

Revised: August 8, 2025

Release Notes for Cisco Catalyst 9400 Series Switches, Cisco IOS XE 17.18.x

Document Change History

The document change history outlines the updates and modifications made to this document for a release train.

Table 1: Document Change History

Date	Release	Sections Updated
August 08, 2025	17.18.1	<ul style="list-style-type: none">• What's New: Software features• Caveats: Open and Resolved Caveats• Compatibility Matrix: Compatibility information for 17.18.1• Software Images: Software images for 17.18.1• ROMMON and CPLD Versions: ROMMON Versions for 17.18.1

Introduction

Cisco Catalyst 9400 Series Switches are Cisco's leading modular enterprise switching access platform and have been purpose-built to address emerging trends of Security, IoT, Mobility, and Cloud.

They deliver complete convergence with the rest of the Cisco Catalyst 9000 Series Switches in terms of ASIC architecture with Unified Access Data Plane (UADP) 2.0 and UADP 3.0. The platform runs an Open Cisco IOS XE that supports model driven programmability, has the capacity to host containers, and run 3rd party applications and scripts natively within the switch (by virtue of x86 CPU architecture, local storage, and a higher memory footprint). This series forms the foundational building block for SD-Access, which is Cisco's lead enterprise architecture.

Cisco Catalyst 9400 Series Switches are enterprise optimized with a dual-serviceable fan tray design, side to side airflow, and are closet-friendly with a 16-inch depth

Supported Cisco Catalyst 9400 Series Switches Model Numbers

The following table lists the supported switch models.

Switch Model (append with “=” for spares)	Description	Introductory Release
C9404R	Cisco Catalyst 9400 Series 4 slot chassis <ul style="list-style-type: none"> • Redundant supervisor module capability • Two switching module slots • Hot-swappable, front and rear serviceable, non-redundant fan tray assembly • Four power supply module slots 	Cisco IOS XE Fuji 16.9.1
C9407R	Cisco Catalyst 9400 Series 7 slot chassis <ul style="list-style-type: none"> • Redundant supervisor module capability • Five switching module slots • Hot-swappable, front and rear serviceable fan tray assembly • Eight power supply module slots 	Cisco IOS XE Everest 16.6.1
C9410R	Cisco Catalyst 9400 Series 10 slot chassis <ul style="list-style-type: none"> • Redundant supervisor module capability • Eight switching module slots • Hot-swappable, front and rear serviceable fan tray assembly • Eight power supply module slots 	Cisco IOS XE Everest 16.6.1

Supported Hardware on Cisco Catalyst 9400 Series Switches

Product ID (append with “=” for spares)	Description	Introductory Release
Supervisor Modules		
C9400-SUP-1	Cisco Catalyst 9400 Series Supervisor 1 Module This supervisor module is supported on the C9404R, C9407R, and C9410R chassis.	Cisco IOS XE Everest 16.6.1
C9400-SUP-1XL	Cisco Catalyst 9400 Series Supervisor 1XL Module This supervisor module is supported on the C9404R, C9407R, and C9410R chassis.	Cisco IOS XE Everest 16.6.2

Product ID (append with “=” for spares)	Description	Introductory Release
C9400-SUP-1XL-Y	Cisco Catalyst 9400 Series Supervisor 25XL Module This supervisor module is supported on the C9404R, C9407R, and C9410R chassis.	Cisco IOS XE Fuji 16.9.1
C9400X-SUP-2	Cisco Catalyst 9400 Series Supervisor 2 Module This supervisor module is supported on the C9404R, C9407R, and C9410R chassis.	Cisco IOS XE Cupertino 17.7.1
C9400X-SUP-2XL	Cisco Catalyst 9400 Series Supervisor 2XL Module This supervisor module is supported on the C9404R, C9407R, and C9410R chassis.	Cisco IOS XE Cupertino 17.7.1
Line Cards		
C9400-LC-12QC	12-port fiber optic Ethernet switching module that supports 10, 25, 40, and 100 Gbps connectivity.	Cisco IOS XE Dublin 17.12.1
C9400-LC-24S	24-port, 1 Gigabit Ethernet SFP module that supports 100/1000 BASE-T with Cu-SFP	Cisco IOS XE Fuji 16.8.1a
C9400-LC-24XS	24-port Gigabit Ethernet module that supports 1 and 10 Gbps connectivity.	Cisco IOS XE Everest 16.6.2
C9400-LC-24XY	24-port fiber optic Ethernet switching module that supports 1, 10, and 25 Gbps connectivity.	Cisco IOS XE Dublin 17.12.1
C9400-LC-48H	48-port Gigabit Ethernet UPOE+ module supporting up to 90W on each of its 48 RJ45 ports.	Cisco IOS XE Gibraltar 16.12.1
C9400-LC-48HN	48-port, UPOE+ 100 Mbps/1G/2.5G/5G Multigigabit Ethernet Module	Cisco IOS XE Bengaluru 17.5.1
C9400-LC-48HX	48-port UPOE+ 100 Mbps/1G/2.5G/5G/10G Multigigabit Module	Cisco IOS XE Cupertino 17.8.1
C9400-LC-48P	48-port, 1 Gigabit Ethernet POE/POE+ module supporting up to 30W per port.	Cisco IOS XE Fuji 16.8.1a
C9400-LC-48S	48-port, 1 Gigabit Ethernet SFP module that supports 100/1000 BASE-T with Cu-SFP.	Cisco IOS XE Fuji 16.8.1a
C9400-LC-48T	48-port, 10/100/1000 BASE-T Gigabit Ethernet module.	Cisco IOS XE Everest 16.6.1
C9400-LC-48TX	48-port, 100 Mbps/1G/2.5G/5G/10G Multigigabit Ethernet Module	Cisco IOS XE 17.13.1
C9400-LC-48U	48-port UPOE 10/100/1000 (RJ-45) module supporting up to 60W per port.	Cisco IOS XE Everest 16.6.1

Product ID (append with “=” for spares)	Description	Introductory Release
C9400-LC-48UX	48-port, UPOE Multigigabit Ethernet Module with: <ul style="list-style-type: none"> • 24 ports (Ports 1 to 24) 1G UPOE 10/100/1000 (RJ-45) • 24 ports (Ports 25 to 48) MultiGigabit Ethernet 100/1000/2500/5000/10000 UPOE ports 	Cisco IOS XE Everest 16.6.2
C9400-LC-48XS	Cisco Catalyst 9400 Series 48-Port SFP/SFP+ Module	Cisco IOS XE Cupertino 17.8.1
M.2 SATA SSD Modules¹ (for the Supervisor)		
C9400-SSD-240GB	Cisco Catalyst 9400 Series 240GB M2 SATA memory	Cisco IOS XE Everest 16.6.1
C9400-SSD-480GB	Cisco Catalyst 9400 Series 480GB M2 SATA memory	Cisco IOS XE Everest 16.6.1
C9400-SSD-960GB	Cisco Catalyst 9400 Series 960GB M2 SATA memory	Cisco IOS XE Everest 16.6.1
AC Power Supply Modules		
C9400-PWR-2100AC	Cisco Catalyst 9400 Series 2100W AC Power Supply	Cisco IOS XE Fuji 16.8.1a
C9400-PWR-3200AC	Cisco Catalyst 9400 Series 3200W AC Power Supply	Cisco IOS XE Everest 16.6.1
C9400-PWR-3200ACT	Cisco Catalyst 9400 Series 3200W AC Titanium Power Supply	Cisco IOS XE 17.13.1
DC Power Supply Modules		
C9400-PWR-3200DC	Cisco Catalyst 9400 Series 3200W DC Power Supply	Cisco IOS XE Fuji 16.9.1

¹ M.2 Serial Advanced Technology Attachment (SATA) Solid State Drive (SSD) Module

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

What's New in Cisco IOS XE 17.18.x

Hardware Features in Cisco IOS XE 17.18.1

There are no new hardware features in this release.

Software Features in Cisco IOS XE 17.18.1

Feature Name	Description
BGP EVPN VXLAN <ul style="list-style-type: none"> • BGP EVPN IPv6 Originator ID • Next-hop recursive support with EVPN PBR 	The following BGP EVPN VXLAN features are introduced in this release: <ul style="list-style-type: none"> • BGP EVPN IPv6 originator ID support in Route Type 3 (RT3). • Traffic steering in VXLAN campus fabric using PBR and next-hop recursive support with EVPN PBR (ip2fabric).
BGP neighbors monitoring with SNMP	Introduces the ability to use SNMP to monitor BGP neighbors based on the VRF the neighbor is in. This feature is enabled by default.
Maximum number of allowed MAC address moves	Introduces the ability to configure the maximum number of allowed MAC address moves in a given time interval. By default, there is no limit on the number of MAC address moves.
Message authenticator attribute in RADIUS	Introduces support for sending message authenticator attribute in the RADIUS packets which are sent out from the IOS-XE. With this feature, RADIUS packets that do not have the message authenticator attribute are dropped.
Programmability: <ul style="list-style-type: none"> • YANG Data Models 	The following programmability features are introduced in this release: <ul style="list-style-type: none"> • YANG Data Models: For the list of Cisco IOS XE YANG models available with this release, navigate to: https://github.com/YangModels/yang/tree/main/vendor/cisco/xe/17181.
Product Analytics	Cisco IOS XE Product Analytics collects device Systems Information for the purposes of understanding product usage, enabling product improvements and product development, and assisting in product adoption and sales support. Only summarized data of feature usage and statistical counters of configuration are collected. No personal identifiable information, such as MAC/IP addresses, usernames, custom configuration names, or user provided strings, are collected as part of Cisco IOS XE Product Analytics. Cisco processes this data following the General Terms , the Cisco Privacy Statement, and any other applicable agreement with Cisco. See Cisco Enterprise Networking Product Analytics Frequently Asked Questions .
Resource Manager System (RMS) and Resource Manager Controller (RMC) commands	Introduces support for the following commands: <ul style="list-style-type: none"> • RMS: show platform software process database fed active details RMS_DB table np_i_rms content • RMS IPC (Interprocess Communications Protocol): show platform software resource-manager switch active R0 ipc stats • RMC: show platform software process database fed active details RMC_DB "table np_i_rmc" content • RMS and RMC: show platform software resource-manager switch active R0 available-resource RMS
TLS for TACACS+	Introduces support for TACACS+ over Transport Layer Security (TLS). This feature enhances security and provides stronger certificate-based AAA services.

New on the WebUI
There are no new WebUI features in this release.

Hardware and Software Behavior Changes in Cisco IOS XE 17.18.1

There are no new behavior changes in this release.

Notice of upcoming changes in the Cisco IOS XE 17.18.2 release and beyond

Cisco is committed to safeguarding our products and customer networks against increasingly sophisticated threat actors. As computing power and the threat landscape have evolved, some features and protocols currently in use have become vulnerable to attack. While more secure alternatives are now available, legacy protocols may still be in use in some environments.

To improve network security, reduce the attack surface, and protect sensitive data, Cisco will begin phasing out legacy and insecure features and protocols, encouraging customers to transition to more secure alternatives. This process will be gradual and designed to minimize operational impact. The first phase begins with the Cisco IOS XE 17.18 release train. This is part of a broader initiative to make Cisco products more secure by default and secure by design.

Starting with the Cisco IOS XE 17.18.2 release and in future releases, Cisco software will display warning messages when configuring features or protocols that do not provide sufficient security such as those transmitting sensitive data without encryption or using outdated encryption mechanisms. Warnings will also appear when security best practices are not followed, along with suggestions for secure alternatives.

This list is subject to change, but the following is a list of features and protocols that are planned to generate warnings in releases beyond the version Cisco IOS XE 17.18.1. Release notes for each release will describe exact changes for that release.

- **Plain-text and weak credential storage:** Type 0 (plain text), 5 (MD5), or 7 (Vigenère cipher) in configuration files.

Recommendation: Use Type 6 (AES) for reversible credentials, and Type 8 (PBKDF2-SHA-256) or Type 9 (Scrypt) for non-reversible credentials.

- **SSHv1**

Recommendation: Use SSHv2.

- **SNMPv1 and SNMPv2, or SNMPv3 without authentication and encryption**

Recommendation: Use SNMPv3 with authentication and encryption (authPriv).

- **MD5 (authentication) and 3DES (encryption) in SNMPv3**

Recommendation: Use SHA1 or, preferably, SHA2 for authentication, and AES for encryption.

- **IP source routing based on IP header options**

Recommendation: Do not use this legacy feature.

- **TLS 1.0 and TLS 1.1**

Recommendation: Use TLS 1.2 or later.

- **TLS ciphers using SHA1 for digital signatures**

Recommendation: Use ciphers with SHA256 or stronger digital signatures.

- **HTTP**

Recommendation: Use HTTPS.

- **Telnet**

Recommendation: Use SSH for remote access.

- **FTP and TFTP**

Recommendation: Use SFTP or HTTPS for file transfers.

- **On-Demand Routing (ODR)**

Recommendation: Use a standard routing protocol in place of CDP-based routing information exchange.

- **BootP server**

Recommendation: Use DHCP or secure boot features such as Secure ZTP.

- **TCP and UDP small servers (echo, chargen, discard, daytime)**

Recommendation: Do not use these services on network devices.

- **IP finger**

Recommendation: Do not use this protocol on network devices.

- **NTP control messages**

Recommendation: Do not use this feature.

- **TACACS+ using pre-shared keys and MD5**

Recommendation: Use TACACS+ over TLS 1.3, introduced in release Cisco IOS XE 17.18.1.

Cisco is committed to supporting customers through this transition. Subsequent releases in the Cisco IOS XE 17.18 train will continue to support these features but will display warnings if they are used. Future release trains may impose additional restrictions on these features which will be communicated through release notes.

Caveats

Caveats describe unexpected behavior in Cisco IOS-XE releases. Caveats listed as open in a prior release are carried forward to the next release as either open or resolved.

Open Caveats in Cisco IOS XE 17.18.x

There are no open caveats in this release.

Resolved Caveats in Cisco IOS XE 17.18.1

There are no resolved caveats in this release.

Feature Support

This section lists the supported and unsupported features.

All Supported Features

For the complete list of features supported on a platform, see the [Cisco Feature Navigator](#).

Differences in Feature Support Between Switch Models

For the most part, the list of supported software features is common across Cisco Catalyst 9400 Series Supervisor 1, 1XL, 1XL-Y, 2, and 2XL Modules. However, the differences in the hardware and software capabilities between these variants, means that there are exceptions to this. The following sections list these exceptions, that is, when a feature is introduced, but not supported on all available supervisor modules.

For the list of Cisco Catalyst 9400 Series Supervisor Module PIDs, see [Supported Cisco Catalyst 9400 Series Switches Model Numbers, on page 1](#).

Table 2: Cisco TrustSec

Feature	Not Supported On These Variants
Cisco TrustSec Network Device Admission Control (NDAC) on Uplinks	All

Table 3: High Availability

Feature	Not Supported On These Variants
Cisco StackWise Virtual solution does not support Resilient Ethernet Protocol (REP) and Remote Switched Port Analyzer (RSPAN).	All

Table 4: Interface and Hardware

Feature	Not Supported On These Variants
Fast PoE	All

Table 5: Layer 2

Feature	Not Supported On These Variants
Audio Video Bridging (including IEEE802.1AS, IEEE 802.1Qat, and IEEE 802.1Qav)	All

Table 6: Security

Feature	Not Supported On These Variants
IPsec VPN	All
MACsec switch-to-switch connections on C9400-SUP-1XL-Y.	All
MACsec switch-to-host connections in an overlay network.	All

Table 7: System Management

Feature	Not Supported On These Variants
Performance Monitoring (PerfMon)	All

Limitations and Restrictions

- Control Plane Policing (CoPP): The **show running-config** command does not display information about classes configured under `system-cpp policy`, when they are left at default values. Use the **show policy-map system-cpp-policy** or the **show policy-map control-plane** commands in privileged EXEC mode instead.
- Cisco TrustSec restrictions: Cisco TrustSec can be configured only on physical interfaces, not on logical interfaces.
- Flexible NetFlow limitations
 - You cannot configure NetFlow export using the Ethernet Management port (GigabitEthernet0/0).
 - You can not configure a flow monitor on logical interfaces, such as layer 2 port-channels, loopback, tunnels.
 - You can not configure multiple flow monitors of same type (ipv4, ipv6 or datalink) on the same interface for same direction.
- Hardware Limitations (Optics): Multi-rate SFPs are not preferred for SVL or DAD links because auto-negotiation may lead to speed mismatches on some ports. If they are used, set both sides to the same speed; highest speed is recommended (example, 25G for SFP-10/25G and 100G for QSFP-40/100G). Also, both sides of the link should be multi-rate SFPs and all the other SVL or DAD link ports should use multi-rate SFPs. Use the **show interfaces transceiver** command to view the physical properties of SFPs used in the device.
- Hardware limitations: When you use Cisco QSFP-4SFP10G-CUxM Direct-Attach Copper Cables, autonegotiation is enabled by default. If the other end of the line does not support autonegotiation, the link does not come up.
- Interoperability limitations: When you use Cisco QSFP-4SFP10G-CUxM Direct-Attach Copper Cables, if one end of the 40G link is a Catalyst 9400 Series Switch and the other end is a Catalyst 9500 Series Switch, the link does not come up, or comes up on one side and stays down on the other. To avoid this interoperability issue between devices, apply the **speed nonegotiate** command on the Catalyst 9500 Series Switch interface. This command disables autonegotiation and brings the link up. To restore autonegotiation, use the **no speed nonegotiation** command.
- In-Service Software Upgrade (ISSU)
 - Within a major release train (16.x or 17.x or 18.x), ISSU is supported between any two EMs that are released not more than 3 years apart.
 - Within a major release train, ISSU is supported from:
 - Any EM (EM1, EM2, EM3) to another EM (EM1, EM2, EM3)
Example: 16.9.x to 16.12.x, 17.3.x to 17.6.x, 17.6.x to 17.9.x
 - Any release within the same EM
Example: 16.9.2 to 16.9.3 or 16.9.4 or 16.9.x, 16.12.1 to 16.12.2 or 16.12.3 or 16.12.x, 17.3.1 to 17.3.2 or 17.3.3 or 17.3.x
 - Between major release trains, ISSU is not supported from:
 - An EM of a major release train to an EM of another major release train

Example: 16.x.x to 17.x.x or 17.x.x to 18.x.x is not supported

- An SM to EM or EM to SM

Example: 16.10.x or 16.11.x to 16.12.x is not supported

- ISSU is not supported on engineering special releases and .s (or similar) images.
- ISSU is not supported between Licensed Data Payload Encryption (LDPE) and No Payload Encryption (NPE) Cisco IOS XE software images.
- ISSU downgrades are not supported.
- While performing ISSU from Cisco IOS XE Fuji 16.9.x to Cisco IOS XE Gibraltar 16.12.x, if **interface-id snmp-if-index** command is not configured with OSPFv3, packet loss can occur. Configure the **interface-id snmp-if-index** command either during the maintenance window or after isolating the device (by using maintenance mode feature) from the network before doing the ISSU.
- While ISSU allows you to perform upgrades with zero downtime, we recommend you to do so during a maintenance window only.
- If a new feature introduced in a software release requires a change in configuration, the feature should not be enabled during ISSU.
- If a feature is not available in the downgraded version of a software image, the feature should be disabled before initiating ISSU.
- M.2 SATA SSD drive: With bootloader version 16.6.2r, you cannot access the M.2 SATA SSD drive at the ROMMON prompt (`rommon> dir disk0`). The system displays an error message indicating that the corresponding file system protocol is not found on the device. The only way to access the drive when on bootloader version 16.6.2r, is through the Cisco IOS prompt, after boot up.
- No service password recovery: With ROMMON versions R16.6.1r and R16.6.2r, the 'no service password-recovery' feature is not available.
- QoS restrictions
 - When configuring QoS queuing policy, the sum of the queuing buffer should not exceed 100%.
 - Policing and marking policy on sub interfaces is supported.
 - Marking policy on switched virtual interfaces (SVI) is supported.
 - QoS policies are not supported for port-channel interfaces, tunnel interfaces, and other logical interfaces.
 - Stack Queuing and Scheduling (SQS) drops CPU bound packets exceeding 1.4 Gbps.
- Redundancy: The supervisor module (hardware) supports redundancy. Software redundancy is supported starting with Cisco IOS XE Everest 16.6.2. However, the associated route processor redundancy (RPR) feature is not supported. Quad-supervisor with Route Processor Redundancy (RPR) with Cisco StackWise Virtual is also not supported.

Before performing a switchover, use the **show redundancy**, **show platform**, and **show platform software iomd redundancy** commands to ensure that both the SSOs have formed and that the IOMD process is completed.

In the following sample output for the **show redundancy**, note that both the SSOs have formed.

```
Switch# show redundancy
Redundant System Information :
-----
```

```

Available system uptime = 3 hours, 30 minutes
Switchovers system experienced = 2
Standby failures = 0
Last switchover reason = active unit removed

Hardware Mode = Duplex
Configured Redundancy Mode = sso
Operating Redundancy Mode = sso
Maintenance Mode = Disabled
Communications = Up

Current Processor Information :
-----
Active Location = slot 3
Current Software state = ACTIVE
Uptime in current state = 2 hours, 57 minutes
Image Version = Cisco IOS Software [Fuji], Catalyst L3 Switch Software (CAT9K_IOSXE), Version 16.8.1,
RELEASE SOFTWARE (fc3)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2018 by Cisco Systems, Inc.
Compiled Tue 27-Mar-18 13:43 by mcpre
BOOT = bootflash:packages.conf;
CONFIG_FILE =
Configuration register = 0x1822

Peer Processor Information :
-----
Standby Location = slot 4
Current Software state = STANDBY HOT
Uptime in current state = 2 hours, 47 minutes
Image Version = Cisco IOS Software [Fuji], Catalyst L3 Switch Software (CAT9K_IOSXE), Version 16.8.1,
RELEASE SOFTWARE (fc3)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2018 by Cisco Systems, Inc.
Compiled Tue 27-Mar-18 13:43 by mcpre
BOOT = bootflash:packages.conf;
CONFIG_FILE =
Configuration register = 0x1822

```

In the following sample output for the **show platform software iomd redundancy** command, note that both SSOs have formed and the HA_STATE field is ready.

```

Switch# show platform software iomd redundancy
Configured Redundancy Mode = sso
Operating Redundancy Mode = sso
Local RF state = ACTIVE
Peer RF state = STANDBY HOT

slot  PSM STATE   SPA INTF   HA_STATE HA_ACTIVE
  1    ready   started    ready    00:01:16
  2    ready   started    ready    00:01:22
  3    ready   started    ready    00:01:27 ***active RP
  4    ready   started    ready    00:01:27
<output truncated>

```

In the following sample output for the **show platform** command, note that the State for all the linecards and supervisor modules is ok. This indicates that the IOMD processes are completed.

```

Switch# show platform
Chassis type: C9407R

```

Slot	Type	State	Insert time (ago)
1	C9400-LC-24XS	ok	3d09h

2	C9400-LC-48U	ok	3d09h
R0	C9400-SUP-1	ok, active	3d09h
R1	C9400-SUP-1	ok, standby	3d09h
P1	C9400-PWR-3200AC	ok	3d08h
P2	C9400-PWR-3200AC	ok	3d08h
P17	C9407-FAN	ok	3d08h

<output truncated>

• Secure Shell (SSH)

- Use SSH Version 2. SSH Version 1 is not supported.
- When the device is running SCP and SSH cryptographic operations, expect high CPU until the SCP read process is completed. SCP supports file transfers between hosts on a network and uses SSH for the transfer.

Since SCP and SSH operations are currently not supported on the hardware crypto engine, running encryption and decryption process in software causes high CPU. The SCP and SSH processes can show as much as 40 or 50 percent CPU usage, but they do not cause the device to shutdown.

- Smart Licensing Using Policy: Starting with Cisco IOS XE Amsterdam 17.3.2a, with the introduction of Smart Licensing Using Policy, even if you configure a hostname for a product instance or device, only the Unique Device Identifier (UDI) is displayed. This change in the display can be observed in all licensing utilities and user interfaces where the hostname was displayed in earlier releases. It does not affect any licensing functionality. There is no workaround for this limitation.

The licensing utilities and user interfaces that are affected by this limitation include only the following: Cisco Smart Software Manager (CSSM), Cisco Smart License Utility (CSLU), and Smart Software Manager On-Prem (SSM On-Prem).

This limitation is removed from Cisco IOS XE Cupertino 17.9.1. If you configure a hostname and disable hostname privacy (**no license smart privacy hostname** global configuration command), hostname information is sent from the product instance and displayed on the applicable user interfaces (CSSM, CSLU, SSM On-Prem). For more information, see the command reference for this release.

- TACACS legacy command: Do not configure the legacy **tacacs-server host** command; this command is deprecated. If the software version running on your device is Cisco IOS XE Gibraltar 16.12.2 or a later release, using the legacy command can cause authentication failures. Use the **tacacs server** command in global configuration mode.
- Uplink Symmetry: When a redundant supervisor module is inserted, we recommend that you have symmetric uplinks, to minimize packet loss during a switchover.

Uplinks are said to be in symmetry when the same interface on both supervisor modules have the same type of transceiver module. For example, a TenGigabitEthernet interface with no transceiver installed operates at a default 10G mode; if the matching interface of the other supervisor has a 10G transceiver, then they are in symmetry. Symmetry provides the best SWO packet loss and user experience.

Asymmetric uplinks have at least one or more pairs of interfaces in one supervisor not matching the transceiver speed of the other supervisor.

- USB Authentication: When you connect a Cisco USB drive to the switch, the switch tries to authenticate the drive against an existing encrypted preshared key. Since the USB drive does not send a key for authentication, the following message is displayed on the console when you enter **password encryption aes** command:

```
Device(config)# password encryption aes
Master key change notification called without new or old key
```

- Catatyst 9000 Series Switches support MACsec switch-to-switch connections. We do not recommend configuring MACsec switch-to-host connections in an overlay network. For assistance with an existing switch-to-host MACsec implementation or a design review, contact your Cisco Sales Representative or Channel Partner.

- **VLAN Restriction:** It is advisable to have well-defined segregation while defining data and voice domain during switch configuration and to maintain a data VLAN different from voice VLAN across the switch stack. If the same VLAN is configured for data and voice domains on an interface, the resulting high CPU utilization might affect the device.
- **YANG data modeling limitation:** A maximum of 20 simultaneous NETCONF sessions are supported.
- **Embedded Event Manager:** Identity event detector is not supported on Embedded Event Manager.
- **The File System Check (fsck) utility** is not supported in install mode.
- The command **service-routing mdns-sd** is being deprecated. Use the **mdns-sd gateway** command instead.
- Switch Web UI allows configuration of data VLANs only and not voice VLANs. If you remove a voice VLAN configured to an interface using the Web UI, then all data VLANs associated with the interface are also removed by default.

Licensing

For information about licenses required for the features available on Cisco Catalyst 9000 Series Switches, see [Configuring Licenses on Cisco Catalyst 9000 Series Switches](#).

All licensing information relating to Cisco Catalyst 9000 Series Switches are available on this collection page: [Cisco Catalyst 9000 Switching Family Licensing](#).

Available Licensing Models and Configuration Information

- Cisco IOS XE Fuji 16.8.x and earlier: RTU Licensing is the default and the only supported method to manage licenses.
- Cisco IOS XE Fuji 16.9.1 to Cisco IOS XE Amsterdam 17.3.1: Smart Licensing is the default and the only supported method to manage licenses.
- Cisco IOS XE Amsterdam 17.3.2a and later: Smart Licensing Using Policy, which is an enhanced version of Smart Licensing, is the default and the only supported method to manage licenses.

Compatibility Matrix

To view the software compatibility information between Cisco Catalyst 9400 Series Switches, Cisco Identity Services Engine, and Cisco Prime Infrastructure, go to [Cisco Catalyst 9000 Series Switches Software Version Compatibility Matrix](#).

Switch Software Version Information

This section provides information about software, images, and Field-Programmable Gate Array (FGPA) versions.

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

Release	Image Type	File Name
Cisco IOS XE 17.18.1	CAT9K_IOSXE	cat9k_iosxe.17.18.01.SPA.bin
	No Payload Encryption (NPE)	cat9k_iosxe_npe.17.18.01.SPA.bin

To download software images, visit the software downloads page: [Cisco Catalyst 9400 Series Switches](#).

ROMMON and CPLD Versions

This topic lists the ROMMON and CPLD versions for Cisco Catalyst 9400 Series Switches.

ROMMON

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.

Complex Programmable Logic Device (CPLD)

CPLD refers to hardware-programmable firmware. CPLD upgrades may be required to resolve firmware defects, or to support new features, but there may not be new versions with every release. CPLD version upgrade process must be completed after upgrading the software image.

The following table provides ROMMON and CPLD version information for the Cisco Catalyst 9400 Series Supervisor Modules. For ROMMON and CPLD version information of Cisco IOS XE 16.x.x releases, refer to the corresponding Cisco IOS XE 16.x.x release notes of the respective platform.

Release	ROMMON Version (C9400-SUP-1, C9400-SUP-1XL, C9400-SUP-1XL-Y)	CPLD Version (C9400-SUP-1, C9400-SUP-1XL, C9400-SUP-1XL-Y)	ROMMON Version (C9400X-SUP-2, C9400X-SUP-2XL)	CPLD Version (C9400X-SUP-2, C9400X-SUP-2XL)
17.18.1	17.10.1r	20062105	17.12.1r[FC1]	21080305

Release	ROMMON Version (C9400-SUP-1, C9400-SUP-1XL, C9400-SUP-1XL-Y)	CPLD Version (C9400-SUP-1, C9400-SUP-1XL, C9400-SUP-1XL-Y)	ROMMON Version (C9400X-SUP-2, C9400X-SUP-2XL)	CPLD Version (C9400X-SUP-2, C9400X-SUP-2XL)
17.17.1	17.10.1r	20062105	17.12.1r[FC1]	21080305
17.16.1	17.10.1r	20062105	17.12.1r[FC1]	21080305
17.15.4	17.10.1r	20062105	17.12.1r[FC1]	21080305
17.15.3	17.10.1r	20062105	17.12.1r[FC1]	21080305
17.15.2	17.10.1r	20062105	17.12.1r[FC1]	21080305
17.15.1	17.10.1r	20062105	17.12.1r[FC1]	21080305
17.14.1	17.10.1r	20062105	17.12.1r[FC1]	21080305
17.13.1	17.10.1r	20062105	17.12.1r[FC1]	21080305
Dublin 17.12.4	17.10.1r	20062105	17.12.1r[FC1]	21080305
Dublin 17.12.3	17.10.1r	20062105	17.12.1r[FC1]	21080305
Dublin 17.12.2	17.10.1r	20062105	17.12.1r[FC1]	21080305
Dublin 17.12.1	17.10.1r	20062105	17.12.1r[FC1]	21080305
Dublin 17.11.1	17.10.1r	20062105	17.11.1r	21080305
Dublin 17.10.1	17.10.1r	20062105	17.9.1r[FC1]	21080305
Cupertino 17.9.5	17.8.1r[FC1]	20062105	17.9.3r	21080305
Cupertino 17.9.4	17.8.1r[FC1]	20062105	17.9.3r	21080305
Cupertino 17.9.3	17.8.1r[FC1]	20062105	17.9.3r	21080305
Cupertino 17.9.2	17.8.1r[FC1]	20062105	17.9.2r	21080305
Cupertino 17.9.1	17.8.1r[FC1]	20062105	17.9.1r[FC1]	21080305
Cupertino 17.8.1	17.8.1r[FC1]	20062105	17.8.1r[FC1]	21080305
Cupertino 17.7.1	17.6.1r[FC2]	20062105	17.7.1r[FC3]	21080305
Bengaluru 17.6.7	17.6.1r[FC2]	20062105	-	-
Bengaluru 17.6.6a	17.6.1r[FC2]	20062105	-	-
Bengaluru 17.6.6	17.6.1r[FC2]	20062105	-	-
Bengaluru 17.6.5	17.6.1r[FC2]	20062105	-	-
Bengaluru 17.6.4	17.6.1r[FC2]	20062105	-	-

Release	ROMMON Version (C9400-SUP-1, C9400-SUP-1XL, C9400-SUP-1XL-Y)	CPLD Version (C9400-SUP-1, C9400-SUP-1XL, C9400-SUP-1XL-Y)	ROMMON Version (C9400X-SUP-2, C9400X-SUP-2XL)	CPLD Version (C9400X-SUP-2, C9400X-SUP-2XL)
Bengaluru 17.6.3	17.6.1r[FC2]	20062105	-	-
Bengaluru 17.6.2	17.6.1r[FC2]	20062105	-	-
Bengaluru 17.6.1	17.6.1r[FC2]	20062105	-	-
Bengaluru 17.5.1	17.5.1r	20062105	-	-
Bengaluru 17.4.1	17.3.1r[FC2]	20062105	-	-
Amsterdam 17.3.8a	17.3.1r[FC2]	19082605	-	-
Amsterdam 17.3.8	17.3.1r[FC2]	19082605	-	-
Amsterdam 17.3.7	17.3.1r[FC2]	19082605	-	-
Amsterdam 17.3.6	17.3.1r[FC2]	19082605	-	-
Amsterdam 17.3.5	17.3.1r[FC2]	19082605	-	-
Amsterdam 17.3.4	17.3.1r[FC2]	19082605	-	-
Amsterdam 17.3.3	17.3.1r[FC2]	19082605	-	-
Amsterdam 17.3.2a	17.3.1r[FC2]	19082605	-	-
Amsterdam 17.3.1	17.3.1r[FC2]	19082605	-	-
Amsterdam 17.2.1	17.1.1r	19082605	-	-
Amsterdam 17.1.1	17.1.1r	19032905	-	-

Upgrading and Downgrading the Switch Software

This section covers the various aspects of upgrading or downgrading the device software.



Note

You cannot use the Web UI to install, upgrade, or downgrade device software.

Upgrading in Install Mode

Follow these instructions to upgrade from one release to another, in install mode. To perform a software image upgrade, you must be booted into IOS via **boot flash:packages.conf**.

Caution


You must comply with these cautionary guidelines during an upgrade:

- Do not power cycle the switch.
- Do not disconnect power or remove the supervisor module.
- Do not perform an online insertion and replacement (OIR) of either supervisor (in a High Availability setup), if one of the supervisor modules in the chassis is in the process of a bootloader upgrade or when the switch is booting up.
- Do not perform an OIR of a switching module (linecard) when the switch is booting up.

Note


Disconnecting and reconnecting power to a Cisco Catalyst 9400 Series Supervisor 1 Module within a 5-second window, can corrupt the boot SPI.

Note that you can use this procedure for the following upgrade scenarios.

When upgrading from ...	Permitted Supervisor Setup (Applies to the release you are upgrading from)	First upgrade to...	To upgrade to ...
Cisco IOS XE Everest 16.6.1 ²	<p>Upgrade a single supervisor, and complete the boot loader and CPLD upgrade. After completing the first supervisor upgrade, remove and swap in the second supervisor. After both supervisors are upgraded, they can be inserted and booted in a high availability setup.</p> <p> Note Do not simultaneously upgrade dual supervisors from Cisco IOS XE Everest 16.6.1 to a later release. Doing so may cause hardware damage.</p>	Cisco IOS XE Everest 16.6.3 Follow the upgrade steps as in the Release Notes for Cisco Catalyst 9400 Series Switches, Cisco IOS XE Everest 16.6.x → Upgrading the Switch Software → Upgrading in Install Mode	Cisco IOS XE 17.18.x
Cisco IOS XE Everest 16.6.2 and later releases	This procedure automatically copies the images to both active and standby supervisor modules. Both supervisor modules are simultaneously upgraded.	Not applicable	

² When upgrading from Cisco IOS XE Everest 16.6.1 to a later release, the upgrade may take a long time, and the system will reset three times due to rommon and complex programmable logic device (CPLD) upgrade. Stateful switchover is supported from Cisco IOS XE Everest 16.6.2

This procedure shows the steps to upgrade the Cisco IOS XE software on a switch, from Cisco IOS XE 17.17.1 to Cisco IOS XE 17.18.1 using **install** commands, followed by sample output.

- Step 1** Clean-up
install remove inactive
- Use this command to clean-up old installation files in case of insufficient space and to ensure that you have at least 1GB of space in flash, to expand a new image.
- Step 2** Copy new image to flash
- a) **copy tftp:[[/location]/directory]/filename flash:**
- Use this command to copy the new image from a TFTP server to flash memory. The location is either an IP address or a host name. The filename is specified relative to the directory used for file transfers. Skip this step if you want to use the new image from a TFTP server.
- b) **dir flash:**
- Use this command to confirm that the image has been successfully copied to flash.
- Step 3** Set boot variable
- a) **boot system flash:packages.conf**
- Use this command to set the boot variable to **flash:packages.conf**.
- b) **no boot manual**
- Use this command to configure the switch to auto-boot. Settings are synchronized with the standby switch, if applicable.
- c) **write memory**
- Use this command to save boot settings.
- d) **show bootvar**
- Use this command to verify the boot variable (packages.conf) and manual boot setting (no):
- Step 4** Install image to flash
install add file activate commit
- Use this command to install the image.
-  Old files listed in the logs will not be removed from flash.
- Note**
- Step 5** Verify installation
- After the software has been successfully installed, check that the ten new .pkg files and two .conf are in the flash partition, and also check the version installed on the switch.
- a) **dir flash:*.pkg**
- b) **dir flash:*.conf**
- c) **show install summary**
- d) **show version**
- After the image boots up, use this command to verify the version of the new image.

Example

The following sample output displays the cleaning up of unused files, by using the **install remove inactive** command:

```
Switch# install remove inactive

install_remove: START Thu Jul 31 14:14:40 UTC 2025
Cleaning up unnecessary package files
No path specified, will use booted path flash:packages.conf
Cleaning flash:
Scanning boot directory for packages ... done.
Preparing packages list to delete ...
cat9k-cc_srdriver.17.17.01.SPA.pkg
File is in use, will not delete.
cat9k-espbases.17.17.01.SPA.pkg
File is in use, will not delete.
cat9k-rpbases.17.17.01.SPA.pkg
File is in use, will not delete.
cat9k-rpboot.17.17.01.SPA.pkg
File is in use, will not delete.
cat9k-sipbases.17.17.01.SPA.pkg
File is in use, will not delete.
cat9k-sipspas.17.17.01.SPA.pkg
File is in use, will not delete.
cat9k-srdriver.17.17.01.SPA.pkg
File is in use, will not delete.
cat9k-webui.17.17.01.SPA.pkg
File is in use, will not delete.
packages.conf
File is in use, will not delete.
done.

The following files will be deleted:
[R0]:
/flash/cat9k-cc_srdriver.17.17.01.SPA.pkg
/flash/cat9k-espbases.17.17.01.SPA.pkg
/flash/cat9k-guestshell.17.17.01.SPA.pkg
/flash/cat9k-rpbases.17.17.01.SPA.pkg
/flash/cat9k-rpboot.17.17.01.SPA.pkg
/flash/cat9k-sipbases.17.17.01.SPA.pkg
/flash/cat9k-sipspas.17.17.01.SPA.pkg
/flash/cat9k-srdriver.17.17.01.SPA.pkg
/flash/cat9k-webui.17.17.01.SPA.pkg
/flash/cat9k-wlc.17.17.01.SPA.pkg
/flash/packages.conf
/flash/cat9k_iosxe.17.17.01.SPA.bin

Do you want to remove the above files? [y/n]y
[R0]:
Deleting file flash:cat9k-cc_srdriver.17.17.01.SPA.pkg ... done.
Deleting file flash:cat9k-espbases.17.17.01.SPA.pkg ... done.
Deleting file flash:cat9k-guestshell.17.17.01.SPA.pkg ... done.
Deleting file flash:cat9k-rpbases.17.17.01.SPA.pkg ... done.
Deleting file flash:cat9k-rpboot.17.17.01.SPA.pkg ... done.
Deleting file flash:cat9k-sipbases.17.17.01.SPA.pkg ... done.
Deleting file flash:cat9k-sipspas.17.17.01.SPA.pkg ... done.
Deleting file flash:cat9k-srdriver.17.17.01.SPA.pkg ... done.
Deleting file flash:cat9k-webui.17.17.01.SPA.pkg ... done.
Deleting file flash:cat9k-wlc.17.17.01.SPA.pkg ... done.
Deleting file flash:packages.conf ... done.
SUCCESS: Files deleted.
SUCCESS: Files deleted.
--- Starting Post_Remove_Cleanup ---
```

```
Performing Post_Remove_Cleanup on Active/Standby
[R0] Post_Remove_Cleanup package(s) on R0
[R0] Finished Post_Remove_Cleanup on R0
Checking status of Post_Remove_Cleanup on [R0]
Post_Remove_Cleanup: Passed on [R0]
Finished Post_Remove_Cleanup
```

```
SUCCESS: install_remove Thu Jul 31 14:16:29 UTC 2025
Switch#
```

```
Switch# copy tftp://10.8.0.6/image/cat9k_iosxe.17.18.01.SPA.bin flash:
destination filename [cat9k_iosxe.17.18.01.SPA.bin]?
Accessing tftp://10.8.0.6/image/cat9k_iosxe.17.18.01.SPA.bin...
Loading /cat9k_iosxe.17.18.01.SPA.bin from 10.8.0.6 (via GigabitEthernet0/0):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 601216545 bytes]
```

```
601216545 bytes copied in 50.649 secs (11870255 bytes/sec)
```

```
Switch# dir flash:*.bin
Directory of flash:/*.bin
```

```
Directory of flash:/
```

```
434184 -rw- 601216545 Jul 31 2025 10:18:11 -07:00 cat9k_iosxe.17.18.01.SPA.bin
11353194496 bytes total (8976625664 bytes free)
```

```
Switch(config)# boot system flash:packages.conf
```

```
Switch(config)# no boot manual
```

```
Switch(config)# exit
```

```
Switch# write memory
```

```
Switch# show bootvar
```

```
BOOT variable = bootflash:packages.conf
```

```
MANUAL_BOOT variable = no
```

```
BAUD variable = 9600
```

```
ENABLE_BREAK variable = yes
```

```
BOOTMODE variable does not exist
```

```
IPXE_TIMEOUT variable does not exist
```

```
CONFIG_FILE variable =
```

```
Standby BOOT variable = bootflash:packages.conf
```

```
Standby MANUAL_BOOT variable = no
```

```
Standby BAUD variable = 9600
```

```
Standby ENABLE_BREAK variable = yes
```

```
Standby BOOTMODE variable does not exist
```

```
Standby IPXE_TIMEOUT variable does not exist
```

```
Standby CONFIG_FILE variable =
```

The following sample output displays installation of the Cisco IOS XE 17.18.1 software image in the flash memory:

```
Switch# install add file flash:cat9k_iosxe.17.18.01.SPA.bin
activate commit
```

```
install_add_activate_commit: START Thu Jul 31 22:49:41 UTC 2025
```

```
*Jul 31 22:49:42.772: %IOSXE-5-PLATFORM: Switch 1 R0/0: Jul 31 22:49:42 install_engine.sh:
%INSTALL-5-INSTALL_START_INFO: Started install one-shot flash:cat9k_iosxe.17.18.01.SPA.bin
```

```
install_add_activate_commit: Adding PACKAGE
```

```

--- Starting initial file syncing ---
Info: Finished copying flash:cat9k_iosxe.17.18.01.SPA.bin
to the selected switch(es)
Finished initial file syncing

--- Starting Add ---
Performing Add on all members
[1] Add package(s) on switch 1
[1] Finished Add on switch 1
Checking status of Add on [1]
Add: Passed on [1]
Finished Add

install_add_activate_commit: Activating PACKAGE

/flash/cat9k-webui.17.18.01.SPA.pkg
/flash/cat9k-srdriver.17.18.01.SPA.pkg
/flash/cat9k-sipspa.17.18.01.SPA.pkg
/flash/cat9k-sipbase.17.18.01.SPA.pkg
/flash/cat9k-rpboot.17.18.01.SPA.pkg
/flash/cat9k-rpbase.17.18.01.SPA.pkg
/flash/cat9k-guestshell.17.18.01.SPA.pkg
/flash/cat9k-esppbase.17.18.01.SPA.pkg
/flash/cat9k-cc_srdriver.17.18.01.SPA.pkg

This operation requires a reload of the system. Do you want to proceed? [y/n]y

--- Starting Activate ---
Performing Activate on all members
[1] Activate package(s) on switch 1
[1] Finished Activate on switch 1
Checking status of Activate on [1]
Activate: Passed on [1]
Finished Activate

--- Starting Commit ---
Performing Commit on all members
[1] Commit package(s) on switch 1
[1] Finished Commit on switch 1
Checking status of Commit on [1]
Commit: Passed on [1]
Finished Commit

Install will reload the system now!

Chassis 1 reloading, reason - Reload command
SUCCESS: install_add_activate_commit
/flash/cat9k-webui.17.18.01.SPA.pkg
/flash/cat9k-srdriver.17.18.01.SPA.pkg
/flash/cat9k-sipspa.17.18.01.SPA.pkg
/flash/cat9k-sipbase.17.18.01.SPA.pkg
/flash/cat9k-rpboot.17.18.01.SPA.pkg
/flash/cat9k-rpbase.17.18.01.SPA.pkg
/flash/cat9k-guestshell.17.18.01.SPA.pkg
/flash/cat9k-esppbase.17.18.01.SPA.pkg
/flash/cat9k-cc_srdriver.17.18.01.SPA.pkg
Jul 31 11 22:53:58 UTC 2025
Switch#

```

The following is sample output of the **dir flash:*.pkg** command:

```

Switch# dir flash:*.pkg
Directory of flash:/*.pkg
Directory of flash:/

```

```

475140 -rw- 2012104      Mar 25 2025 09:52:41 -07:00 cat9k-cc_srdriver.17.17.01.SPA.pkg
475141 -rw- 70333380     Mar 25 2025 09:52:44 -07:00 cat9k-espbases.17.17.01.SPA.pkg
475142 -rw- 13256        Mar 25 2025 09:52:44 -07:00 cat9k-guestshell.17.17.01.SPA.pkg
475143 -rw- 349635524    Mar 25 2025 09:52:54 -07:00 cat9k-rpbases.17.17.01.SPA.pkg
475149 -rw- 24248187      Mar 25 2025 09:53:02 -07:00 cat9k-rpboot.17.17.01.SPA.pkg
475144 -rw- 25285572      Mar 25 2025 09:52:55 -07:00 cat9k-sipbase.17.17.01.SPA.pkg
475145 -rw- 20947908      Mar 25 2025 09:52:55 -07:00 cat9k-sipspace.17.17.01.SPA.pkg
475146 -rw- 2962372       Mar 25 2025 09:52:56 -07:00 cat9k-srdriver.17.17.01.SPA.pkg
475147 -rw- 13284288      Mar 25 2025 09:52:56 -07:00 cat9k-webui.17.17.01.SPA.pkg
475148 -rw- 13248         Mar 25 2025 09:52:56 -07:00 cat9k-wlc.17.17.01.SPA.pkg

491524 -rw- 25711568      Jul 31 2025 11:49:33 -07:00 cat9k-cc_srdriver.17.18.01.SPA.pkg
491525 -rw- 78484428      Jul 31 2025 11:49:35 -07:00 cat9k-espbases.17.18.01.SPA.pkg
491526 -rw- 1598412       Jul 31 2025 11:49:35 -07:00 cat9k-guestshell.17.18.01.SPA.pkg
491527 -rw- 404153288     Jul 31 2025 11:49:47 -07:00 cat9k-rpbases.17.18.01.SPA.pkg
491533 -rw- 31657374       Jul 31 2025 11:50:09 -07:00 cat9k-rpboot.17.18.01.SPA.pkg
491528 -rw- 27681740       Jul 31 2025 11:49:48 -07:00 cat9k-sipbase.17.18.01.SPA.pkg
491529 -rw- 52224968       Jul 31 2025 11:49:49 -07:00 cat9k-sipspace.17.18.01.SPA.pkg
491530 -rw- 31130572       Jul 31 2025 11:49:50 -07:00 cat9k-srdriver.17.18.01.SPA.pkg
491531 -rw- 14783432       Jul 31 2025 11:49:51 -07:00 cat9k-webui.17.18.01.SPA.pkg
491532 -rw- 9160          Jul 31 2025 11:49:51 -07:00 cat9k-wlc.17.18.01.SPA.pkg
11353194496 bytes total (8963174400 bytes free)

```

The following is sample output of the **dir flash:*.conf** command. It displays the .conf files in the flash partition; note the two .conf files:

```

Switch# dir flash:*.conf

Directory of flash:/*.conf
Directory of flash:/

16631  -rw- 4882 Jul 31 2025 05:39:42 +00:00  packages.conf
16634  -rw- 4882 Jul 31 2025 05:34:06 +00:00  cat9k_iosxe.17.18.01.SPA.conf

```

- packages.conf—the file that has been re-written with the newly installed .pkg files
- cat9k_iosxe.17.18.01.SPA.conf—a backup copy of the newly installed packages.conf file

The following is sample output of the **show install summary** command:

```

Switch# show install summary

[ R0 ] Installed Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted,
C - Activated & Committed, D - Deactivated & Uncommitted
-----
Type St Filename/Version
-----
IMG C 17.18.01.0.58

-----
Auto abort timer: inactive
-----

```

The following sample output of the **show version** command displays the Cisco IOS XE 17.18.1 image on the device:

```

Switch# show version

Cisco IOS XE Software, Version 17.18.01
Cisco IOS Software, Catalyst L3 Switch Software (CAT9K_IOSXE), Version 17.18.1, RELEASE SOFTWARE (fcl)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2025 by Cisco Systems, Inc.
<output truncated>

```

Downgrading in Install Mode

Follow these instructions to downgrade from one release to another, in install mode. To perform a software image downgrade, you must be booted into IOS through **boot flash:packages.conf**.

Note that you can use this procedure for the following downgrade scenarios:

When downgrading from ...	Use these commands...	To downgrade to...
Cisco IOS XE 17.18.x	Either install commands or request platform software command ³ .	Cisco IOS XE 17.17.x or earlier releases.

³ The **request platform software** commands are deprecated. So although they are still visible on the CLI, we recommend that you use **install** commands.



Note

New switch models that are introduced in a release cannot be downgraded. The release in which a switch model is introduced is the minimum software version for that model.

This procedure shows the steps to downgrade the Cisco IOS XE software on a switch, from Cisco IOS XE 17.18.1 to Cisco IOS XE 17.17.1 using **install** commands, followed by sample output.

Microcode Downgrade Prerequisite:

Starting from Cisco IOS XE Gibraltar 16.12.1, a new microcode is introduced to support IEEE 802.3bt Type 3 standard for UPOE switches in the series (C9300-24U, C9300-48U, C9300-24UX, C9300-48UXM, C9300-48UN). The new microcode is not backward-compatible with some releases, because of which you must also downgrade the microcode when you downgrade to one of these releases. If the microcode is not downgraded, PoE features will be impacted after the downgrade.

Depending on the *release* you are downgrading to and the *commands* you use to downgrade, review the table below for the action you may have to take:

When downgrading from ...	To one of These Releases	by Using...	Action For Microcode Downgrade
Cisco IOS XE Gibraltar 16.12.1 or a later release	Cisco IOS XE Everest 16.6.1 through Cisco IOS XE Everest 16.6.6	install commands	Microcode will roll back automatically as part of the software installation. No further action is required.
	Cisco IOS XE Fuji 16.9.1 through Cisco IOS XE Fuji 16.9.2	request platform software commands or or bundle boot	Manually downgrade the microcode before downgrading the software image. Enter the hw-module mcu rollback command in global configuration mode, to downgrade microcode.

Step 1 Clean-up **install remove inactive**

Use this command to clean-up old installation files in case of insufficient space and to ensure that you have at least 1GB of space in flash, to expand a new image.

Step 2 Copy new image to flash

a) **copy tftp:[[/location]/directory]/filename flash:**

Use this command to copy the new image from a TFTP server to flash memory. The location is either an IP address or a host name. The filename is specified relative to the directory used for file transfers. Skip this step if you want to use the new image from a TFTP server.

b) **dir flash:**

Use this command to confirm that the image has been successfully copied to flash.

Step 3 Set boot variable

a) **boot system flash:packages.conf**

Use this command to set the boot variable to **flash:packages.conf**.

b) **no boot manual**

Use this command to configure the switch to auto-boot.

c) **write memory**

Use this command to save boot settings.

d) **show boot**

Use this command to verify the boot variable (packages.conf) and manual boot setting (no):

Step 4 Downgrade software image

install add file activate commit

Use this command to install the image.

We recommend that you point to the source image on your TFTP server or the flash drive of the *active* switch, if you have copied the image to flash memory. If you point to an image on the flash or USB drive of a member switch (instead of the active), you must specify the exact flash or USB drive - otherwise installation fails. For example, if the image is on the flash drive of member switch 3 (flash-3): `Switch# install add file flash-3:cat9k_iosxe.17.17.01.SPA.bin activate commit.`



Note

The system reloads automatically after executing the **install add file activate commit** command. You do not have to manually reload the system.

Step 5 Verify version

show version

After the image boots up, use this command to verify the version of the new image.



Note

When you downgrade the software image, the ROMMON version does not downgrade. It remains updated.

Example

The following sample output displays the cleaning up of unused files, by using the **install remove inactive** command:

```
Switch# install remove inactive
```

```
install_remove: START Thu Jul 31 10:34:24 PDT 2025
```


install_remove: Removing IMG
Cleaning up unnecessary package files
No path specified, will use booted path /flash/packages.conf

Cleaning /flash

Scanning boot directory for packages ... done.

Preparing packages list to delete ...

[R0]: /flash/packages.conf File is in use, will not delete.
[R1]: /flash/packages.conf File is in use, will not delete.
[R0]: /flash/cat9k-cc_srdriver.17.18.01.SPA.pkg File is in use, will not delete.
[R1]: /flash/cat9k-cc_srdriver.17.18.01.SPA.pkg File is in use, will not delete.
[R0]: /flash/cat9k-esppbase.17.18.01.SPA.pkg File is in use, will not delete.
[R1]: /flash/cat9k-esppbase.17.18.01.SPA.pkg File is in use, will not delete.
[R0]: /flash/cat9k-guestshell.17.18.01.SPA.pkg File is in use, will not delete.
[R1]: /flash/cat9k-guestshell.17.18.01.SPA.pkg File is in use, will not delete.
[R0]: /flash/cat9k-lni.17.18.01.SPA.pkg File is in use, will not delete.
[R1]: /flash/cat9k-lni.17.18.01.SPA.pkg File is in use, will not delete.
[R0]: /flash/cat9k-rpbase.17.18.01.SPA.pkg File is in use, will not delete.
[R1]: /flash/cat9k-rpbase.17.18.01.SPA.pkg File is in use, will not delete.
[R0]: /flash/cat9k-sipbase.17.18.01.SPA.pkg File is in use, will not delete.
[R1]: /flash/cat9k-sipbase.17.18.01.SPA.pkg File is in use, will not delete.
[R0]: /flash/cat9k-sipspa.17.18.01.SPA.pkg File is in use, will not delete.
[R1]: /flash/cat9k-sipspa.17.18.01.SPA.pkg File is in use, will not delete.
[R0]: /flash/cat9k-srdriver.17.18.01.SPA.pkg File is in use, will not delete.
[R1]: /flash/cat9k-srdriver.17.18.01.SPA.pkg File is in use, will not delete.
[R0]: /flash/cat9k-webui.17.18.01.SPA.pkg File is in use, will not delete.
[R1]: /flash/cat9k-webui.17.18.01.SPA.pkg File is in use, will not delete.
[R0]: /flash/cat9k-wlc.17.18.01.SPA.pkg File is in use, will not delete.
[R1]: /flash/cat9k-wlc.17.18.01.SPA.pkg File is in use, will not delete.
[R0]: /flash/cat9k_iosxe.17.18.01.SPA.conf File is in use, will not delete.
[R1]: /flash/cat9k_iosxe.17.18.01.SPA.conf File is in use, will not delete.
[R0]: /flash/cat9k-rpboot.17.18.01.SPA.pkg File is in use, will not delete.
[R1]: /flash/cat9k-rpboot.17.18.01.SPA.pkg File is in use, will not delete.

The following files will be deleted:

[R0]: /flash/cat9k_iosxe.17.18.01.SPA.bin
[R1]: /flash/cat9k_iosxe.17.18.01.SPA.bin
[R0]: /flash/cat9k-cc_srdriver.17.09.02.SPA.pkg
[R1]: /flash/cat9k-cc_srdriver.17.09.02.SPA.pkg
[R0]: /flash/cat9k-esppbase.17.09.02.SPA.pkg
[R1]: /flash/cat9k-esppbase.17.09.02.SPA.pkg
[R0]: /flash/cat9k-guestshell.17.09.02.SPA.pkg
[R1]: /flash/cat9k-guestshell.17.09.02.SPA.pkg
[R0]: /flash/cat9k-lni.17.09.02.SPA.pkg
[R1]: /flash/cat9k-lni.17.09.02.SPA.pkg
[R0]: /flash/cat9k-rpbase.17.09.02.SPA.pkg
[R1]: /flash/cat9k-rpbase.17.09.02.SPA.pkg
[R0]: /flash/cat9k-sipbase.17.09.02.SPA.pkg
[R1]: /flash/cat9k-sipbase.17.09.02.SPA.pkg
[R0]: /flash/cat9k-sipspa.17.09.02.SPA.pkg
[R1]: /flash/cat9k-sipspa.17.09.02.SPA.pkg
[R0]: /flash/cat9k-srdriver.17.09.02.SPA.pkg
[R1]: /flash/cat9k-srdriver.17.09.02.SPA.pkg
[R0]: /flash/cat9k-webui.17.09.02.SPA.pkg
[R1]: /flash/cat9k-webui.17.09.02.SPA.pkg
[R0]: /flash/cat9k-wlc.17.09.02.SPA.pkg
[R1]: /flash/cat9k-wlc.17.09.02.SPA.pkg
[R0]: /flash/cat9k_iosxe.17.09.02.SPA.conf
[R1]: /flash/cat9k_iosxe.17.09.02.SPA.conf
[R0]: /flash/cat9k-rpboot.17.09.02.SPA.pkg
[R1]: /flash/cat9k-rpboot.17.09.02.SPA.pkg

Do you want to remove the above files? [y/n]

```

Deleting file /flash/cat9k_iosxe.17.18.01.SPA.bin ... done.
Deleting file /flash/cat9k-cc_srdriver.17.09.02.SPA.pkg ... done.
Deleting file /flash/cat9k-esppbase.17.09.02.SPA.pkg ... done.
Deleting file /flash/cat9k-guestshell.17.09.02.SPA.pkg ... done.
Deleting file /flash/cat9k-lni.17.09.02.SPA.pkg ... done.
Deleting file /flash/cat9k-rpbase.17.09.02.SPA.pkg ... done.
Deleting file /flash/cat9k-sipbase.17.09.02.SPA.pkg ... done.
Deleting file /flash/cat9k-sipspa.17.09.02.SPA.pkg ... done.
Deleting file /flash/cat9k-srdriver.17.09.02.SPA.pkg ... done.
Deleting file /flash/cat9k-webui.17.09.02.SPA.pkg ... done.
Deleting file /flash/cat9k-wlc.17.09.02.SPA.pkg ... done.
Deleting file /flash/cat9k_iosxe.17.09.02.SPA.conf ... done.
Deleting file /flash/cat9k-rpboot.17.09.02.SPA.pkg ... done.
Deleting /flash/.images/17.18.01.0.172764.1674613814 ... done.
SUCCESS: Files deleted.

```

```

--- Starting Post_Remove_Cleanup ---

```

```

Performing REMOVE_POSTCHECK on all members

```

```

Finished Post_Remove_Cleanup

```

```

SUCCESS: install_remove Thu Jul 31 10:34:32 PDT 2025

```

```

Switch# copy tftp://10.8.0.6/image/cat9k_iosxe.17.17.01.SPA.bin flash:

```

```

Destination filename [cat9k_iosxe.17.17.01.SPA.bin]?

```

```

Accessing tftp://10.8.0.6/cat9k_iosxe.17.17.01.SPA.bin...

```

```

Loading /cat9k_iosxe.17.17.01.SPA.bin from 10.8.0.6 (via GigabitEthernet0/0):

```

```

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

```

```

[OK - 508584771 bytes]

```

```

508584771 bytes copied in 101.005 secs (5035244 bytes/sec)

```

```

Switch# dir flash:*.bin

```

```

Directory of flash:/*.bin

```

```

Directory of flash:/

```

```

434184 -rw- 508584771 Jul 31 2025 13:35:16 -07:00 cat9k_iosxe.17.17.01.SPA.bin
11353194496 bytes total (9055866880 bytes free)

```

```

Switch(config)# boot system flash:packages.conf

```

```

Switch(config)# no boot manual

```

```

Switch(config)# exit

```

```

Switch# write memory

```

```

Switch# show boot

```

```

Current Boot Variables:

```

```

BOOT variable = flash:packages.conf;

```

```

Boot Variables on next reload:

```

```

BOOT variable = flash:packages.conf;

```

```

Manual Boot = no

```

```

Enable Break = yes

```

```

Boot Mode = DEVICE

```

```

iPXE Timeout = 0

```

The following example displays the installation of the Cisco IOS XE 17.17.1 software image to flash, by using the **install add file activate commit** command.

```

Switch# install add file flash:cat9k_iosxe.17.17.01.SPA.bin activate commit

```

```

install_add_activate_commit: START Thu Jul 31 10:55:53 PDT 2025

```

```

install_add: START Thu Jul 31 10:55:53 PDT 2025

```

```

install_add: Adding IMG
[2] Switch 2 Warning!!! Image is being downgraded from 17.18.01.0.1186 to 17.17.01.0.1444.
--- Starting initial file syncing ---
Copying flash:cat9k_iosxe.17.17.01.SPA.bin from Switch 1 to Switch 1 2
Info: Finished copying to the selected Switch
Finished initial file syncing

--- Starting Add ---
Performing Add on all members
Checking status of Add on [1 2]
Add: Passed on [1 2]
Image added. Version: 17.17.01.0.1444

Finished Add

install_activate: START Thu Jul 31 10:57:32 PDT 2025
install_activate: Activating IMG
Following packages shall be activated:
/flash/cat9k-cc_srdriver.17.17.01.SPA.pkg
/flash/cat9k-esppbase.17.17.01.SPA.pkg
/flash/cat9k-guestshell.17.17.01.SPA.pkg
/flash/cat9k-lni.17.17.01.SPA.pkg
/flash/cat9k-rpbase.17.17.01.SPA.pkg
/flash/cat9k-sipbase.17.17.01.SPA.pkg
/flash/cat9k-sipspa.17.17.01.SPA.pkg
/flash/cat9k-srdriver.17.17.01.SPA.pkg
/flash/cat9k-webui.17.17.01.SPA.pkg
/flash/cat9k-wlc.17.17.01.SPA.pkg
/flash/cat9k-rpboot.17.17.01.SPA.pkg

This operation may require a reload of the system. Do you want to proceed? [y/n]y

--- Starting Activate ---
Performing Activate on all members
[1] Activate package(s) on Switch 1
[2] Activate package(s) on Switch 2
[2] Finished Activate on Switch 2
[1] Finished Activate on Switch 1
Checking status of Activate on [1 2]
Activate: Passed on [1 2]
Finished Activate

--- Starting Commit ---
Performing Commit on all members
[1] Commit package(s) on Switch 1
[2] Commit package(s) on Switch 2
[2] Finished Commit on Switch 2
[1] Finished Commit on Switch 1
Checking status of Commit on [1 2]
Commit: Passed on [1 2]
Finished Commit operation

SUCCESS: install_add_activate_commit Thu Jul 31 11:00:19 PDT 2025
stack-nyqcr3#
Chassis 1 reloading, reason - Reload command
Jul 31 11:00:25.253: %PMAN-5-EXITACTION: F0/0: pvp: Process manager is exiting: reload fp action requested
Jul 31 11:00:26.878: %PMAN-5-EXITACTION: R0/0: pvp: Process manager is exiting: rp processes exit with reload
switch code

Initializing Hardware.....

System Bootstrap, Version 17.18.1r[FC1], RELEASE SOFTWARE (P)

```

Compiled Wed 02/08/2025 14:36:07.63 by rel

Current ROMMON image : Primary
Last reset cause : SoftwareReload
C9300-48UXM platform with 8388608 Kbytes of main memory

Preparing to autoboot. [Press Ctrl-C to interrupt] 0
boot: attempting to boot from [flash:packages.conf]
boot: reading file packages.conf

#

#####

Waiting for 120 seconds for other switches to boot

Switch number is 1
All switches in the stack have been discovered. Accelerating discovery

The following sample output of the **show version** command displays the Cisco IOS XE 17.17.1 image on the device:

Switch# **show version**

Cisco IOS XE Software, Version 17.17.01
Cisco IOS Software [Dublin], Catalyst L3 Switch Software (CAT9K_IOSXE), Version 17.17.1, RELEASE SOFTWARE (fc1)
Technical Support: <http://www.cisco.com/techsupport>
Copyright (c) 1986-2025 by Cisco Systems, Inc.
<output truncated>

Upgrading the ROMMON

To know the ROMMON or bootloader version that applies to every major and maintenance release, see [ROMMON and CPLD Versions, on page 14](#).

You can upgrade the ROMMON before, or, after upgrading the software version. If a new ROMMON version is available for the software version you are upgrading to, proceed as follows:

- Upgrading the ROMMON in the primary SPI flash device

This ROMMON is upgraded automatically. When you upgrade from an existing release on your switch to a later or newer release for the first time, and there is a new ROMMON version in the new release, the system automatically upgrades the ROMMON in the primary SPI flash device, based on the hardware version of the switch.

- Upgrading the ROMMON in the golden SPI flash device

You must manually upgrade this ROMMON. Enter the **upgrade rom-monitor capsule golden switch** command in privileged EXEC mode.



Note

- Golden ROMMON upgrade is only applicable to Cisco IOS XE Amsterdam 17.3.5 and later releases.
- Golden ROMMON upgrade will fail if the FPGA version is 17101705 or older. To upgrade the FPGA version, see [Upgrading the Complex Programmable Logic Device Version](#).
- In case of a Cisco StackWise Virtual setup, upgrade the active and standby supervisor modules.
- In case of a High Availability set up, upgrade the active and standby supervisor modules.

After the ROMMON is upgraded, it will take effect on the next reload. If you go back to an older release after this, the ROMMON is not downgraded. The updated ROMMON supports all previous releases.

Upgrading the Complex Programmable Logic Device Version

You can trigger a CPLD version upgrade after upgrading the software image. During CPLD upgrade, the supervisor module automatically power cycles which may cause a temporary loss of uplink connectivity. This completes the CPLD upgrade process for the supervisor module. Auto-upgrade of CPLD is not supported, and so you must manually perform CPLD upgrade.

Upgrading the CPLD Version: High Availability Setup

Beginning in the privileged EXEC mode, complete the following steps:

When performing the CPLD version upgrade as shown, the **show platform** command can be used to confirm the CPLD version after the upgrade. This command output shows the CPLD version on all modules. However, the CPLD upgrade only applies to the supervisors, not the line cards. The line cards CPLD version is a cosmetic display. After the upgrade is completed in a high availability setup, the supervisors will be upgraded, but the line cards will still show the old CPLD version. The version mismatch between the supervisors and line cards is expected until a chassis reload.

Step 1 Upgrade the CPLD Version of the standby supervisor module

Enter the following commands on the active supervisor:

- a) Device# **configure terminal**
- b) Device(config)# **service internal**
- c) Device(config)# **exit**
- d) Device# **upgrade hw-programmable cpld filename bootflash: rp standby**

The standby supervisor module reloads automatically and the upgrade occurs in ROMMON. During the upgrade, the supervisor module automatically power cycles and remains inactive for approximately 5 minutes.

Wait until the standby supervisor module boots up and the SSO has formed (HOT) before you proceed to the next step; this takes approximately 17 minutes.

Step 2 Perform a switch over

- a) Device# **redundancy force-switchover**

This causes the standby supervisor (on which you have completed the CPLD upgrade in Step 1) to become the active supervisor module

Step 3 Upgrade the CPLD Version of the new standby supervisor module

Repeat Step 1 and all its substeps.



Note

Do not operate an HA system with mismatched FPGA versions. FPGA version should be upgraded on both the supervisors one at a time.

Upgrading the CPLD Version: Cisco StackWise Virtual Setup

Beginning in the privileged EXEC mode, complete the following steps:

Step 1 Upgrade the CPLD version of the standby supervisor module

Enter the following commands on the active supervisor:

- a) Device# **configure terminal**
- b) Device(config)# **service internal**
- c) Device(config)# **exit**
- d) Device# **upgrade hw-programmable cpld filename bootflash: switch standby [r0 | r1]**

Use **r0** if the targeted Supervisor is on the lower slot of the chassis, and **r1** if the targeted Supervisor is on the upper slot of the chassis.



Note

For the **upgrade hw-programmable cpld filename bootflash** command, configure with the **switch** keyword only. The other available keywords are not applicable when upgrading with Cisco StackWise Virtual.

Step 2 Reload the standby supervisor module

- a) Device# **redundancy reload peer**

The upgrade occurs in ROMMON. During the upgrade, the supervisor module automatically power cycles and remains inactive for approximately 5 minutes.

Wait until the standby supervisor module boots up and the SSO has formed (HOT) before you proceed to the next step; this takes approximately 17 minutes.

Step 3 Perform a switch over

- a) Device# **redundancy force-switchover**

This causes the standby supervisor (on which you have completed the CPLD upgrade in step 1) to become the active supervisor module

Step 4 Upgrade the CPLD version of the new standby supervisor module

Perform Steps 1 and 2, including all substeps, on the new standby supervisor module

Upgrading the CPLD Version: Single Supervisor Module Setup

Beginning in the privileged EXEC mode, complete the following steps:

Upgrade the CPLD version of the active supervisor module

Enter the following commands on the active supervisor:

- a) Device# **configure terminal**
- b) Device(config)# **service internal**
- c) Device(config)# **exit**
- d) Device# **upgrade hw-programmable cpld filename bootflash: rp active**

The supervisor module reloads automatically and the upgrade occurs in ROMMON. During the upgrade, the supervisor module automatically power cycles and remains inactive for approximately 5 minutes.

In-Service Software Upgrade with Cisco Stackwise Virtual

In-Service Software Upgrade (ISSU) is a process that upgrades an image to another image on a device while the network continues to forward packets. ISSU helps network administrators avoid a network outage when performing a software upgrade. ISSU is supported in install mode.

ISSU is supported in dual SUP HA and StackWise Virtual system. In-Service Software Upgrade is performed either in a single step or in three-steps.

ISSU Support between Releases

- Within a major release train (16.x or 17.x or 18.x), ISSU is supported between any two Extended Maintenance (EM) releases that are released not more than 3 years apart.
- Within a major release train, ISSU is supported from:
 - Any EM (EM1, EM2, EM3) release to another EM (EM1, EM2, EM3) release

Example:

16.9.x to 16.12,

17.3.x to 17.6.x, 17.3.x to 17.9.x, 17.3.x to 17.12.x and so on

17.6.x to 17.9.x, 17.6.x to 17.12.x, 17.6.x to 17.15.x and so on

17.9.x to 17.12.x, 17.9.x to 17.15.x and so on

- Any release within the same EM release

Example:

16.9.2 to 16.9.3 or 16.9.4 or 16.9.x

16.12.1 to 16.12.2 or 16.12.3 or 16.12.x

17.3.1 to 17.3.2 or 17.3.3 or 17.3.x

- ISSU Recommendation: From any EM recommended release on CCO to current EM Recommended release on CCO.



Note

The **snmp-server enable traps energywise** command and related subcommands must be removed before upgrading to Cisco IOS XE 17.15.1 and 17.15.2 using ISSU.

See [In-Service Software Upgrade \(ISSU\)](#) for information on ISSU support for Catalyst platforms and [Software Lifecycle Support Statement](#) for information extended and standard maintenance releases.

Scaling Information

For information about feature scaling guidelines, see these datasheets for Cisco Catalyst 9400 Series Switches:

<https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9400-series-switches/nb-06-cat9400-ser-data-sheet-cte-en.html>

<https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9400-series-switches/nb-06-cat9600-series-line-data-sheet-cte-en.html>

<https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9400-series-switches/nb-06-cat9400-ser-sup-eng-data-sheet-cte-en.html>

Related Content

This section provides links to the product documentation and troubleshooting 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

Starting with Cisco IOS XE Fuji 16.8.1a, as an improved security measure, the way in which hidden commands can be accessed has changed.

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.

Starting with Cisco IOS XE Fuji 16.8.1a, 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 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 information about Cisco IOS XE, visit [Cisco IOS XE](#).

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

For all supported documentation of Cisco Catalyst 9400 Series Switches, visit [Cisco Catalyst 9400 Series Switches](#).

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](#).

Product Information

Information on end-of-life (EOL) details specific to the Cisco Catalyst 9400 Series Switches is at this URL: <https://www.cisco.com/c/en/us/products/switches/catalyst-9400-series-switches/eos-eol-notice-listing.html>

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](#).

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.