Release Notes for Cisco C9350 Series Smart Switches, Release Cisco IOS XE 26.1.x

Cisco C9350 Series Smart Switches, Release Cisco IOS XE 26.1.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 this release.

Table 1. New software features for Cisco C9350 Series Smart Switches, Release Cisco IOS XE 26.1.1

Product impact	Feature	Description
Software Reliability	Application Visibility and Control-based QoS	Application Visibility and Control (AVC) enhances network performance by enabling precise traffic management and prioritization based on application recognition. It achieves this through deep packet inspection using Network-Based Application Recognition (NBAR) to classify IPv4 and IPv6 TCP/UDP applications. AVC incorporates Flexible NetFlow to include application names in flow records and supports AVC-QoS, allowing QoS policies to match protocols in class maps, thereby optimizing resource use and reducing congestion in wired networks.
Software Reliability	Dynamic protocol switching for communication between network devices and policy servers	Network devices can now switch the transport protocols and seamlessly download the security group access control list (SGACL) policies from the policy server (ISE), without any policy persistence or data traffic issues. This feature introduces the capability to dynamically switch between RADIUS and HTTPS protocols for communication between the policy server and the network device.
Software Reliability	IPv6 Source Guard	IPv6 Source Guard validates the source of IPv6 traffic to prevent source address spoofing.
Software Reliability	MACsec Encryption	MACsec is the IEEE 802.1AE standard for authenticating and encrypting packets between two MACsec-capable devices.
Software Reliability	Resilient Infrastructure	As part of the ongoing commitment to network security, this release introduces secure alternatives to legacy commands. These updates are designed to mitigate potential risks and assist in establishing a more robust and secure operational baseline. The identified insecure commands are categorized as: • Line transport: Updates to secure remote access methods. • Device server configuration: Hardening of server-side settings. • File transfer protocols: Transitioning to encrypted transfer methods. • SNMP: Enhancements to secure management traffic. • Passwords: Strengthening authentication and credential management. • Miscellaneous: General security improvements for various system functions. The show system insecure configuration command introduced in Cisco IOS XE 17.18.2 release lists all insecure commands

Product impact	Feature	Description
		configured on the device. For all detected insecure configurations during device boot or upgrade, error messages are displayed. In Cisco IOS XE 26.1.1 release, all insecure CLI commands are blocked by default to strengthen your network infrastructure. If your environment requires the use of a legacy command, you must enable the system mode insecure command in global configuration mode. • Recommendation: Do not use insecure mode. This mode is temporary and will be removed in a future release. Identify and replace all insecure commands with their secure alternatives. • Upgrade behavior: If you upgrade to Cisco IOS XE 26.1.1 release with insecure commands already present in the running configuration, the system mode insecure command is automatically added to your configuration to prevent service disruption. For more information, refer this document Cisco C9000 Switching IOS XE – Resilient Infrastructure Playbook.
Software Reliability	Spanning Tree Protocol	Introduces support for Spanning Tree Protocol (STP) in Layer 2 switching mode.

New hardware features

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

Table 2. New hardware features for Cisco C9350 Series Smart Switches, Release Cisco IOS XE 26.1.1

Product impact	Feature	Description
Hardware Reliability	25-Gigabit, 50-Gigabit, and 100-Gigabit transceivers	25-Gigabit, 50-Gigabit, and 100-Gigabit transceivers support has been introduced on the Cisco C9350 Series Smart Switches. Compatible line cards: • C9350-NM-8Y: 25-Gigabit, 50-Gigabit • C9350-NM-2C, C9350-NM-4C: 100-Gigabit

Changes in behavior

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

Table 3. Behavior changes for Cisco C9350 Series Smart Switches, Release Cisco IOS XE 26.1.1

Description	Behavior changes
platform ip multicast command modified	A new **ssdp** keyword has been introduced for the **platform ip multicast** command to allow and disable SSDP packet forwarding.
show eee command output modified	On C9350-48HX and C9350-48TX platforms, the **show eee** command output has been modified to remove ASIC status and counter information.
show platform hardware fed command modified	The stackport range in the **show platform hardware fed** command has been updated from <0-1> to <1-2>.

Description	Behavior changes
show platform software fed switch active acl bind sdk command modified	The **detail** keyword of the **show platform software fed switch active acl bind sdk** command has been replaced with {**cell** | **if-id** | **interface** | **svi** | **vlan**} keywords.
Stack port behavior	A stack port is forced to down state if port authentication fails.
Switch number configuration	The system automatically defaults to switch number 1 if the configured switch number exceeds the maximum supported value.

Resolved issues

This table lists the resolved issues in this specific software release.

Table 4. Resolved issues for Cisco C9350 Series Smart Switches, Release Cisco IOS XE 26.1.1

Bug ID	Description
CSCws90617	On booting a switch (with switch number conflict) a few minutes later than the other switches, the switch cannot join the stack

Open issues

There are no open issues in this release.

Known issues

There are no known limitations in this release.

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.

Table 5. Cisco C9350 Series Smart Switches model numbers

Switch model	Description	Introductory release
C9350-24P	Stackable 24 1G and 10/100M downlink ports, PoE+ budget of 30W, supports Stackwise-1.6T	Cisco IOS XE 17.18.1

Switch model	Description	Introductory release
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 6. 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 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 7. Software images

Release	Image type	File name
Cisco IOS XE 26.1.1	CISCO9K_IOSXE	cisco9k_iosxe.26.1.01.SPA.bin
	No Payload Encryption (NPE)	cisco9k_iosxe_npe.26.1.01.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 8. ROMMON versions

Release	ROMMON Version
26.1.1	17.18.1r[FC3]
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.
- 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.

Legal information