Release Notes for Cisco C9350 Series Smart Switches, Release Cisco IOS XE 17.18.x

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

Cisco C9350 Series Smart Switches, Release Cisco IOS XE 17.18.x 3
New software features 3
New hardware features 4
Changes in behavior 4
Resolved issues 4
Open issues 5
Known issues 5
Compatibility 5
Supported hardware 5
Supported software packages 6
Related resources 8
Legal information 10

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

Cisco C9350 Series Smart Switches, Release Cisco IOS XE 17.18.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 17.18.x releases.

Software Features in Cisco IOS XE 17.18.4

There are no new software features introduced in this release.

Software Features in Cisco IOS XE 17.18.3a

There are no new software features introduced in this release.

Software Features in Cisco IOS XE 17.18.2

Table 1. New software features for Cisco C9350 Series Smart Switches, Release Cisco IOS XE 17.18.2

Product impact	Feature	Description
Software Reliability	Audit commands	The **platform security audit monitor** and **show platform software audit** commands have been introduced. These commands provide enhanced visibility into software operational integrity by allowing you to configure and monitor audit rules across network devices.
Software Reliability	Application Visibility and Control	AVC is a solution that provides application-level classification, monitoring, and traffic control. It uses deep packet inspection techniques with the Network-Based Application Recognition (NBAR2) engine to classify applications on the network.
Software Reliability	Fabric-SDA	Introduces Fabric Edge support with foundational LISP, SDA control-plane, and mobility functions.
Software Reliability	Flexible NetFlow byte counter	Bytes counter for Flexible NetFlow collect parameters has been introduced.
Software Reliability	IPv6 multicast key	Introduces full key support for IPv6 multicast.
Software Reliability	L3VPN MPLS	Introduces MPLS L3VPN services, PE-CE routing, and baseline MPLS capabilities including LDP, static labels, VRF routing, and multiprotocol transport.
Software Reliability	MPLS QoS	MPLS QoS feature allows you to classify, mark, and queue network traffic by modifying the MPLS experimental bits field.

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

New hardware features

Hardware Features in Cisco IOS XE 17.18.4

There are no new hardware features introduced in this release.

Hardware Features in Cisco IOS XE 17.18.3a

There are no new hardware features introduced in this release.

Hardware Features in Cisco IOS XE 17.18.2

There are no new hardware features introduced in this release.

Changes in behavior

This section provides a brief description of the behavior changes introduced in Cisco IOS XE 17.18.x releases.

Hardware and Software Behavior Changes in Cisco IOS XE 17.18.4

There are no new behavior changes introduced in this release.

Hardware and Software Behavior Changes in Cisco IOS XE 17.18.3a

There are no new behavior changes introduced in this release.

Hardware and Software Behavior Changes in Cisco IOS XE 17.18.2

Table 2. Behavior changes for Cisco C9350 Series Smart Switches, Release Cisco IOS XE 17.18.2

Description	Behavior changes
show eee command outputs modified	On C9350-48HX and C9350-48TX platforms, the **show eee** command outputs have been modified to remove ASIC status and counter information.

Resolved issues

This section lists the resolved issues in Cisco IOS XE 17.18.x releases.

Resolved Caveats in Cisco IOS XE 17.18.4

There are no resolved caveats in this release.

Resolved Caveats in Cisco IOS XE 17.18.3a

Table 3. Resolved issues for Cisco C9350 Series Smart Switches, Release Cisco IOS XE 17.18.3a

Bug ID	Description
CSCwr67971	9350 - ARP and DHCP fail to be copied to switch control plane on multi-asic switches
CSCwr91942	C9350-48T on 17.18.01: Per Port DHCP doesn't assign static IP's
CSCwt90927	Upgrading a 9350 switch stack from 17.18.1 to 17.18.3 can trigger an unexpected reload during bootloader upgrade, corrupting primary ROMMON and causing fallback to Golden ROMMON

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

Resolved Caveats in Cisco IOS XE 17.18.2

Table 4. Resolved issues for Cisco C9350 Series Smart Switches, Release Cisco IOS XE 17.18.2

Bug ID	Description
CSCws36761	Adding a powered-on 9350 (active) switch directly to a live switch or stack can disrupt operations, or potentially make one or more of the switches unusable.

Open issues

This table lists the open issues in Cisco IOS XE 17.18.x releases.

Table 5. Open issues for Cisco C9350 Series Smart Switches, Release Cisco IOS XE 17.18.x

Bug ID	Description
CSCwh31528	autoconf_asp template pps sub-command not available in CLI
CSCwi68290	QoS Trust: Egress COS marking policy not working for non-IP from untrusted port
CSCwi66552	QoS Trust: Wrong COS value for IP packet switch from DSCP trust port to tagged port.
CSCwi94467	EPC not capturing EAPOL or RADIUS packets
CSCwj01754	EPC does not capture Layer 2 LPTS packets when enabled on an interface
CSCwn66205	ERSPAN: Packets going over SVI is flooded and spanned again when MAC expires before ARP expiry
CSCws47959	On replacing a switch with a different SKU, without removing the old provision, the interface created for the newly switch may be wrong

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 6. Cisco C9350 Series Smart Switches model numbers

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

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
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 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.

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

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 17.18.4	CISCO9K_IOSXE	cisco9k_iosxe.17.18.04.SPA.bin
	No Payload Encryption (NPE)	cisco9k_iosxe_npe.17.18.04.SPA.bin
Cisco IOS XE 17.18.3a	CISCO9K_IOSXE	cisco9k_iosxe.17.18.03a.SPA.bin
	No Payload Encryption (NPE)	cisco9k_iosxe_npe.17.18.03a.SPA.bin
Cisco IOS XE 17.18.2	CISCO9K_IOSXE	cisco9k_iosxe.17.18.02.SPA.bin
	No Payload Encryption (NPE)	cisco9k_iosxe_npe.17.18.02.SPA.bin
Cisco IOS XE 17.18.1	CISCO9K_IOSXE	cisco9k_iosxe.17.18.01.SPA.bin
	No Payload Encryption (NPE)	cisco9k_iosxe_npe.17.18.01.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
17.18.4	17.18.1r[FC3]

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

Release	ROMMON Version
17.18.3a	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.

© 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.

© 2025 Cisco Systems, Inc. All rights reserved.