Release Notes for Cisco C9350 Series Smart Switches, Release Cisco IOS XE 26.2.x

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

Cisco C9350 Series Smart Switches, Release Cisco IOS XE 26.2.x 3
New software features 3
New hardware features 5
Changes in behavior 6
Resolved issues 7
Open issues 7
Known issues 7
Compatibility 7
Supported hardware 7
Supported software packages 9
Related resources 10
Legal information 12

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

Cisco C9350 Series Smart Switches, Release Cisco IOS XE 26.2.x

Cisco C9350 Series Smart Switches are fixed-access switches based on the Silicon-One ASIC architecture. The primary position of these switches is in a campus access network. You can also position these switches in campus distribution or collapsed core networks. A distribution network focuses on connecting one or more access layers to the core layer, and a collapsed core network connects multiple distribution layers to other network domains.

Look up Cisco Feature Navigator for the complete list of supported features.

New software features

This section provides a brief description of the new software features introduced in Cisco IOS XE 26.2.x releases.

Software Features in Cisco IOS XE 26.2.1

Table 1. New software features for Cisco C9350 Series Smart Switches, Release Cisco IOS XE 26.2.1

Product impact	Feature	Description
Ease of Setup	Local Area Bonjour in Multicast DNS (mDNS)	Local Area Bonjour in Multicast DNS (mDNS) enables devices to discover local network services across LAN and wireless network segments. You can configure service definitions, service lists, and service policies to control the Bonjour service traffic allowed on each VLAN interface. Wireless deployments require transparent mDNS forwarding through the wireless LAN controller.
Ease of Setup	Port Security	Port Security restricts access to an interface by limiting and identifying the MAC addresses allowed on the port. It prevents traffic from unknown source MAC addresses and helps control device access to the network. You can configure static, dynamic, or sticky secure MAC addresses, set the maximum number of allowed addresses, and define actions for violations, including protect, restrict, shutdown, or shutdown VLAN.
Ease of Use	FQDN Redirect ACL	FQDN Redirect ACLs simplify web redirection by allowing policies to use fully qualified domain names instead of static IP addresses. The switch dynamically resolves domain names through DNS snooping and programs the resolved IPv4 or IPv6 addresses in hardware for traffic filtering. The feature integrates with central web authentication and supports FQDNs in both redirect ACLs and redirect URLs.
Software Reliability	IPsec	IPsec secures sensitive data over unprotected networks by providing confidentiality, integrity, authentication, and anti-replay protection. It uses IKEv2 to negotiate security associations between peers and supports ESP tunnel mode with GCM128 or GCM256 transforms. IPsec also supports IPv4 Static Virtual Tunnel Interfaces (SVTIs), which use IP routing to forward traffic through encrypted tunnels and support unicast and multicast traffic.
Software Reliability	IPv6 Prefix Guard	The IPv6 Prefix Guard feature operates within the IPv6 source guard framework to ensure that only traffic from topologically correct source addresses is permitted.
Software Reliability	Live Protect	Live Protect validates security shields that protect Cisco products without requiring device reloads or service interruptions. You can deploy security shields in two modes:

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

Product impact	Feature	Description
		• Monitoring mode: Provides visibility into potential exploit attempts without enforcement, allowing you to assess threats before taking action. • Enforce (Protecting) mode: Actively applies mitigation policies to reduce exposure to known vulnerabilities. Live Protect allows you to monitor, enforce, disable, and retire the security shields enabling a smooth transition to remediation. This capability helps businesses maintain continuous operations while managing risks until the software upgrades or patches are deployed.
Software Reliability	MAC/MATM Static MAC Entry	Support for static MAC address drop entries in the MAC Address Table Manager (MATM) has been introduced.
Software Reliability	Multicast VPN-Rosen with PIM + GRE encapsulation (Rosen) IPv4/IPv6	Multicast VPN (mVPN) using the Rosen model is a mechanism for carrying IP multicast traffic across an MPLS/IP backbone, enabling service providers or large enterprises to deliver multicast services over a shared network infrastructure while maintaining per-VPN routing isolation.
Software Reliability	Negotiated port-speed	On-change subscriptions support negotiated-port-speed leaf to enable real-time notifications along with the existing subscription-based access.
Software Reliability	Flexible NetFlow enhancements	The following enhancements have been introduced for Flexible NetFlow: • Layer 2 fields, M/N sampling, multicast ingress, TCP flags, and VRF-aware NDE export • AVC ACE support to learn flows only for TCP/UDP packets • Multicast traffic on SVI or Layer 3 • Layer 3 AC and FWD VLAN ingress • New insight commands
Software Reliability	PQC dual-sign support	Dual signing enhances software authenticity and integrity by preparing systems for post quantum cryptographic requirements while maintaining backward compatibility. This approach adds both a legacy RSA signature and a quantum-resistant ML-DSA-87 signature to IOS-XE software images. Supported platforms verify the stronger quantum-resistant seal, while older systems continue to rely on the existing RSA signature. This method ensures seamless operation in mixed environments and reduces disruption during the transition to next-generation security standards.
Software Reliability	Resilient Infrastructure changes	As part of Cisco's Resilient Infrastructure program and Cisco's commitment to secure infrastructure, this release includes additional changes aimed towards continuing to make Cisco IOS XE more secure by default. Note that some of these changes may require operational changes if you are not following secure best practices. This release includes the following changes: • The RADIUS client appends the Message-Authenticator attribute (Attribute 80 HMAC-MD5) to all outgoing Access-Request packets to mitigate cryptographic forgery and Blast-RADIUS vulnerabilities (CVE-2024-3596). • The RADIUS client drops incoming Access-Accept, Access-Reject, and Access-Challenge packets if the Message-Authenticator packet is absent or invalid. Ensure AAA servers (example, Cisco ISE) are configured to return Attribute 80.

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

Product impact	Feature	Description
		• Outbound SSH connections enforce Trust-On-First-Use (TOFU). The device prompts to verify and store remote server host keys in the known-hosts database on first connection and validates against them on subsequent sessions. • Proxy ARP is disabled by default across all routed interfaces, SVIs, and subinterfaces to reduce Layer 2 broadcast domains and prevent ARP spoofing. Configure the **ip proxy-arp** command explicitly if required. • The embedded web server daemon is disabled by default on factory configurations to restrict unauthenticated management access. Web UI and RESTCONF require explicit enablement of the **ip http secure-server** command. • The IOS XE device rejects unauthenticated NTP Mode 6 and Mode 7 control queries (monlist) to prevent NTP reflection and amplification DDoS attacks. Standard time synchronization (Modes 3 and 4) is unaffected. • System logging timestamps automatically include the four-digit calendar year (service timestamps log datetime msec year) to standardize multi-year audit logs and SIEM compliance. • Integrates Linux auditd inside Cisco IOx Guest Shell. All commands, system calls, and privilege escalation events (sudo) executed inside the container are forwarded to the host syslog facility. • Warning messages are emitted on the console and logged to syslog whenever legacy insecure protocols (telnet, ftp, tftp, http) are enabled in the configuration. • Real-time tracking of active insecure services is published to the operational database (operDB) and YANG data models, allowing management controllers (such as Cisco Catalyst Center) to monitor security compliance. For more information, refer Resilient Infrastructure.
Software Reliability	Storm Control PPS	Storm Control Packets Per Second (pps) option support has been introduced.
Software Reliability	Switch-to-host MACsec encryption	MACsec is the IEEE 802.1AE standard for authenticating and encrypting packets between two MACsec-capable devices. Support for switch-to-host MACsec encryption was introduced.

New hardware features

This section provides a brief description of the new hardware features introduced in Cisco IOS XE 26.2.x releases.

Hardware Features in Cisco IOS XE 26.2.1

Table 2. New hardware features for Cisco C9350 Series Smart Switches, Release Cisco IOS XE 26.2.1

Product impact	Feature	Description
Hardware Reliability	10GBASE SFP+ Modules	Supported transceiver module product number: • SFP-10G-T-X Compatible network module: • C9350-NM-8L • C9350-NM-8Y Compatible switch models:

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

Product impact	Feature	Description
		• C9350-12Y • C9350-24Y For information about the module, see Cisco 10GBASE SFP+ Modules Data Sheet. For information about device compatibility, see the Transceiver Module Group (TMG) Compatibility Matrix.
Hardware Reliability	100BASE-X Small Form-Factor Pluggable Modules for Fast Ethernet Applications	Supported transceiver module product number: • GLC-GE-100FX **Note**: The LED remains solid instead of blinking green due to a hardware limitation. Compatible switch models: • C9350-24S • C9350-48S For information about the module, see Cisco 100BASE-X Small Form-Factor Pluggable Modules for Fast Ethernet Applications Data Sheet. For information about device compatibility, see the Transceiver Module Group (TMG) Compatibility Matrix.
Hardware Reliability	Cisco C9350 Series Smart Switches	The following new models are introduced in the series: • C9350-12Y: Stackable 12 x 1/10/25 G SFP+ ports, supports StackWise-1.6T. • C9350-24Y: Stackable 24 x 1/10/25 G SFP+ ports, supports StackWise-1.6T. • C9350-48HM: Stackable 48 x 10/100 M and 1/2.5 GE MultiGigabit Ethernet downlink ports; UPoE+ budget of 90W, supports StackWise-1.6T.
Hardware Reliability	Cisco C9350 Network Modules	Support network module numbers: • C9350-NM-8L: Eight 1/10/25/50 GE slots with a SFP56 connector in each slot. Compatible switch models: • C9350-NM-8L: C9350-24Y, C9350-48HX, C9350-48TX

Changes in behavior

This section provides a brief description of the behavior changes introduced in Cisco IOS XE 26.2.x releases.

Hardware and Software Behavior Changes in Cisco IOS XE 26.2.1

Table 3. Behavior changes for Cisco C9350 Series Smart Switches, Release Cisco IOS XE 26.2.1

Description	Behavior changes
CDP and LLDP device ID	In cloud-managed mode, CDP and LLDP use the device hostname as the device ID instead of the switch MAC address.
Port-channel VLAN configuration synchronization	When the **switchport trunk allowed vlan** command is applied to a portchannel via the configuration database (CDB) or NETCONF, the inherited configurations on member interfaces do not synchronize with the CDB database.

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

Description	Behavior changes
PPS coexistence with percentage and BPS configuration	The device enforces either packets per second (PPS) mode or bandwidth mode system-wide. PPS cannot coexist with percentage or bits per second (BPS) based storm-control configurations, and conflicting commands are rejected. Percentage and BPS configurations can coexist because both use bandwidth mode.
show platform software fed switch active fabric udp command	The **show platform software fed switch active fabric udp** command is introduced.

Resolved issues

This section lists the resolved issues in Cisco IOS XE 26.2.x releases.

Resolved Caveats in Cisco IOS XE 26.2.1

Table 4. Resolved issues for Cisco C9350 Series Smart Switches, Release Cisco IOS XE 26.2.1

Bug ID	Description
CSCwt07089	Catalyst 9350: SNMP VLAN contexts (vlan-xxx) are not automatically created for BRIDGE-MIB polling in IOS XE 17.18.1

Open issues

This table lists the open issues in Cisco IOS XE 26.2.x releases.

Table 5. Open issues for Cisco C9350 Series Smart Switches, Release Cisco IOS XE 26.2.x

Bug ID	Description
CSCww53939	9350-48HX/24HX : Port 7 Packet loss encountered when using Intel i219-LM network card on this port

Known issues

There are no known limitations in Cisco IOS XE 26.2.x releases.

Compatibility

To view the software compatibility information between Cisco C9350 Series Smart Switches, Cisco Identity Services Engine, and Cisco Prime Infrastructure, go to Cisco C9000 Series Smart Switches Software Version Compatibility Matrix.

Supported hardware

This section lists the hardware support information.

Supported Cisco C9350 Series Smart Switches model numbers

The following table lists the supported hardware models and the default license levels they are delivered with.

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

Table 6. Cisco C9350 Series Smart Switches model numbers

Switch model	Description	Introductory release
C9350-24HX	Stackable 24 10/100 M and 1/2.5/5/10 GE Multigigabit Ethernet downlink ports; UPoE+ budget of 90W, supports Stackwise-1.6T	Cisco IOS XE 26.1.1a
C9350-48HXN	Stackable 36 10/100 M and 1/2.5/5 GE and 12 10/100 M and 1/2.5/5/10 GE Multigigabit Ethernet downlink ports, UPoE+ budget of 90W, supports Stackwise-1.6T	Cisco IOS XE 26.1.1a
C9350-24P	Stackable 24 1G and 10/100M downlink ports, PoE+ budget of 30W, supports Stackwise-1.6T	Cisco IOS XE 17.18.1
C9350-24T	Stackable 24 1G and 10/100M downlink ports, supports Stackwise-1.6T	Cisco IOS XE 17.18.1
C9350-24U	Stackable 24 1G and 10/100M downlink ports. UPoE+ budget of 60W, supports Stackwise-1.6T	Cisco IOS XE 17.18.1
C9350-48HX	Stackable 48 10/100M and 1/2.5/5/10GE Multigigabit Ethernet downlink ports; UPoE+ budget of 90W, supports Stackwise-1.6T	Cisco IOS XE 17.18.1
C9350-48P	Stackable 48 1G and 10/100M downlink ports, PoE+ budget of 30W, supports Stackwise-1.6T	Cisco IOS XE 17.18.1
C9350-48T	Stackable 48 1G and 10/100M downlink ports, supports Stackwise-1.6T	Cisco IOS XE 17.18.1
C9350-48TX	Stackable 48 10/100 M and 1/2.5/5/10GE Multigigabit Ethernet downlink ports, supports Stackwise-1.6T	Cisco IOS XE 17.18.1
C9350-48U	Stackable 48 1G and 10/100 M downlink ports, UPoE+ budget of 60 W, supports Stackwise-1.6T	Cisco IOS XE 17.18.1

Supported network modules

The following table lists the optional uplink network modules with 1-Gigabit, 10-Gigabit, 25-Gigabit, 40-Gigabit slots, and 100-Gigabit slots. You should only operate the switch with either a network module or a blank module installed.

Table 7. Supported network modules

Network Module	Description	Introductory release
C9350-NM-2C	Two 40/100GE slots with a QSFP28 connector in each slot	Cisco IOS XE 17.18.1
C9350-NM-4C	Four 40/100GE slots with a QSFP28 connector in each slot	Cisco IOS XE 17.18.1
C9350-NM-8Y	Eight 1/10/25GE or four 50GE slots with an SFP28 port in each slot	Cisco IOS XE 17.18.1

Supported optics modules

Cisco Catalyst Series Switches support a wide range of optics and the list of supported optics is updated on a regular basis. Use the Transceiver Module Group (TMG) Compatibility Matrix tool, or consult the tables at this URL for the latest transceiver module compatibility

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

information: https://www.cisco.com/en/US/products/hw/modules/ps5455/products_device_support_tables_list.html

Supported software packages

This section provides information about the release packages associated with Cisco C9350 Series Smart Switches.

Finding the software version

The package files for the Cisco IOS XE software are stored on the system board flash device (flash:).

You can use the **show version** privileged EXEC command to see the software version that is running on your switch.

Note: Although the **show version** output always shows the software image running on the switch, the model name shown at the end of this display is the factory configuration and does not change if you upgrade the software license.

You can also use the **dir** *filesystem:* privileged EXEC command to see the directory names of other software images that you might have stored in flash memory.

Finding the software Images

Table 8. Software images

Release	Image type	File name
Cisco IOS XE 26.2.1	CISCO9K_IOSXE	cisco9k_iosxe.26.2.01.SPA.bin
	No Payload Encryption (NPE)	cisco9k_iosxe_npe.26.2.01.SPA.bin

To download software images, visit the software downloads page: Cisco C9350 Series Smart Switches.

ROMMON versions

ROMMON, also known as the boot loader, is firmware that runs when the device is powered up or reset. It initializes the processor hardware and boots the operating system software (Cisco IOS XE software image). The ROMMON is stored on the following Serial Peripheral Interface (SPI) flash devices on your switch:

- Primary: The ROMMON stored here is the one the system boots every time the device is powered-on or reset.
- Golden: The ROMMON stored here is a backup copy. If the one in the primary is corrupted, the system automatically boots the ROMMON in the golden SPI flash device.

ROMMON upgrades may be required to resolve firmware defects, or to support new features, but there may not be new versions with every release.

Table 9. ROMMON versions

Release	ROMMON Version
26.2.1	26.2.1r
26.1.2	17.18.1r[FC3]
26.1.1a	17.18.1r[FC3]

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

Release	ROMMON Version
17.18.2	17.18.1r[FC3]
17.18.1	17.18.1r[FC3]

Field-programmable gate array version upgrade

A field-programmable gate array (FPGA) is a type of programmable memory device that exists on Cisco switches. They are re-configurable logic circuits that enable the creation of specific and dedicated functions.

To check the current FPGA version, enter the **version -v** command in ROMMON mode.

Notes:

- Not every software release has a change in the FPGA version.
- The version change occurs as part of the regular software upgrade, and you do not have to perform any other additional steps.

Related resources

This section provides troubleshooting information, links to the product documentation, and licensing information.

Troubleshooting

For the most up-to-date, detailed troubleshooting information, see the Cisco TAC website at Support & Downloads.

Go to Product Support and select your product from the list or enter the name of your product. Look under Troubleshoot and Alerts, to find information for the problem that you are experiencing.

Accessing hidden commands

Hidden commands have always been present in Cisco IOS XE but were not equipped with CLI help. That is, entering a question mark (?) at the system prompt did not display the list of available commands. These commands were only meant to assist Cisco TAC in advanced troubleshooting and were not documented either.

Hidden commands are available under:

- Category 1—Hidden commands in privileged or User EXEC mode. Begin by entering the **service internal** command to access these commands.
- Category 2—Hidden commands in one of the configuration modes (global, interface and so on). These commands do not require the **service internal** command.

Further, the following applies to hidden commands under Category 1 and 2:

- The commands have CLI help. Enter enter a question mark (?) at the system prompt to display the list of available commands.
- **Note**: For Category 1, enter the **service internal** command before you enter the question mark; you do not have to do this for Category 2.

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

- The system generates a %PARSER-5-HIDDEN syslog message when a hidden command is used. For example:

```
*Feb 14 10:44:37.917: %PARSER-5-HIDDEN: Warning!!! 'show processes memory old-header '
is a hidden command.

Use of this command is not recommended/supported and will be removed in future.
```

Apart from category 1 and 2, there remain internal commands displayed on the CLI, for which the system does NOT generate the %PARSER-5-HIDDEN syslog message.

Important: We recommend that you use any hidden command only under TAC supervision.

If you find that you are using a hidden command, open a TAC case for help with finding another way of collecting the same information as the hidden command (for a hidden EXEC mode command), or to configure the same functionality (for a hidden configuration mode command) using non-hidden commands.

Related documentation

For all support documentation of Cisco C9350 Series Smart Switches, visit Cisco C9350 Series Smart Switches.

For information about Cisco IOS XE, visit Cisco IOS XE.

For information about Cisco IOS XE releases, visit Networking Software (IOS & NX-OS).

For Cisco Validated Designs documents, visit Cisco Validated Design Zone.

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at Cisco Feature Navigator.

Communications, services, and additional information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business results you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco DevNet.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Licensing

For information about licenses required for the features available on Cisco 9000 Series Smart Switches, see Cisco Networking Subscription for Cisco C9000 Series Smart Switches.

Cisco bug search tool

Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.

Documentation feedback

To provide technical feedback on this document, or to report an error or omission, send your comments to cisco9k-docfeedback@cisco.com.

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

Legal information

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2026 Cisco Systems, Inc. All rights reserved.