Release Notes for Cisco 8000 Series Routers, IOS XR Release 26.3.1

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

Cisco 8000 Series Routers, IOS XR Release 26.3.1 3
New software features 3
New hardware 15
Changes in behavior 16
Open issues 19
Known issues 20
Compatibility 20
Supported hardware 22
Supported software packages 27
Related resources 27
Legal information 29

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

Cisco 8000 Series Routers, IOS XR Release 26.3.1

Cisco IOS XR Release 26.3.1 for Cisco 8000 Series Routers introduces robust enhancements across architecture, IP/QoS, routing, programmability, security, and operational simplification. Key improvements include BGP full add-path reflection, inline ACL action modifications, 4K MTU support for RDMA RoCEv2, egress class-level traffic shaping for subinterfaces, and bandwidth remaining percent for class-based queuing. Routing and programmability are advanced with inter-area route propagation limits in IS-IS, RCC-based encapsulation ID checks, GNSS Anti-jamming and Anti-Spoofing, and gNOI Containerz on active and standby route processors. Security is strengthened through PQC-enabled MACsec with EAP-TLS, FIPS 140-3 certification, SSH remote public key authentication using TACACS, gated shell access, SNMP secure-v3, and persistent logging. Operational efficiency is elevated by optics firmware management and upgrade using CMIS CDB, encapsulation default catch-all mode, AuditD process keepalive, and egress traffic mirroring support on Local SPAN.

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 8000 Series Routers, Release 26.3.1

Product impact	Feature	Description
BGP		
Software Reliability	BGP full add-path reflection	Introduced in this release on: Fixed Systems (8200 [ASIC: Q100, Q200, P100], 8700 [ASIC: P100, K100], 8010 [ASIC: A100]); Centralized Systems (8600); Modular Systems (8800 [LC ASIC: Q100, Q200, P100]) You gain full visibility into all unique 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.
Software Reliability	BGP FIB Out of Resources mitigation	Introduced in this release on: Fixed Systems (8010 [ASIC: A100]), (8200 [ASIC: Q100, Q200], (8700 [ASIC: K100]) (select variants only*) When the IOS-XR Forwarding Information Base (FIB) approaches hardware resource limits, the system employs a BGP-driven eviction mechanism to maintain operational stability. This process ensures that system performance is preserved by selectively removing routes rather than suffering unpredictable hardware-level failures.
IP Addresses and Services		
Software Reliability	Inline ACL action modifications	Introduced in this release on: Fixed Systems (8010 [ASIC: A100], 8700 [ASIC: K100, P100], 8200 [ASIC: P100]); Modular Systems (8800) (select variants only*) Adds inline hardware updates for supported action-only changes to existing ACL entries. Match-field changes continue to use the existing hardware update method.

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

Product impact	Feature	Description
		The update method is selected automatically and does not add a configuration command. *This feature is supported on: • 8011-4G24Y4H-I • 8011-32Y8L2H2FH • 8011-12G12X4Y-A/D • 8712-MOD-M • 8711-48Z-M • 8212-48FH-M • 8711-32FH-M Line cards: • 88-LC1-36EH • 88-LC1-12TH24FH-E • 88-LC1-52Y8H-EM
Interface and Hardware Component		
Ease of Setup	Auto-Negotiation software mode for 1G SFP optical ports	Introduced in this release on: Fixed Systems (8700 [ASIC: K100]) (select variants only*) This release introduces auto negotiation on 1G fiber optics across 1G-capable hardware. Enable this support by configuring the negotiation auto command on the 1G optics. *This feature is supported on 8KMPA-18Z1D Modular Port Adapter.
Upgrade	CMIS transceiver firmware management	Introduced in this release on: Fixed Systems (8200 [ASIC: P100, P200], 8700 [ASIC: P100, P200]); Modular Systems (8800 [LC ASIC: P100, P200] You can keep supported CMIS optical transceiver firmware up to date by identifying applicable firmware, comparing versions, and downloading, running, committing, or aborting updates. Hitless restart is used when supported by the transceiver.
Upgrade	Extended Support for DP04QSDD-ULH-A1 optical module	This release introduces support for the Cisco 400G QSFP-DD Ultra Long-Haul (ULH) coherent optical module on this router: • Cisco 8011-32Y8L2H2FH The 400G QSFP-DD ULH optics are supported on port numbers 0 and 3.
Software Reliability	Auto-negotiation support for 1G SFP optical ports	Introduced in this release on: Fixed Systems (8010 [ASIC: A100]) (select variants only*) You can enable auto-negotiation in software mode on 1G SFP optical ports, allowing your fiber interfaces to dynamically negotiate speed and duplex settings with peer devices for improved link interoperability and reduced link failures. *This feature is supported on: • 8011-4G24Y4H-I • 8011-32Y8L2H2FH • 8011-12G12X4Y-A/D

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

Product impact	Feature	Description
Ease of Use	CFM Down MEPs without L2VPN services	Introduced in this release on: Fixed Systems (8200 [ASIC: Q200, P100], 8700 [ASIC: P100, K100], 8010 [ASIC: A100]); Centralized Systems (8600 [ASIC: Q200], 8400 [ASIC: K100]); Modular Systems (8800 [LC ASIC: Q200, P100]) You can now monitor direct L2 links and L2 transport interfaces with CFM Down MEPs without creating an L2VPN service only to enable CFM. This support reduces configuration overhead for standalone L2 interface monitoring. The support applies to physical interfaces, physical subinterfaces, bundle interfaces, and bundle subinterfaces. CFM continues to operate when L2VPN configuration is added to or removed from the same interface.
Hardware Reliability	Partial breakout for 4×100GE QSFP-DD optics	Introduced in this release on: Fixed Systems (8010 [ASIC: A100])(select variants only*) This feature enables flexible port combinations and maximizes hardware utilization on the Cisco 8011-32Y8L2H2FH router by allowing a 4x100GE optic to be used as a 1x100GE, 2x100GE, or 3x100GE so that unused SerDes (Serializer/Deserializer) lanes can be reallocated to other ports. *This feature is supported only on the Cisco 8011-32Y8L2H2FH router.
Software Reliability	Increase in number of CFM sessions to 4000	Introduced in this release on: Fixed Systems (8010 [ASIC: A100]) (select variants only*) The number of supported Connectivity Fault Management (CFM) sessions is now increased to 4000 from the previously supported value of 500. This enhancement enables faster fault detection and simplifies troubleshooting in high-performance networks. *This feature is now supported on: • 8011-4G24Y4H-I • 8011-32Y8L2H2FH • 8011-12G12X4Y-A/D
L2VPN		
Ease of Setup	Encapsulation default catch-all mode	Introduced in this release on: Fixed Systems (8010 [ASIC: A100], 8700 [ASIC: K100, P100], 8210 [ASIC: P100]); Centralized Systems (8400); Modular Systems (8800 [LC ASIC: K100, P100]) This feature enables an encapsulation default Layer 2 subinterface to match untagged traffic and unsupported encapsulation formats, in addition to unmatched VLAN-tagged traffic. This catch-all capability allows the matched traffic to be carried over VPWS or VPLS services through a single subinterface.
Licensing		
Licensing Process	Support for Smart Licensing Using Policy	Introduced in this release on: Fixed Systems (8700 [ASIC: K100]); Modular Systems (8800 [LC ASIC: K100]) (select variants only*) Cisco Smart Licensing Using Policy (SLP) 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.

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

Product impact	Feature	Description
		*This feature support is extended to • 88-LC1-16H16F-EM • 8711-28H8F-M
Licensing Process	Configure device data privacy for Smart Licensing	Introduced in this release on: Fixed Systems (8200 [ASIC: Q200, P100], 8700 [ASIC: P100, K100], 8010 [ASIC: A100]); Centralized Systems (8600 [ASIC: Q200]); Modular Systems (8800 [LC ASIC: Q100, Q200, P100]) Device data privacy for Smart Licensing provides a privacy control that suppresses the device hostname and Smart Agent version in Smart Licensing usage reports.
MACsec		
Software Reliability	PQC-enabled MACsec with EAP-TLS	Introduced in this release on: Fixed Systems (8200 [ASIC: P100], 8700 [ASIC: P100, K100], 8010 [ASIC: A100]) (select variants only*); Centralized Systems (8400 [ASIC: K100]) (select variants only*) Introduces PQC-capable TLS key exchange support to 802.1X EAP-TLS, with default CiscoSSL group advertisement and per-profile group configuration. *This feature is supported on all MACsec-supported IOS XR platforms.
Modular QoS		
Software Reliability	Queue buffer optimization based on average packet size	Introduced in this release on: Fixed Systems (8200 [ASIC: Q200]); Centralized Systems (8600 [ASIC: Q200]); Modular Systems (8800 [LC ASIC: Q200]) You can now optimize the maximum buffering available to a queue for a configured average packet size. This increases burst absorption before packet drops in non-PFC deployments and helps prevent queue drops in PFC deployments that use high pause thresholds and headroom, including Data Center Interconnect (DCI) links up to 120 km. The feature enables this behavior by configuring the NPU average-packet-size profile and reloading the router to apply the profile.
Upgrade	Egress feature capability	Introduced in this release on: Fixed Systems (8700 [ASIC: K100])(select variants only*); Centralized Systems (8400 [ASIC: K100]) You can now enable Egress feature capability on supported platforms to expand support for egress traffic management features. It uses an egress processing path to enable capabilities such as scalable egress queuing, egress policing, and multicast QoS scheduling. The feature introduces these changes: **CLI:** • hw-module profile edge-mode • show hw-module profile edge-mode *This feature is now supported on: • 8711-28H8F-M

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

Product impact	Feature	Description
		• 8404-SYS-D
Ease of Use	Absolute-value shaping on bundle interfaces	Introduced in this release on: Fixed Systems (8200 [ASIC: Q200, P100], 8700 [ASIC: P100, K100], 8010 [ASIC: A100]); Centralized Systems (8600 [ASIC: Q200], 8400 [ASIC: K100]); Modular Systems (8800 [LC ASIC: Q200, P100, K100]) You can control egress bandwidth with fixed shaping rates on supported bundle interfaces. This helps enforce predictable bandwidth allocations for customers, services, or AI workloads without relying on interface-relative percentages.
Ease of Use	Absolute-value policing on bundle interfaces	Introduced in this release on: Fixed Systems (8200 [ASIC: Q200, P100], 8700 [ASIC: P100, K100], 8010 [ASIC: A100]); Centralized Systems (8600 [ASIC: Q200], 8400 [ASIC: K100]); Modular Systems (8800 [LC ASIC: Q200, P100, K100]) You can control ingress bandwidth with fixed policing rates on supported bundle interfaces. This helps enforce predictable bandwidth limits for customers, services, or AI workloads using explicit bandwidth values instead of interface-relative percentages.
Ease of Use	Egress QoS policing with configurable burst values	Introduced in this release on: Fixed Systems (8700 [ASIC: K100])(select variants only*); Centralized Systems (8400 [ASIC: K100])(select variants only*); Modular Systems (8800 [LC ASIC: P100, K100])(select variants only*) You can now enforce bandwidth limits on outbound Layer 2 and Layer 3 traffic and configure burst values to control how the policer handles short-term traffic bursts. This capability helps prevent excessive outbound traffic from affecting downstream network resources while providing granular control over permitted burst traffic. *This feature is supported on: • 8712-MOD-M • 8711-48Z-M • 8404-SYS-D • 88-LC1-12TH24FH-E • 88-LC1-52Y8H-EM
Ease of Use	Bandwidth remaining percent for class-based queuing	Introduced in this release on: Fixed Systems (8200 [ASIC: P100], 8700 [ASIC: P100, K100], 8010 [ASIC: A100]); Centralized Systems (8400 [ASIC: K100]); Modular Systems (8800 [LC ASIC: P100, K100]) You can configure percentage-based sharing of remaining egress bandwidth among class-based queues on supported main interfaces and subinterfaces. This helps service provider and data center operators express bandwidth-sharing policies for customer services, AI workloads, and application traffic more intuitively without calculating scheduler ratios.
Ease of Use	Identify the source of stuck VOQs	Introduced in this release on: Modular Systems (8800 [LC ASIC: Q100, Q200]) You can now determine whether a detected stuck VOQ condition originates on the ingress or egress NPU and line card. Previously, isolating the affected side required debug-shell commands. The

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

Product impact	Feature	Description
		new operational commands display the affected VOQ and interface information, diagnostic status, and recommended action. *This feature is supported on: • 8800-LC-36FH • 8800-LC-48H • 88-LC0-36FH • 88-LC0-36FH-M • 88-LC0-34H14FH
Ease of use	Two-level hierarchical ingress policing	Introduced in this release on: Fixed Systems (8200 [ASIC: P100], 8700 [ASIC: P100, K100], 8010 [ASIC: A100]); Centralized Systems (8400 [ASIC: K100]); Modular Systems (8800 [LC ASIC: P100, K100]) You can enforce an aggregate bandwidth limit for a customer, service, or traffic aggregate while preserving per-class traffic policies. This helps keep aggregate ingress traffic within contracted bandwidth limits while maintaining application-level and class-level traffic handling.
Multicast		
Software reliability	Full 128-bit IPv6 multicast route keys	Introduced in this release on: Fixed Systems (8010 [ASIC: A100], 8700 [ASIC: K100, P100], 8210 [ASIC: P100]); Modular Systems (8800 [LC ASIC: K100, P100]) IPv6 Layer 2 and Layer 3 multicast route programming now uses all 128 bits of the IPv6 source and multicast group addresses as the hardware route key. Multicast group addresses that differ in any bit are programmed as distinct hardware entries. Previously, group addresses were restricted to a /96 mask and could vary only in the last 32 bits.
Programmability		
Software reliability	GNSS Anti-jamming and Anti-Spoofing	Introduced in this release on: Fixed Systems (8700 [ASIC: K100], 8010 [ASIC: A100]) (select variants only*) You are alerted in real time to GNSS jamming and spoofing events, with syslog alarms and alarm states displayed in show command outputs when a GNSS receiver detects or mitigates a threat. This enables you to monitor GNSS threats quickly and maintain service reliability. *This feature is supported on: • 8711-48Z-M • 8711-28H8F-M • 8011-4G24Y4H-I • 8011-12G12X4Y-A/D • 8011-32Y8L2H2FH
Software reliability	gNOI Containerz on active and standby route processors	Introduced in this release on: Centralized Systems (8600 [ASIC: Q200], 8400 [ASIC: K100]); Modular Systems (8800 [LC ASIC: Q100, Q200, P100, K100]) The gNOI Containerz service now supports seamless onboarding and management of third-party applications without service interruption. High availability is provided for Containerz on both

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

Product impact	Feature	Description
		active and standby Route Processors (RPs), allowing switchover to occur without resetting or reloading line cards. This guarantees continuous operation and minimizes downtime. For the specification on gNOI.containerz, see the GitHub repository.
Routing		
Software reliability	RCC-based encapsulation ID checks	Introduced in this release on: Fixed Systems (8200 [ASIC: Q200, P100], 8700 [ASIC: P100, K100], 8010 [ASIC: A100]); Centralized Systems (8600 [ASIC: Q200]); Modular Systems (8800 [LC ASIC: Q200, P100]) This enhancement provides better visibility into system-wide consistency verification and improves the RCC (Route Consistency Checker) output by reflecting a broader set of validation checks, giving better visibility into what RCC has verified across the system. RCC now accounts for Encap ID consistency verification on the RIB, increasing the number of consistency checks between RIB and FIB databases on nodes.
Software reliability	Inter-area route propagation limits in IS-IS	Introduced in this release on: Fixed Systems (8200 [ASIC: Q100, Q200, P100], 8700 [ASIC: P100, K100], 8010 [ASIC: A100]) (select variants only*); Centralized Systems (8600 [ASIC: Q200]); Modular Systems (8800 [LC ASIC: Q100, Q200, P100]) (select variants only*) 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.
Segment Routing		
Ease of use	EVPN RT5 support for L3VPN over SRv6	Introduced in this release on: Fixed Systems (8200 [ASIC: P100], 8700 [ASIC: P100, K100], 8010 [ASIC: A100]); Modular Systems (8800 [LC ASIC: P100]) Simplifies Layer 3 route advertisement across an SRv6 core by reducing the need for separate VPNv4 and VPNv6 unicast address families. This feature supports carrying L3VPN routes in the L2VPN EVPN Route Type 5 address family to provide end-to-end Layer 3 connectivity across an SRv6 core.
Ease of use	Lightweight host routing using LLDP	Introduced in this release on: Fixed Systems (8200 [ASIC: Q100, Q200, P100], 8700 [ASIC: P100, K100], 8010 [ASIC: A100]); Modular Systems (8800 [LC ASIC: K100)] You can now simplify host reachability by advertising IPv6 prefixes or SRv6 locators from a host or hypervisor to a directly connected Leaf or ToR router through LLDP IP Host Prefix TLVs. This capability removes the need to run a routing protocol stack on each host or hypervisor. The Leaf router installs the LLDP-learned prefixes in the routing table and redistributes them into routing protocols such as IS-IS or BGP.

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

Product impact	Feature	Description
Software reliability	Loopback-based performance monitoring for IPv6 endpoints	Introduced in this release on: Fixed Systems (8200 [ASIC: Q200, P100], 8700 [ASIC: P100, K100], 8010 [ASIC: A100]); Centralized Systems (8600 [ASIC: Q200]); Modular Systems (8800 [LC ASIC: Q200, P100]) You can now simplify IPv6 endpoint performance monitoring by eliminating the need to configure remote devices, enable IPM or STAMP support on those endpoints, or synchronize clocks with PTP. IPM loopback mode uses hardware-offloaded SRv6 probes to measure latency, packet loss, and liveness, and uses flow-label spraying to validate available Equal-Cost Multipath (ECMP) paths. The feature provides high-precision performance metrics through hardware-based timestamping and exports real-time results through telemetry and syslog alerts.
Ease of Use	EVPN ELAN Services over SRv6 TE Policies	Introduced in this release on: Fixed Systems (8200 [ASIC: P100], 8700 [ASIC: P100, K100], 8010 [ASIC: A100]); Modular Systems (8800 [LC ASIC: P100]) You can now maintain consistent path selection and efficient traffic delivery across your IPv6 networks. This is achieved by deploying a multipoint Layer 2 VPN service that uses colored routes to select specific SRv6 Traffic Engineering (TE) paths between your Provider Edge (PE) routers. You will use Route Type 1 (Ethernet Auto-Discovery) to advertise multihoming reachability and Route Type 3 (Inclusive Multicast Ethernet Tag) to support the forwarding of broadcast, unknown-unicast, and multicast (BUM) traffic. By applying an export route policy that adds a Segment Routing color extended community, you can steer both route types to matching SRv6 TE policies.
Software reliability	SRv6 Layer 3 gateway traffic class propagation	Introduced in this release on: Fixed Systems (8200 [ASIC: Q200, P100], 8700 [ASIC: P100, K100], 8010 [ASIC: A100]); Centralized Systems (8600 [ASIC: Q200]); Modular Systems (8800 [LC ASIC: Q200, P100]) Maintain consistent Quality of Service across your SRv6 domain and prevent high-priority traffic degradation caused by inner IPv4 or IPv6 DSCP values overwriting transport-level markings during packet re-origination.
Software reliability	SRv6 Per-Flow next-hop redirection using ABF	Introduced in this release on: Fixed Systems (8200 [ASIC: Q200, P100], 8700 [ASIC: P100, K100], 8010 [ASIC: A100]); Centralized Systems (8600 [ASIC: Q200]); Modular Systems (8800 [LC ASIC: Q200, P100]) Simplifies traffic steering by providing a lightweight, scalable alternative to full SR-TE policy configurations. This feature enables ABF policy-based redirection of IPv4 or IPv6 flows to a configured next-hop with SRv6 reachability, allowing for granular, per-flow steering without requiring explicit segment lists or candidate paths.
Setup and Upgrade		
Ease of setup	Bootz dynamic configuration	Introduced in this release on: Fixed Systems (8200 [ASIC: Q100, Q200, P100], 8700 [ASIC: P100, K100], 8010 [ASIC: A100]); Centralized Systems (8600 [ASIC: Q200], 8400 [ASIC: K100]); Modular Systems (8800 [LC ASIC: Q100, Q200, P100, K100]) 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.

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

Product impact	Feature	Description
System Management		
Software Reliability	Configure SNMP secure-v3	Introduced in this release on: Fixed Systems-Cisco 8010 Series Routers (ASIC: A100), Cisco 8200 Series Routers (ASICs:Q100, Q200, and P100), and Cisco 8700 Series Routers (ASICs: P100 and K100) 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	AuditD process keepalive	Introduced in this release on: Fixed Systems (8200 [ASIC: Q200, P100], 8700 [ASIC: P100, K100], 8010 [ASIC: A100]); Centralized Systems (8600 [ASIC: Q200]); Modular Systems (8800 [LC ASIC: Q200, P100]) AuditD process keepalive improves compliance verification and helps detect silent AuditD failures earlier by periodically generating an identifiable Linux audit event. Monitoring systems can use these events as a heartbeat to help detect interruptions in audit-event generation or delivery.
Software reliability	Persistent logging	Introduced in this release on: Fixed Systems (8200 [ASIC: Q200, P100], 8700 [ASIC: P100, K100], 8010 [ASIC: A100]); Centralized Systems (8600 [ASIC: Q200]); Modular Systems (8800 [LC ASIC: Q200, P100]) 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	Monitor XR shell commands	Introduced in this release on: Fixed Systems (8200 [ASIC: Q100, Q200, P100], 8700 [ASIC: P100, K100], 8010 [ASIC: A100]); Centralized Systems (8600 [ASIC: Q200]); Modular Systems (8800[LC ASIC: Q100, Q200, P100]) You can now trace **run** and **bash** commands to specific users and identify potential system compromises. By implementing shell-level user activity tracking, the router records each action, the user who performed it, and its timestamp. You can use this data to monitor user behavior, detect potentially malicious activity, and respond rapidly to security incidents.
Software Reliability	Upgrade CURL libraries for HTTP client	Introduced in this release on: Fixed Systems (8200 [ASIC: Q100, Q200, P100], 8700[ASIC: P100, K100], 8010 [ASIC: A100]; Centralized Systems (8600 [ASIC: Q200]); Modular Systems (8800 [LC ASIC: Q100, Q200, P100])

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

Product impact	Feature	Description
		You gain enhanced security and improved reliability through an upgraded embedded libcurl library. This transparent update preserves existing functionality and continues to support HTTP/1.0 and HTTP/1.1.
Software reliability	FIPS 140-3 certification	Introduced in this release on: Modular Systems (8800 [LC ASIC: K100]) (select variants only*) FIPS 140-3 (Federal Information Processing Standard 140-3) certification provides extended cryptographic standards including software, firmware, and hybrid modules. FIPS140-3 is used to approve cryptographic modules for the security of both hardware and software products. *This feature is supported on: • 88-LC1-48Y8F-EM • 88-LC1-16H16F-EM
Ease of setup	SSH remote public key authentication using TACACS	Introduced in this release on: Fixed Systems (8010 [ASIC: A100], 8200 [ASIC: Q100, Q200, P100], 8700 [ASIC: P100, K100]); Modular Systems (8800 [LC ASIC: P100]) (select variants only*) You can centrally manage SSH public keys on IOS XR by enabling devices to retrieve and validate user public keys from TACACS+ servers at login. This feature simplifies key management, streamlines access control, and supports fallback to local keys for continued access if the server is unavailable.
Software Reliability	Gated shell access	Introduced in this release on: Fixed Systems (8200 [ASIC: Q100, Q200, P100], 8700 [ASIC: P100, K100], 8010 [ASIC: A100]); Centralized Systems (8600 [ASIC: Q200]); Modular Systems (8800 [LC ASIC: Q100, Q200, P100]) 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: Fixed Systems (8200 [ASIC: Q200, P100], 8700 [ASIC: P100, K100], 8010 [ASIC: A100]); Centralized Systems (8600 [ASIC: Q200], 8400 [ASIC: K100]); Modular Systems (8800 [LC ASIC: Q200, P100]) 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	Introduced in this release on: Fixed Systems (8200 [ASIC: Q200, P100], 8700 [ASIC: P100, K100], 8010 [ASIC: A100]); Centralized Systems (8600 [ASIC: Q200]); Modular Systems (8800 [ASIC: Q100, Q200, P100]) The router now automatically detects duplicate Internal Paths that appear across different gNMI subscription lists and shares collection for those paths. This optimization reduces redundant processing and provides consistent data snapshots to collectors. No user configuration is necessary for this functionality.

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

Product impact	Feature	Description
Timing and Synchronization		
Software reliability	Use PTP Virtual Port and APTS to Select Timing Source	Introduced in this release on: Fixed Systems (8400 [ASIC: K100], 8700 [ASIC: K100]) (select variants only*) *This feature is supported on: • 8404-SYS-D • 8712-MOD-M
Software reliability	Synchronous Ethernet ESMC and SSM on Cisco 88-LC1-16H16F-EM cards	Introduced in this release on: Modular Systems (8800 [LC ASIC: K100]) (select variants only*) 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. Supported SyncE profiles: • G.8262 • G.8264 *This feature is supported on Cisco 88-LC1-16H16F-EM line cards.
Software reliability	PTP profiles support on Cisco 88-LC1-16H16F-EM line cards	Introduced in this release on: Modular Systems (8800 [LC ASIC: K100]) (select variants only*) 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 88-LC1-16H16F-EM line cards.
Software reliability	Synchronous Ethernet ESMC and SSM on Cisco 8711-28H8F-M	Introduced in this release on: Fixed Systems (8700 [ASIC: K100]) (select variants only*); Modular Systems (8800 [LC ASIC: K100]) (select variants only*) 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. Supported SyncE profiles: • G.8262 • G.8264

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

Product impact	Feature	Description
		*This feature is supported on Cisco 8711-28H8F-M routers.
Software reliability	PTP profiles support on Cisco 8711-28H8F-M	Introduced in this release on: Fixed Systems (8700 [ASIC: K100]) (select variants only*); Modular Systems (8800 [LC ASIC: K100]) (select variants only*) 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 8711-28H8F-M routers.
Software reliability	Global Navigation Satellite System (GNSS) support on Cisco 8711-28H8F-M	Introduced in this release on: Fixed Systems (8700 [ASIC: K100]) (select variants only*); Modular Systems (8800 [LC ASIC: K100]) (select variants only*) Global Navigation Satellite System (GNSS) is a satellite system used as a timing interface. GNSS receiver receives signals from GNSS satellites and decodes the information from multiple satellites to determine its distance from each satellite. Based on this data, the GNSS receiver identifies the location of each satellite. The supported GNSS class is PRTC-B. *This feature is supported on Cisco 8711-28H8F-M routers.
Software reliability	PTP frequency-assisted holdover	Introduced in this release on: Fixed Systems (8010 [ASIC: A100]), 8700 [ASIC: K100]; Modular Systems (8800 [LC ASIC: K100]) The frequency-assisted holdover feature enhances network stability by allowing for an extended holdover duration within the network-limits specification, when a Primary Reference Clock (PRC) frequency source remains available. This ensures that even if the GNSS or PTP time source is lost, the system can advertise timing stability for a longer, user-defined period without significant degradation.
Traffic Mirroring		
Ease of Use	Egress Traffic Mirroring Support on Local SPAN	Introduced in this release on: Fixed Systems (8200 [ASIC: P100], 8700 [ASIC: P100, K100], 8010 [ASIC: A100]); Centralized Systems (8400 [ASIC: K100]); Modular Systems (8800 [LC ASIC: P100]) You can now mirror outgoing traffic on the Cisco 8000 Series routers to verify exactly what the device forwards toward the next hop. This egress-only mirroring focuses on outgoing traffic without mixing in unrelated ingress traffic. With this feature, you create a monitor session, define a destination interface, and attach the source interface to this session and specify the transmission direction. The router replicates the egress packets to the destination, allowing you to troubleshoot network performance and connectivity effectively. This enhancement provides better visibility into your network traffic flow.

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

New hardware

Table 2. New hardware for Cisco 8000 Series Routers, Release 26.3.1

Hardware	Description
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

88-LC1-16H16F-EM Line Card based on K100 NPU	The 88-LC1-16H16F-EM line card based on K100 NPU supports the following:
	• Forty ports provide an overall throughput of 9.6Tbps:
	  ○ 16 ports of 400/200/100/40 GbE using QSFP56-DD/QSFP56/QSFP28-DD/QSFP28/QSFP+ optics.
	  ○ 16 ports of 100/40 GbE using QSFP28/QSFP+ optics. They support 25/10 GbE using SFP28/SFP+ over the QSFP CVR adapter.
	  ○ 8 ports of 200/100/40 GbE using QSFP56/QSFP28-DD/QSFP28/QSFP+ optics.
	• PTP Timing with Class C performance on all ports.
	• Supports MACsec on all port speeds at line rate.
	The 88-LC1-16H16F-EM line card is supported on the following modular chassis configurations, both requiring the 8800-RP2 route processor:
	• Cisco 8804 with 8804-FC1 fabric card.
	• Cisco 8808 with 8808-FC1 fabric card.
	For more information on this line card, see the Cisco 8000 Series Routers Data Sheet.

88-LC1-48Y8H-EM Line Card based on K100 NPU	The 88-LC1-48Y8H-EM line card based on K100 NPU supports the following:
	• Sixty-four ports provide an overall throughput of 4.8Tbps—
	  ○ 8 ports of 400/200/100/40 GbE usingQSFP56-DD/QSFP28-DD/QSFP28/QSFP+ optics.
	  ○ 8 ports of 100/40 GbE using QSFP28/QSFP+ optics.
	  ○ 48 ports of SFP supporting various speed combinations accounting to a maximum bandwidth of 800Gbps:
	  ▪ 32 ports of 25/10/1 GbE using SFP28/SFP+/SFPoptics.
	  ▪ 16 ports of 10/1 GbE using SFP+/SFP optics.
	• PTP Timing with Class C performance on all ports.
	• Supports MACsec on all port speeds at line rate.
	The 88-LC1-48Y8H-EM line card is supported on the following modular chassis configurations, both requiring the 8800-RP2 route processor:
	• Cisco 8804 with 8804-FC1 fabric card.
	• Cisco 8808 with 8808-FC1 fabric card.

Updates in fan replacement guidelines	Introduced in this release on: Centralized Systems (8600 [ASIC: Q200]); (select variants only*) With this release, the chassis does not initiate an immediate shutdown upon fan failure. To ensure system stability, we recommend to replace the failed fan within two minutes. This feature is supported on: • Cisco 8608 router
8812-FAN-V2 fan tray	To maintain optimal cooling, the 8812-FAN-V2 high-performance fan tray must be installed in the Cisco 8812 router.

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

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 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...
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.

- Logging Bootz, Authz, and Pathz policy updates

  Changes to certificates or other credentials related to Bootz, Authz, and gNSI (Pathz) are explicitly logged through IOS messages.

  Example logs:

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

#Bootconfig through boot up flow

RP/0/RP0/CPU0:Feb 4 01:30:02.403 UTC: emsd[1122]: %MGBL-EMS-6-EMSD_POLICY_UPDATE : Bootz policy committed. source: bootconfig

#Bootconfig through SetBootConfig RPC

RP/0/RP0/CPU0:Feb 5 08:10:41.711 UTC: emsd[1122]: %MGBL-EMS-6-EMSD_POLICY_UPDATE : Bootz policy committed. source: bootconfig

#Authz and Pathz through rotate CLI

RP/0/RP0/CPU0:Feb 4 00:44:57.349 UTC: emsd[1122]: %MGBL-EMS-6-EMSD_POLICY_UPDATE : Authz policy committed. source: CLI

RP/0/RP0/CPU0:Feb 4 00:45:23.470 UTC: emsd[1122]: %MGBL-EMS-6-EMSD_POLICY_UPDATE : PathZ policy committed. source: CLI

#Authz and Pathz through Rotate RPC

RP/0/RP0/CPU0:Feb 4 21:05:06.591 UTC: emsd[1122]: %MGBL-EMS-6-EMSD_POLICY_UPDATE : Authz policy committed. source: Rotate

- 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

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

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.Egress policer values in the show qos interface command output

- Egress feature capability on additional Cisco 8000 routers:

  Starting with Cisco IOS XR Release 26.3.1, the egress feature capability is available on the 8404-SYS-D and 8711-28H8F-M routers. This enhancement enables these routers to use egress QoS features that require the capability. You enable the capability by configuring the hw-module profile edge-mode command and reloading the router.

- Deprecation of Type 7 passwords for PCEP

  Starting with Cisco IOS XR Release 26.3.1, Type 7 password configuration is deprecated for PCEP (Path Computation Element Protocol). Previously, you could configure clear-text or encrypted passwords directly for a PCE or PCE peer by using the pce password and pce peer ipv4 <IPv4/IPv6 address> password CLI commands. You must migrate to the more secure keychain-based configuration by using the pce keychain or pce peer ipv4 <IPv4/IPv6 address> keychain CLI command.

- Dedicated gRPC server requirement for system health checks

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

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.

- Cisco 8600 series router switch card removal using graceful shutdown

  Starting from Release 26.3.1, removing a switch card by only opening the ejector lever (non-graceful shutdown) is no longer supported. To remove a switch card, use the shutdown CLI command, wait until the shutdown process is complete, open the ejector lever, and then remove the switch card.

- 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.

- Debug output for failed callbacks changed from IOS to LTRACE

  The debug message output for unsuccessful callbacks has been changed from ios to ltrace. Previously, fh_reg_callback_hndlr printed an ios message when the callback to the client failed. With this fix, it now prints an LTRACE message instead. You will no longer see IOS debug messages when the callback to the client fails after an FC reload.

- On the Cisco 8404-SYS-D platform, dual Route Switch Processors (RSPs) can be installed, and the Route Processor Failover (RPFO) is now supported in Cisco IOS XR release 26.3.1.

- Egress policer values in the show qos interface command output:

  Starting with Cisco IOS XR Release 26.3.1, the show qos interface interface-name output command displays the CIR (configured committed information) and burst values for an egress policer under the associated class map. Previously, the command displayed the class map but omitted these configured policer values. With this enhancement, you can verify the configured egress policer values directly from the command output.

- Default SPAN Drop Session Disabled on A100-based Silicon One ASICs

  Starting with Cisco IOS XR Release 26.2.2 and Release 26.3.1, the automatically generated default SPAN-on-drop session is not created on A100-based Silicon One ASICs on Cisco 8000 systems.

  As a result, default_monitor_session does not appear in the show monitor-session status output on the A100-based Silicon One ASICs systems. This behavior applies only to the internally generated default drop session. User-configured SPAN and ERSPAN sessions continue to be supported.

Open issues

Table 4. Open issues for Cisco 8000 Series Routers, Release 26.3.1

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

Bug ID	Description
CSCww26715	LSPNH_ASYNC_ERROR and HW_PROG_ERROR occur on PE1 during IS-IS remove/add operations at 3K scale.
CSCws11743	DMM TS correction on 1-Gigabit Ethernet interfaces requires the ingress-port SSP value.
CSCwu12973	Vendor information is not displayed for optics in the show controller speed CLI.
CSCww29358	Continuous MACsec session flaps on 10-Gigabit Ethernet subinterfaces after optics OIR.
CSCwv82429	After the router reload, the system encounters an " unable to open trace file" error, which prevents the Active RP from completing its startup sequence. This failure leads to a watchdog timeout and a subsequent unexpected RP reload once the maximum restart attempt threshold is exceeded.

Known issues

- Cisco 8404-SYS-D is not supported in the MACsec non-key server mode. The minimum rekey interval for the MACsec key server should be set to 30 minutes or greater.
- Ensure that MACsec is not configured before performing a physical optics OIR on 8212-32FH-M, 8711-32FH-M, and 8202-32FH-M routers. If MACsec remains configured during the optics OIR, continuous MACsec session flapping may occur afterward. To recover, reload the system.

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 5. Compatibility matrix for Cisco 8000 Series Routers, Release 26.3.1

Cisco IOS XR	Crosswork	EPNM
Release 26.3.1	Cisco Crosswork Network Controller 6.0	Evolved Programmable Network Manager 8.1.1

Upgrade and downgrade paths

To view all supported Cisco IOS XR Software upgrades from the current version according to the support data installed on the running system, enter the **show install upgrade-matrix running** command:

```
Router# show install upgrade-matrix running all
Thu Sep 10 21:52:00.394 PDT
Matrix: XR version: 26.3.1, File version: 1.0, Version: N/A


The upgrade matrix indicates that the following system upgrades and downgrades are supported
from the current XR version:

From       To         Restrictions
---------- ---------- ----------------------------------------------------
26.3.1     24.2.2     Target fixes; Caveats; Replace performed via reimage
26.3.1     24.2.20    Caveats; Replace performed via reimage
```

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

```
26.3.1     24.2.200   Caveats; Replace performed via reimage
26.3.1     24.2.204   Caveats; Replace performed via reimage
26.3.1     24.2.206   Caveats; Replace performed via reimage
26.3.1     24.2.21    Caveats; Replace performed via reimage
26.3.1     24.2.210   Caveats; Replace performed via reimage
26.3.1     24.2.215   Caveats; Replace performed via reimage
26.3.1     24.2.216   Caveats; Replace performed via reimage
26.3.1     24.3.2     Target fixes; Caveats; Replace performed via reimage
26.3.1     24.3.20    Caveats; Replace performed via reimage
26.3.1     24.3.30    Caveats; Replace performed via reimage
26.3.1     24.4.1     Caveats; Replace performed via reimage
26.3.1     24.4.2     Caveats; Replace performed via reimage
26.3.1     25.1.1     Caveats; Replace performed via reimage
26.3.1     25.1.2     Caveats; Replace performed via reimage
26.3.1     25.1.30    Caveats; Replace performed via reimage
26.3.1     25.2.15    Caveats; Replace performed via reimage
26.3.1     25.2.16    Caveats; Replace performed via reimage
26.3.1     25.2.17    Caveats; Replace performed via reimage
26.3.1     25.2.18    Caveats; Replace performed via reimage
26.3.1     25.2.2     Caveats; Replace performed via reimage
26.3.1     25.2.21    Caveats; Replace performed via reimage
26.3.1     25.3.1     Caveats; Replace performed via reimage
26.3.1     25.4.1     Replace performed via reimage
26.3.1     25.4.15    Replace performed via reimage
26.3.1     25.4.2     Replace performed via reimage
26.3.1     25.4.201   Replace performed via reimage
26.3.1     25.4.30    Replace performed via reimage
26.3.1     26.1.1     Replace performed via reimage
26.3.1     26.1.2     Replace performed via reimage
26.3.1     26.2.1     Replace performed via reimage
26.3.1     26.2.100   Replace performed via reimage
26.3.1     26.2.101   Replace performed via reimage
26.3.1     26.2.2     Replace performed via reimage
26.3.1     26.2.300   Replace performed via reimage
26.3.1     7.11.21    Target fixes; Caveats; Replace performed via reimage
```

```
Add the from and to versions to the end of the CLI command, for data on versions with
additional restrictions

For example, to display restrictions for the 26.3.1->24.2.2 upgrade, use
        'show install upgrade-matrix running 26.3.1 24.2.2''
```

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

Software version

Log in to the router and enter the **show version** command:

```
RP/0/RP0/CPU0#show version
Thu Sep 10 15:28:13.968 PDT
Cisco IOS XR Software, Version 26.3.1 LNT
Copyright (c) 2013-2026 by Cisco Systems, Inc.

Build Information:
 Built By     : swtools
 Built On     : Thu Sep 10 08:16:44 UTC 2026
 Build Host   : iox-ucs-1018
 Workspace    : /auto/srcarchive13/prod/26.3.1/8000/ws
 Version      : 26.3.1
 Label        : 26.3.1-2631_renum

cisco 8000 (Intel(R) Xeon(R) CPU D-1530 @ 2.40GHz)
cisco 8201-24H8FH (Intel(R) Xeon(R) CPU D-1530 @ 2.40GHz) processor with 32GB of memory
R1 uptime is 3 hours, 50 minutes
```

Supported hardware

Table of supported hardware components and the minimum required software versions.

Table 6. Supported hardware for Cisco 8010 Series Routers

Part Number	Description	Support Initially Provided in IOS XR Release
Cisco 8010 Series Routers - Chassis		
8011-12G12X4Y-A	Cisco 8011 12x1G, 12x1/10G, 4X1/10/25G	Release 25.4.1
8011-12G12X4Y-D	Cisco 8011 12x1G, 12x1/10G, 4X1/10/25G	Release 25.4.1
8011-32Y8L2H2FH	Cisco 8010 32X25G SFP28, 8x50G, 2x100GQSFP28, 2x400G QSFP-DD	Release 25.4.1
8011-4G24Y4H-I	Cisco 8010 1 RU Fixed System - 4 QSFP28 100GbE, 24 SFP28 25GbE, and 4 RJ-45 100MbE	Release 25.1.1
Cisco 8010 Series Routers - Power Supply Unit (PSU)		
PWR-650-AC-R	Cisco 650W AC Power Module	Release 25.4.1
PWR-930-DC-R	Cisco 930W DC Power Module	Release 25.4.1
PWR-400-AC	Cisco 400W AC Power Module	Release 25.1.1
PWR-400-DC	Cisco 400W DC Power Module	Release 25.1.1

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

Table 7. Supported hardware for Cisco 8200 Series Routers

Part Number	Description	Support Initially Provided in IOS XR Release
Cisco 8200 Series Routers - Chassis		
8201-32FH	Cisco 8200 1 RU Fixed System - 32 QSFP56-DD 400GbE	Release 7.3.15
8201-24H8FH	Cisco 8200 1 RU Fixed System - 8 QSFP56-DD 400GbE and 24 QSFP28 100GbE	Release 7.7.1
8202-32FH-M	Cisco 8200 2 RU Fixed System - 32 QSFP56-DD 400GbE with MACsec	Release 7.5.2
8212-48FH-M	Cisco 8200 2 RU Fixed System - 24 QSFP-DD 800G or 48 QSFP56-DD 400GbE with MACsec	Release 24.3.1
Cisco 8200 Series Routers - Power Supply Unit (PSU)		
PSU1.4KW-ACPI	Cisco 1.4KW AC Power Module with Port-side Air Intake	Release 7.0.12
PSU1.4KW-ACPE	Cisco 1.4KW AC Power Module with Port-side Air Exhaust	Release 7.0.12
PSU2KW-ACPI	Cisco 2KW AC Power Module with Port-side Air Intake	Release 7.3.1
PSU2KW-ACPE	Cisco 2KW AC Power Module with Port-side Air Exhaust	Release 7.3.1
PSU3KW-HVPI	Cisco 3KW HV AC/DC Power Supply Unit	Release 7.5.3

Table 8. Supported hardware for Cisco 8400 Series Routers

Part Number	Description	Support Initially Provided in IOS XR Release
Cisco 8400 Series Routers - Chassis		
8404-SYS-D	Cisco 8404 - 4-Slot Centralized Chassis	Release 26.1.1
Cisco 8400 Series Routers - Modular Port Adapters (MPA)		
84-MPA-2H12Z-M	Cisco 8404 MPA with 2x100G QSFP28 + 12x1/10/25/50G SFP56	Release 26.1.1
84-MPA-2FH/6H-M	Cisco 8404 MPA with 2x400G / 6x100G QSFP56-DD	Release 26.1.1
Cisco 8400 Series Routers - Power Entry Module (PEM)		
8404-DC-PEM	Cisco 8404 DC Power Entry Module	Release 26.1.1

Table 9. Supported hardware for Cisco 8600 Series Routers

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

Part Number	Description	Support Initially Provided in IOS XR Release
Cisco 8600 Series Routers - Chassis		
8608	Cisco 8600 7 RU Centralized System	Release 7.10.1
Cisco 8600 Series Routers - Modular Port Adapters (MPA)		
86-MPA-14H2FH-M	Cisco 8608 MPA - 2 QSFP-DD 400GbE and 14 QSFP / 16 QSFP 100GbE	Release 7.10.1
86-MPA-24Z-M	Cisco 8608 MPA - 24 SFP56 10/25/50 GbE	Release 7.10.1
86-MPA-4FH-M	Cisco 8608 MPA - 4 QSFP-DD 400GbE	Release 7.10.1
Cisco 8600 Series Routers - Power Supply Unit (PSU)		
PSU3.2KW-ACPI	Cisco 3.2-kW AC Power Supply Unit	Release 7.10.1
PSU3.2KW-DCPI	Cisco 3.2-kW DC Power Supply Unit	Release 7.10.1
PSU4.3KW-HVPI	Cisco 4.3KW HV AC/DC Power Supply Unit	Release 7.10.1

Table 10. Supported hardware for Cisco 8700 Series Routers

Part Number	Description	Support Initially Provided in IOS XR Release
Cisco 8700 Series Routers - Chassis		
8711-28H8F-M	Cisco 8700 1 RU Fixed System - 8 QSFP-DD and 28 QSFP28 ports	Release 26.3.1
8711-48Z-M	Cisco 8700 1 RU Fixed System - 6 QSFP-DD, 4 QSFP56, and 48 SFP56 ports	Release 25.4.1
8711-32FH-M	Cisco 8700 1 RU Fixed System - 16 QSFP-DD800 and 16 QSFP56-DD	Release 24.3.1
8712-MOD-M	Cisco 8700 2 RU Fixed System	Release 24.4.1
Cisco 8700 Series Routers - Modular Port Adapters (MPA)		
8K-MPA-4D	Cisco 8712 MPA - 4 QSFP-DD 400GbE	Release 24.4.1
8K-MPA-16H	Cisco 8712 MPA - 16 QSFP-28 100GbE	Release 24.4.1
8K-MPA-16Z2D	Cisco 8712 MPA - 2 QSFP-DD 400GbE, 2 QSFP-DD 200GbE, and 16 SFP 50GbE	Release 24.4.1
8K-MPA-18Z1D	Cisco 8712 MPA - 1 QSFP-DD 400 GbE and 18 zSFP56+ 50GbE	Release 25.1.1
Cisco 8700 Series Routers - Power Supply Unit (PSU)		
PSU2KW-ACPI	Cisco 8711-32FH-M PSU - 2KW AC Power Module with Port-side Air Intake	Release 24.3.1

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

Part Number	Description	Support Initially Provided in IOS XR Release
PSU2KW-ACPE	Cisco 8711-32FH-M PSU – 2KW AC Power Module with Port-side Air Exhaust	Release 24.3.1
PSU2KW-DCPI	Cisco 8711-32FH-M PSU – 2KW DC Power Module with Port-side Air Intake	Release 24.3.1
PSU2KW-DCPE	Cisco 8711-32FH-M PSU – 2KW DC Power Module with Port-side Air Exhaust	Release 24.3.1
PSU2KW-DCPI	Cisco 8712-MOD-M PSU – 2KW 48V DC Power Module with Port-side Air Intake	Release 24.4.1
PSU2KW-DCPE	Cisco 8712-MOD-M PSU – 2KW 48V DC Power Module with Port-side Exhaust	Release 24.4.1
PSU2KW-ACPI	Cisco 8712-MOD-M PSU – 2KW AC Power Module with Port-side Air Intake	Release 24.4.1
PSU2KW-ACPE	Cisco 8712-MOD-M PSU – 2KW AC Power Module with Port-side Exhaust	Release 24.4.1

Table 11. Supported hardware for Cisco 8800 Series Routers

Part Number	Description	Support Initially Provided in IOS XR Release
Cisco 8800 Series Routers - Chassis		
8804-SYS	Cisco 8800 Modular System - 10 RU with 4 Line Card Slots	Release 7.3.2
8808-SYS	Cisco 8800 Modular System - 16 RU with 8 Line Card Slots	Release 7.0.12
8812-SYS	Cisco 8800 Modular System - 21 RU with 12 Line Card Slots	Release 7.0.12
8818-SYS	Cisco 8800 Modular System - 33 RU with 18 Line Card Slots	Release 7.0.14
Cisco 8800 Series Routers - Route Processors		
8800-RP	Cisco 8800 Route Processor - 4 Core	Release 7.0.12
8800-RP2	Cisco 8800 Route Processor - 8 Core	Release 7.11.1
Cisco 8800 Series Routers - Fabric Modules		
8808-FC	Cisco 8808 System Fabric Module - Q100-based fabric modules with 14.4T per LC slot	Release 7.0.12
8812-FC	Cisco 8812 System Fabric Module - Q100-based fabric modules with 14.4T per LC slot	Release 7.0.12
8818-FC	Cisco 8818 System Fabric Module - Q100-based fabric modules with 14.4T per LC slot	Release 7.0.14
8808-FC0	Cisco 8808 System Fabric Module - Q200-based fabric modules with 14.4T per LC slot	Release 7.3.15
8818-FC0	Cisco 8818 System Fabric Module - Q200-based fabric modules with 14.4T per LC slot	Release 7.3.16

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

Part Number	Description	Support Initially Provided in IOS XR Release
8804-FC0	Cisco 8804 System Fabric Module - Q200-based fabric modules with 14.4T per LC slot	Release 7.3.16
8808-FC1	Cisco 8808 System Fabric Module - F100-based fabric modules with 28.8T per LC slot	Release 24.2.1
8804-FC1	Cisco 8804 System Fabric Module - F100-based fabric modules with 28.8T per LC slot	Release 25.1.1
8818-FC1	Cisco 8818 System Fabric Module - F100-based fabric modules with 76T per LC slot	Release 26.1.1
Cisco 8800 Series Routers - Line Cards		
8800-LC-48H	Cisco 8800 Line Card with MACsec - Q100 ASIC based 4.8 Tbps line card	Release 7.0.12
8800-LC-36FH	Cisco 8800 Line Card - Q100 ASIC based 14.4 Tbps line card	Release 7.0.12
88-LC0-36FH	Cisco 8800 Line Card - Q200 ASIC based 14.4 Tbps line card	Release 7.3.15
88-LC0-36FH-M	Cisco 8800 Line Card with MACsec- Q200 ASIC based 14.4 Tbps line card	Release 7.3.15
88-LC0-34H14FH	Cisco 8800 Line Card - Q200 ASIC based 9 Tbps line card	Release 7.3.3 Release 7.5.1
88-LC1-36EH	Cisco 8800 Line Card - P100 ASIC based 28.8 Tbps line card	Release 24.2.11
88-LC1-12TH24FH-E	Cisco 8800 Line Card - P100 ASIC based 12 Tbps line card	Release 24.3.1
88-LC1-52Y8H-EM	Cisco 8800 Line Card - P100 ASIC based 3.7 Tbps line card	Release 24.3.1
88-LC1-16H16F-EM	Cisco 8800 Line Card - K100 ASIC based 9.6 Tbps line card	Release 26.3.1
88-LC1-48Y8H-EM	Cisco 8800 Line Card - K100 ASIC based 4.8 Tbps line card	Release 26.3.1
Cisco 8800 Series Routers - Power Supply Unit (PSU)		
PSU4.8KW-DC100	4.8KW 48V 100A DC Power Supply	Release 7.3.2
PSU6.3KW-HV	6.3KW AC/HVAC/HVDC Power Supply	Release 7.0.12
PSU6.3KW-20A-HV	6.3KW AC/HVAC/HVDC Power Supply-20A	Release 7.0.12
Cisco 8800 Series Routers - FAN		
8812-FAN-V2	Cisco 8812 12-slot chassis	26.3.1
8818-FAN-V2	Cisco 8818 18-slot chassis	26.2.1
8808-FAN-V2	Cisco 8808 8-slot chassis	26.2.1

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

Part Number	Description	Support Initially Provided in IOS XR Release
8804-FAN-V2	Cisco 8804 4-slot chassis	26.2.1
8804-FAN	Cisco 8804 4-slot chassis	7.3.2
8818-FAN	Cisco 8818 18-slot chassis	7.0.14
8812-FAN	Cisco 8812 12-slot chassis	7.0.12
8808-FAN	Cisco 8808 8-slot chassis	7.0.12

Supported software packages

Overview of Cisco IOS XR software

The Cisco IOS XR software is composed of a base image (ISO) that provides the XR infrastructure. The ISO image is made up of a set of packages (also called RPMs). These packages are of three types:

A mandatory package that is included in the ISO

An optional package that is included in the ISO

An optional package that is not included in the ISO
Visit the Cisco Software Download page to download the Cisco IOS XR software images.

View installed software packages

To determine the Cisco IOS XR Software packages installed on your router, log in to the router and enter the **show install active** command. To view the optional and bug fix RPM packages, first install the package and use the **show install active summary** command.

To know about all the RPMs installed including XR, OS and other components use the **show install active all** command.

Flexible software modularity

The software modularity approach provides a flexible model that allows you to install a subset of IOS XR packages on devices based on your individual requirements. All critical components are modularized as packages so that you can select the features that you want to run on your router.

Determine firmware support

To determine firmware support on your router, log in to the router and enter **show fpd package** command.

Related resources

Table 12. 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 *Ask AI About This Product* tab for further information.
Cisco 8000 documentation	Provides CDC documentation for Cisco 8000 series routers.

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

Resource	Description
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.
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.