Release Notes for Cisco IOS XRv 9000 Routers, IOS XR Release 26.3.1

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

Contents

Cisco XRv 9000 Routers, IOS XR Release 26.3.1 3
New software features 3
Changes in behavior 3
Open issues 4
Known issues 4
Compatibility 4
Related resources 7
Legal information 8

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

Cisco XRv 9000 Routers, IOS XR Release 26.3.1

Cisco IOS XR Release 26.3.1 for Cisco XRv 9000 Routers advances software reliability and operational security through targeted innovations in routing and system protection. This release strengthens routing architecture with BGP full path reflection, empowering route reflectors to advertise multiple unique BGP paths per prefix and thereby enhancing network visibility and traffic engineering capabilities. In the realm of security, it introduces gated shell access, which enforces cryptographic Consent Token authorization for direct root shell access, ensuring secure, auditable, and persistent control over privileged operations. Additionally, SSH client strict host key check is implemented to bolster outbound SSH connection security by enforcing rigorous host key validation policies and maintaining trusted key persistence across reloads. Collectively, these features reinforce the platform's reliability, security posture, and operational integrity for service provider and enterprise deployments.

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

New software features

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

Table 1. New software features for Cisco XRv 9000 Routers, Release 26.3.1

Product impact	Feature	Description
BGP		
Software reliability	BGP full path reflection	You gain full visibility into all eligible BGP paths per prefix as route reflectors can now advertise multiple unique paths, not just one per next hop. This enables more informed routing and traffic engineering, with exact duplicate paths still suppressed.

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or protocols that lack sufficient security, such as those that transmit sensitive data without encryption or use outdated encryption mechanisms.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

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

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.

Open issues

There are no open issues in this release.

Known issues

There are no known issues in this release.

Compatibility

Appliance model

Cisco IOS XRv 9000 Appliance is the pre-installed Cisco IOS XRv 9000 Router software that is sent from the factory on a bare metal UCS server hardware. It supports hyper scalability as it can scale to 70 million route prefixes when run as a Virtual Route Reflector. Therefore, the extra layer of software (hypervisor) is not required.

The Appliance also supports Zero Touch Provisioning (ZTP) which allows easier insertion into existing networks.

Table 3. Specification of the Cisco XRv 9000 Appliance

Parameters	Supported
Form Factor	1 RU
Processor	5th Gen Intel Xeon Scalable processor Intel(R) Xeon(R) Gold 5520+ 2.2GHz/205W 28C/52.5MB DDR5 4800MT/s
	4th Gen Intel Xeon Scalable processor Intel I5420+ 2GHz/205W 28C/52.5MB DDR5 4400MT/s
Memory size	128GB (8x16GB DDR5-4800 RDIMM 1Rx8)

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

Parameters	Supported
Internal storage	480GB M.2 Boot SATA Intel SSD
Software version	Cisco IOS-XR version 24.4.2 and later
Firmware version	BIOS version: C220M7.6.0.1a.0_XRV9K CIMC/BMC version: 6.0(1.250129)
Physical NICs	25G Model: Cisco-Intel E810XXVDA4L 4x25/10 GbE SFP28 PCIe 100G Model: Cisco-MLNX MCX623106AS-CDAT 2x100GbE QSFP56 PCIe Cisco-MLNX MCX623106AS-CDAT 2x100GbE QSFP56 PCIe

Hypervisors

A hypervisor enables multiple operating systems to share a single hardware host machine. While each operating system appears to have the dedicated use of the host's processor, memory, and other resources; the hypervisor controls and allocates only needed resources to each operating system and ensures that the operating systems (VMs) do not disrupt each other.

Installation of the Cisco IOS XRv 9000 Router is supported on selected Type 1 (native, bare metal) hypervisors. Installation is not supported on Type 2 (hosted) hypervisors, such as VMware Fusion, VMware Player, or Virtual Box. The following table lists release specific supported hypervisor versions.

Table 4. Support Matrix for Hypervisor Versions

Cisco IOS XR Version	VMWare ESXi	Kernel Based Virtual Machine (KVM)
Release 26.3.1	Version 8.0	Linux KVM based on Red Hat Enterprise Linux 8.10 and 9.6

Virtual machines

Cisco IOS XRv 9000 Router virtual machines must meet the following requirements:

Table 5. VM Requirement for VMware Environment

Parameters	Supported
VMware ESXi	Version 8.0
Virtual CPU cores	1 socket with a minimum of 4 cores Note: For multicast heavy deployments we recommend configuring 8 cores (with 4 assigned for control plane and 4 assigned for data plane). Note: For production environment minimum of 4 cores is recommended.
Virtual Machine memory size	The supported memory size is 64 GB for the default image and a minimum of 115 GB for VRR scenarios.
Virtual Machine hard disk size	128 GB minimum disk size for vPE and vRR image variants

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

Parameters	Supported
Virtual Interfaces	• E1000 • VMXNET3 for traffic interfaces only
Physical NICs	For pass-through: • Intel X710, XXV710 • Mellanox ConnectX 6 SR-IOV supported for: • Intel E810 XXV, E810 C • Intel X710, XXV710
Number of interfaces	Maximum of 11 NICs where: • 1 for management • 2 are reserved • 8 for traffic
Default video, SCSI controller set	Required SCSI controller not required for IDE disk.
Virtual CD/DVD drive installed	Virtual CD/DVD is required when installing the Cisco IOS XRv 9000 Router on the VM using ISO template.
IDE hard disk	Single IDE hard disk Note: Multiple hard disk drives on a VM are not supported.

Firmware update available for UCS M7 appliance (xrv9k-ucs-c220m7-huu-container-6.0.2.260143.tar.gz)

A firmware update package, xrv9k-ucs-c220m7-huu-container-6.0.2.260143.tar.gz, is now available for the UCS M7 appliance. This package includes firmware for both the CIMC and BIOS.

The SHA256SUM checksum for the package is:
a379a1c69aa933fe254544e1be51bab6dc35cf160bb8da36cc03cb23bfa87a54

The SHA256SUM checksum for the CIMC and BIOS binaries are:

- bios.pkg ea2141d410d238b30e8ea083f4ffbf47caf709f6d4d0ad78b487a10631464b03
- cimc.bin dea9473e8b4db868cb275fefe31c3c48121d2b9836b7ffa03094e332ecea4820

For detailed instructions on extracting and installing the firmware, please refer to the documentation at Firmware Files.

Optics support

Table 6. Optics support for the XRv 9000 Routers

Product	Product Code	Product Recommendation
Cisco 100GBASE LR4 QSFP Transceiver, LC, 10km over SMF	Cisco QSFP-100G-LR4-S	XRv9000 Appliance with UCS-C220 M7 server, 2X100G
Cisco 100GBASE SR4 QSFP Transceiver, MPO, 100m over OM4 MMF	Cisco QSFP-100G-SR4-S	

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

Product	Product Code	Product Recommendation
Cisco 10GBASE SFP+, Short Range	Cisco SFP-10G-SR	XRv9000 Appliance with UCS-C220 M7 server - 4X10/25G
Cisco 10GBASE SFP+, Long Range	Cisco SFP-10G-LR	

Related resources

Table 7. Related resources

Resource	Description
Ask AI about this product	Provides access to Cisco product documentation for checking feature support details.
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.
Cisco XRv 9000 documentation	Provides CDC documentation for Cisco XRv 9000 routers.
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.

© 2026 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.

© 2026 Cisco Systems, Inc. All rights reserved.