended to: • NCS-55A2-MOD-S • NCS-55A2-MOD-SE-S • NCS-55A2-MOD-HX-S • NC55A2-MOD-SE-H-S • NCS-55A2-MOD-HD-S • NCS-57C3-MOD-SE-S • NCS-57C3-MODS-SYS • NCS-57C3-MOD-S • NCS-57C3-MOD-SYS • NCS-57C3-MOD-HX
Optics	This release introduces the following new optic on selective hardware within the product portfolio. For details, refer to the Transceiver Module Group (TMG) Compatibility Matrix Cisco QSFP28 100G ZR module • DP01QS28-MX2-A1

Changes in behavior

Deprecation and phasing out features with insecure capabilities and its secure alternatives

In Release 26.3.1, 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 25.3.1. 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 2. 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...
TLS 1.0 TLS 1.1	Use TLS 1.2 or TLS 1.3.
SSH key-exchange algorithm diffie-hellman-group1-sha1	Use stronger SSH key-exchange algorithms. Do not configure diffie-hellman-group1-sha1.
SSH ciphers 3des-cbc	Use stronger SSH ciphers.
SSH host-key DSA algorithm	Use ECDSA, ED25519, or RSA host keys. Note: The SSH host-key DSA algorithm is not recommended. However, it has not been removed. If required, you can still generate and use DSA host keys. Cisco recommends using ECDSA, ED25519, or RSA host keys.
SSHv1	Use SSHv2.

This section provides a brief description of the behavior changes introduced in this release.

- Deprecation of PCE NETCONF CLI

Starting with Cisco IOS XR Release 26.3.1, the PCE NETCONF CLI configuration is deprecated. Previously, you could configure NETCONF attributes directly for the Path Computation Element by using the `pce netconf` CLI commands. Because there is no actual operational use case for this configuration, it has been removed entirely. You do not need to perform any configuration migration or apply replacement commands, as there is no impact from this deprecation.

- Boolean values in gNMI path keys

Starting with Cisco IOS XR Release 26.3.1, Boolean list keys in gNMI Subscribe responses that use proto or JSON_IETF encoding are represented by the canonical strings **true** and **false** instead of **1** and **0**. If your collector explicitly expects or compares the earlier numeric strings, update its parsing logic. You do not need to make any router configuration changes.

- Enable automatic Docker Daemon startup with Application Manager

The **appmgr docker start** command enables the Docker daemon to start automatically when Application Manager starts.

```
Router(config)# appmgr docker start
```

```
Router(config)# commit
```

- Increased CPU and memory limits for TPAs

Starting with Cisco IOS XR Release 26.3.1, the maximum configurable hard resource limits for Third-Party Applications (TPAs) are increased to 100 percent of total system CPU and 80 percent of overall system memory. These limits prevent TPAs from exceeding the CPU and memory thresholds, regardless of resource usage by other IOS XR processes.

- VRF Naming Restriction

Starting with Cisco IOS-XR Release 26.3.1, the uppercase name "DEFAULT" is reserved for the OpenConfig default network instance. You must choose a different name for any user-defined VRF. This restriction applies to global VRF configuration, interface VRF assignments, and dynamic-

template VRF configurations across both CLI and YANG management interfaces. Before upgrading, you must rename or remove any user-defined VRF named "DEFAULT" to prevent startup configuration validation failures. Note that VRF names are case-sensitive; variations such as "Default" or "DEFAULT1" remain valid, and the system default VRF is not affected.

- Standards-compliant OpenConfig BGP identity values

Starting with Cisco IOS XR Release 26.3.1, selected OpenConfig BGP operational values use the module-qualified identity format, such as `openconfig-bgp-types:<identity>`, instead of `<identity>`. This format clearly identifies the YANG module defining each identity. These values include notification error codes and subcodes, `remove-private-AS` state, and supported capabilities. Clients and automation should process the module-qualified format.

- Default values restored after delete operations

Starting with Cisco IOS XR Release 26.3.1, deleting a leaf in a native YANG configuration container restores its defined default value, ensuring consistent configuration data in `show running-config` and `NETCONF get-config` output.

- Deprecation of the `show install packages` command family

Starting with Cisco IOS XR Release 26.3.1, the "show install packages..." family of commands such as the commands to show install packages information, `show install packages search`, and `show install packages` are marked as deprecated. For package names and repository information for uninstalled packages, use the **show install active**, **show install committed**, and **show install available** commands.

- Recommended workflows for removing or deactivating bug fixes

The `show install fixes deactivate` command is no longer the recommended workflow for removing or deactivating a bug fix. Select one of the following workflows based on the software images and rollback points available in your environment:

- Use `install rollback` when a previous rollback point exists where the same Cisco IOS XR version was loaded without the bug fix.
- Use `show install rollback ?` to identify a suitable rollback point.
- Use `install replace` when a suitable previous golden ISO image is available without the bug fix.
- If no previous rollback point or suitable golden ISO image exists, build a new golden ISO image with the desired set of fixes.
- If the golden ISO build fails or still includes the unwanted bug fix, the desired set of fixes cannot be built with the available fixes. Contact Cisco Support for a new version of the unwanted fix.

- Dedicated gRPC server requirement for system health checks

Starting with Cisco IOS XR Release 26.3.1, the system health-check service requires a dedicated gRPC server instance. This server provides a local-only gNMI connection to the Extensible Manageability Services Daemon (EMSD), independent of any other gRPC server configuration on the router. The `grpc local-connection` configuration under the default gRPC server is no longer required. With remote connections disabled, TLS certificate authentication is not required for this dedicated server. This configuration eliminates the system health-check service's reliance on TLS, without impacting the TLS configurations of other gRPC server instances.

- Provider Backbone Bridging Removed

Starting from Cisco IOS XR Release 26.3.1, Provider Backbone Bridging (PBB), including IEEE 802.1ah PBB, PBB-VPLS, and PBB-EVPN related configuration and operational commands, is removed. PBB has been deprecated since Cisco IOS XR Release 7.11.1. PBB configuration is no longer available in the configuration interface. In earlier releases, PBB configuration, if present, has no operational effect.

Open issues

There are no open issues in this release.

Known issues

There are no known issues in this release.

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 software in this release.

Table 3. Compatibility Matrix for EPNM and Crosswork with Cisco IOS XR Software

Cisco IOS XR	Crosswork	EPNM
Release 26.3.1	Cisco Crosswork Network Controller 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.

```
RP/0/RP0/CPU0#show version
Fri Sep 11 07:37:09.777 IST
Cisco IOS XR Software, Version 26.3.1
Copyright (c) 2013-2026 by Cisco Systems, Inc.
```

Build Information:

```
Built By      : swtools
Built On      : Thu Sep 10 03:49:30 PDT 2026
Built Host    : iox-lnx-049
Workspace     : /auto/srcarchive13/prod/26.3.1/ncs5500/ws
Version       : 26.3.1
Location      : /opt/cisco/XR/packages/
Label         : 26.3.1-iso
```

```
cisco NCS-5500 () processor
System uptime is 8 hours 36 minutes
```

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 4. Supported software for NCS 5500 Series Routers, Release 26.3.1

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-r2631.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-r2631.x86_64.rpm ncs5500-mpls-te-rsvp-2.2.0.0-r2631.x86_64.rpm	MPLS and MPLS Traffic Engineering (MPLS-TE) RPM.
Cisco IOS XR Security Package	ncs5500-k9sec-3.1.0.0-r2631.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-r2631.x86_64.rpm	Support ISIS
Cisco IOS XR OSPF package	ncs5500-ospf-2.0.0.0-r2631.x86_64.rpm	Support OSPF
Lawful Intercept (LI) Package	ncs5500-li-1.0.0.0-r2631.x86_64.rpm	Includes LI software images
Multicast Package	ncs5500-mcast-1.0.0.0-r2631.x86_64rpm	Support Multicast
EIGRP	ncs5500-eigrp-1.0.0.0-r2631.x86_64.rpm	Supports Enhanced Interior Gateway Routing Protocol
Lawful Intercept Control	ncs5500-lictrl-1.0.0.0-r2631x86_64.rpm	Supports Lawful Intercept Control

Feature Set	Filename	Description
Healthcheck	ncs5500-healthcheck-1.0.0.0-r2631.x86_64.rpm	Supports System Health Check

Table 5. TAR files for Cisco NCS 5500 Series Router, Release 26.3.1

Feature Set	Filename
NCS 5500 IOS XR Software 3DES	NCS5500-iosxr-k9-26.3.1.tar
NCS 5500 IOS XR Software	NCS5500-iosxr-26.3.1.tar
NCS 5500 IOS XR Software	NCS5500-docs-26.3.1.tar
NCS 5500 IOS XR Software 3DES	NCS5500-iosxr-k9-26.3.1.tar
NCS 5500 IOS XR Software	NCS5500-iosxr-26.3.1.tar

Table 6. Packages for Cisco NCS 5700 Series Router, Release 26.3.1

Feature Set	Filename
NCS 5700 IOS XR Software	ncs5700-x64-26.3.1.iso
NCS 5700 IOS XR Software (only k9 RPMs)	ncs5700-k9sec-rpms.26.3.1.tar
NCS 5700 IOS XR Software Optional Package	NCS5700-optional-rpms.26.3.1.tar This TAR file contains the following RPMS: optional-rpms/cdp/* optional-rpms/eigrp/* optional-rpms/telnet/*

Related resources

Table 7. Related resources

Resource	Description
Ask AI about this product	Provides access to Cisco product documentation for checking product support details. Start by selecting the product family, then use <i>Ask AI About This Product</i> tab for further information.
Cisco IOS XR MIBs	Allows selecting the MIB of your choice from a drop-down to explore an extensive repository of MIB information.
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 NCS 5500 documentation	Provides CDC documentation for Cisco NCS 5500 series routers.

Resource	Description
Feature deprecation and removal details	Outlines the features currently supported by each operating system.
Feature deprecation phasing out insecure capabilities	Provides a list of insecure features and protocols that are scheduled for systematic deprecation and eventual removal from specified Cisco products.
Feature removal and suggested alternatives	Details the reasons why certain features or protocols are deemed insecure and offers secure alternatives when available.
Recommended release	Provides a general guide in case of upgrading IOS XR routers or new deployments that involve IOS XR routers.
Smart licensing	Provides information about Smart Licensing Using Policy solutions and their deployment on IOS XR 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.
Yang data models in GitHub	Provides 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.

© 2026 Cisco Systems, Inc. All rights reserved.