

Revised: September 28, 2026

Release Notes for Cisco Catalyst 9500 Series Switches, Cisco IOS XE 26.2.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
September 28, 2026	26.2.1	• What's New: Software features • Caveats: Open and resolved caveats • Compatibility Matrix: Compatibility information for 26.2.1 • Software Images: Software images for 26.2.1 • ROMMON Versions: ROMMON versions for 26.2.1

Introduction

Cisco Catalyst 9500 Series Switches - High Performance and Cisco Catalyst 9500X Series Switches are Cisco's lead, fixed core and aggregation enterprise switching platforms. They have been purpose-built to address emerging trends of Security, IoT, Mobility, and Cloud.

They deliver complete convergence in terms of ASIC architecture with Unified Access Data Plane (UADP) 3.0 on Cisco Catalyst 9500 Series Switches - High Performance, and Q200 on Cisco Catalyst 9500X Series Switches. The platform runs an Open Cisco IOS XE that supports model driven programmability. This series forms the foundational building block for SD-Access, which is Cisco's lead enterprise architecture.

Note

There may be differences in the supported and unsupported features, limitations, and caveats that apply to the specific models. Throughout this release note document, any such differences are expressly called out. If they are not, the information applies to all models in the series.

Supported Cisco Catalyst 9500 Series Switches Model Numbers

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

Base PIDs are the model numbers of the switch.

Bundled PIDs indicate the orderable part numbers for base PIDs that are bundled with a particular network module. Entering the **show version**, **show module**, or **show inventory** commands on such a switch (bundled PID), displays its base PID.

Table 2: Cisco Catalyst 9500 Series Switches-High Performance

Switch Model	Default License Level ¹	Description	Introductory Release
C9500-24Y4C-E	Network Essentials	24 SFP28 ports that support 1/10/25-GigabitEthernet connectivity, four QSFP uplink ports that support 100/40-GigabitEthernet connectivity; two power supply slots.	Cisco IOS XE Fuji 16.8.1a
C9500-24Y4C-A	Network Advantage		Cisco IOS XE Fuji 16.8.1a
C9500-32C-E	Network Essentials	32 QSFP28 ports that support 40/100 GigabitEthernet connectivity; two power supply slots.	Cisco IOS XE Fuji 16.8.1a
C9500-32C-A	Network Advantage		Cisco IOS XE Fuji 16.8.1a
C9500-32QC-E	Network Essentials	32 QSFP28 ports, where you can have 24 ports that support 40-GigabitEthernet connectivity and 4 ports that support 100-GigabitEthernet connectivity, OR 32 ports that support 40-GigabitEthernet connectivity, OR 16 ports that support 100-GigabitEthernet connectivity; two power supply slots.	Cisco IOS XE Fuji 16.8.1a
C9500-32QC-A	Network Advantage		Cisco IOS XE Fuji 16.8.1a
C9500-48Y4C-E	Network Essentials	48 SFP28 ports that support 1/10/25-GigabitEthernet connectivity; four QSFP uplink ports that supports up to 100/40-GigabitEthernet connectivity; two power supply slots.	Cisco IOS XE Fuji 16.8.1a
C9500-48Y4C-A	Network Advantage		Cisco IOS XE Fuji 16.8.1a

¹ See section *Licensing* → *Table: Permitted Combinations*, in this document for information about the add-on licenses that you can order.

Table 3: Cisco Catalyst 9500X Series Switches

Switch Model	Default License Level ²	Description	Introductory Release
C9500X-28C8D-E	Network Essentials	28x100G QSFP28 and 8x400G QSFP-DD ports; two power supply slots	Cisco IOS XE Cupertino 17.7.1
C9500X-28C8D-A	Network Advantage		Cisco IOS XE Cupertino 17.7.1
C9500X-60L4D-A	Network Advantage	60x50G SFP56 and 4x400G QSFP-DD ports; two power supply slots	Cisco IOS XE Dublin 17.10.1b

² See section *Licensing* → *Table: Permitted Combinations*, in this document for information about the add-on licenses that you can order.

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 26.2.x

Hardware Features in Cisco IOS XE 26.2.1

Table 4: Hardware features introduced on Cisco Catalyst 9500 Series Switches

Feature Name	Description and Documentation Link
100GBASE QSFP-100G module	Supported transceiver module product number: • QSFP-100G-ZR4-S: high powered optics. Compatible switch models: • C9500-32C: Supported only on ports 29 and 31. • C9500-48Y4C: Supported only on ports 49 and 51.  If this optic is inserted in any other port than the supported ports, the port is placed in the error-disabled state. Note For information about the module, see Cisco 100GBASE QSFP-100G Modules Data Sheet. For information about device compatibility, see the Transceiver Module Group (TMG) Compatibility Matrix.

Software Features in Cisco IOS XE 26.2.1

Feature Name	Applicable Models	Description
BGP EVPN VXLAN IRB in the global routing table or non-EVPN VRF	All Models	BGP EVPN VXLAN IRB host routing enables a VTEP to create IPv4 /32 and IPv6 /128 static routes from locally learned EVPN MAC/IP bindings. The VTEP installs these routes in the routing table associated with the IRB SVI: either the global routing table (GRT) or a non-EVPN VRF. The routes are eligible for redistribution into an IGP or BGP, subject to the configured redistribution policy. This provides Layer 3 host reachability without requiring an EVPN L3VNI or route leaking through an EVPN IP-VRF.
BGP IPv4 prefix with IPv6 next-hop	All Models	IPv4 routes via IPv6 next-hop (RFC 5549) is a BGP control plane and data plane solution that allows IPv4 routes to be advertised with IPv6 next-hop address. It enables IPv4 packet forwarding using IPv6 encapsulation across an IPv6-only core network, eliminating the requirement to assign IPv4 addresses on core transit interfaces.

Feature Name	Applicable Models	Description
Cisco Cloud Redirection for device onboarding	All Models	You can now utilize Cisco Cloud Redirection for zero-touch discovery on both IPv4 and IPv6 networks, simplifying device onboarding. When your device boots without configuration or valid certificates, it contacts the Cisco Cloud server and downloads a trustpool bundle, enabling secure communication and streamlined setup processes.
Disable HTTPS servers by default (exceptions allowed)	All Models	Disables HTTPS servers by default with provisions for allowed exceptions.
MACsec PQC	C9500H	MACsec provides quantum-resistant protection for key establishment using Module-Lattice Key Encapsulation Mechanism (ML-KEM) in the TLS 1.3 handshake.
Programmability: • MAC address table mapping • Negotiated port-speed • YANG Data Models	All Models	The following programmability features are introduced in this release: • The MATM-STATE-OPER model manages and monitors large-scale MAC address tables and supports high-scale MAC address telemetry. • On-change subscriptions support negotiated-port-speed leaf to enable real-time notifications along with the existing subscription-based access. • 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/2621.

Feature Name	Applicable Models	Description
Resilient Infrastructure changes	All Models	

Feature Name	Applicable Models	Description
		As part of Cisco’s Resilient Infrastructure program and Cisco’s commitment to secure infrastructure, this release includes additional changes aimed towards continuing to make Cisco IOS XE more secure by default. Note that some of these changes may require operational changes if you are not following secure best practices. This release includes the following changes: • The RADIUS client appends the <code>Message-Authenticator</code> attribute (Attribute 80 HMAC-MD5) to all outgoing <code>Access-Request</code> packets to mitigate cryptographic forgery and Blast-RADIUS vulnerabilities (CVE-2024-3596). • The RADIUS client drops incoming <code>Access-Accept</code>, <code>Access-Reject</code>, and <code>Access-Challenge</code> packets if the <code>Message-Authenticator</code> packet is absent or invalid. Ensure AAA servers (example, Cisco ISE) are configured to return Attribute 80. • Outbound SSH connections enforce Trust-On-First-Use (TOFU). The device prompts to verify and store remote server host keys in the known-hosts database on first connection and validates against them on subsequent sessions. • Proxy ARP is disabled by default across all routed interfaces, SVIs, and subinterfaces to reduce Layer 2 broadcast domains and prevent ARP spoofing. Configure the <code>ip proxy-arp</code> command explicitly if required. • The embedded web server daemon is disabled by default on factory configurations to restrict unauthenticated management access. Web UI and RESTCONF require explicit enablement of the <code>ip http secure-server</code> command. • The IOS XE device rejects unauthenticated NTP Mode 6 and Mode 7 control queries (<code>monlist</code>) to prevent NTP reflection and amplification DDoS attacks. Standard time synchronization (Modes 3 and 4) is unaffected. • System logging timestamps automatically include the four-digit calendar year (<code>service timestamps log datetime msec year</code>) to standardize multi-year audit logs and SIEM compliance. • The system restricts storing credentials in weak or reversible hashing formats (Type 0 cleartext, Type 5 MD5, Type 7 Vigenère) and defaults new password creation to Type 8 (PBKDF2 SHA-256), Type 9 (Scrypt), or Type 6 (AES). • Integrates Linux <code>auditd</code> inside Cisco IOx Guest Shell. All commands, system calls, and privilege escalation events (<code>sudo</code>) executed inside the container are forwarded to the host syslog facility. • Warning messages are emitted on the console and logged to syslog whenever legacy insecure protocols (<code>telnet</code>, <code>ftp</code>, <code>tftp</code>, <code>http</code>) are enabled in the configuration. • Real-time tracking of active insecure services is published to the operational database (<code>operDB</code>) and YANG data models, allowing

Feature Name	Applicable Models	Description
		management controllers (such as Cisco Catalyst Center) to monitor security compliance. For more information, refer Resilient Infrastructure .
Cisco Switching Licensing	All Models	Cisco Switching Licensing is a unified licensing model that provides two software license levels for all Cisco Catalyst 9000 Series Switches: Essentials and Advantage. • Essentials: Provides fundamental features and functionalities to manage a network. • Advantage: Enables management of a network with all essential features, plus advanced capabilities such as StackWise Virtual Link (SVL), Cloud-delivered security, and Cisco AI Network Analytics.

New on the WebUI

Enhanced Day 0 Web UI Account Settings: This feature was modified to improve access security by defining username and password guidelines for the Day 0 Web UI account configuration.

Hardware and Software Behavior Changes in Cisco IOS XE 26.2.1

Behavior Change	Description
CDP and LLDP device ID	In cloud-managed mode, CDP and LLDP use the device hostname as the device ID instead of the switch MAC address.
Port-channel VLAN configuration	When the switchport trunk allowed vlan command is applied to a portchannel via the configuration database (CDB) or NETCONF, the inherited configurations on member interfaces do not synchronize with the CDB database.
Power supply capacity display	Power supply capacity is displayed in watts instead of kilowatts. For example, values that were previously displayed as 1.1KW and 0.75KW are now displayed as 1100W and 750W.

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 26.2.x

There are no open caveats in this release.

Resolved Caveats in Cisco IOS XE 26.2.1

Identifier	Applicable Models	Headline
CSCwu77294	C9500X	C9500X/C9600X VLAN 2 and VLAN 3 Adjacency download failures and IP Prefix download failures after upgrade to 17.15

Feature Support

This section lists the default behaviour, supported, and unsupported features.

Default Behavior

DF Bit Behavior for RADIUS Packets—All Models

Beginning from Cisco IOS XE Gibraltar 16.12.5 and later, do not fragment bit (DF bit) in the IP packet is always set to 0 for all outgoing RADIUS packets (packets that originate from the device towards the RADIUS server).

Default Interface Behavior on Cisco Catalyst 9500 Series Switches - High Performance

From Cisco IOS XE Gibraltar 16.11.1, the default interface for all High Performance models in the series changes from Layer 3 to Layer 2. Use the **no switchport** command to change the Layer 2 interface into Layer 3 mode.

The startup configuration has explicit configuration of the **switchport** command for Layer 2 interfaces and the **no switchport** command for Layer 3 interfaces to address this change in behavior and to support seamless migration.

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 9500 Series-High Performance and 9500X Series Switches. 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 all PIDs.

For the list of Cisco Catalyst 9500 Series-High Performance and 9500X Switches PIDs, see [Supported Cisco Catalyst 9500 Series Switches Model Numbers](#).

BGP EVPN VXLAN

Feature	Not Supported On These Variants
BUM Traffic Rate Limiting	C9500X
Dynamic ARP inspection (DAI) and DHCP Rogue Server Protection	C9500X
EVPN VXLAN Centralized Default Gateway	C9500X
VXLAN-Aware Flexible Netflow	C9500X

Feature	Not Supported On These Variants
MPLS Layer 3 VPN Border Leaf Handoff	C9500X
MPLS Layer 3 VPN Border Spine Handoff	C9500X
VPLS over MPLS Border Leaf Handoff	C9500X
VPLS over MPLS Border Spine Handoff	C9500X
Interworking of Layer 3 TRM with MVPN Networks for IPv4 Traffic	C9500X
Private VLANs (PVLANS)	C9500X
BGP EVPN VXLAN with IPv6 in the Underlay (VXLANv6)	C9500X
VRF aware NAT64 EVPN Fabric	C9500X
EVPN VXLAN Multi-Homing	C9500X

Cisco TrustSec

Feature	Not Supported On These Variants
Cisco TrustSec Security Association Protocol (SAP)	C9500X
Cisco TrustSec SGT Caching	C9500X

High Availability

Feature	Not Supported On These Variants
Graceful Insertion and Removal	C9500X
Secure StackWise Virtual	C9500X
Cisco Nonstop Forwarding with Stateful Switchover	C9500X

Interface and Hardware

Feature	Not Supported On These Variants
EnergyWise	C9500H, C9500X

IP Addressing Services

Feature	Not Supported On These Variants
Next Hop Resolution Protocol (NHRP)	C9500X
Network Address Translation (NAT)	C9500X

Feature	Not Supported On These Variants
Gateway Load Balancing Protocol (GLBP)	C9500X
Web Cache Communication Protocol (WCCP)	C9500X
Switchport Block Unknown Unicast and Switchport Block Unknown Multicast	C9500X
Message Session Relay Protocol (MSRP)	C9500X
TCP MSS Adjustment	C9500X

IP Multicast Routing

Feature	Not Supported On These Variants
IPv6 Multicast and IPv6 Multicast over Point-to-Point GRE	C9500H
Multicast Routing over GRE Tunnel	C9500X
Multicast VLAN Registration (MVR) for IGMP Snooping	C9500X
IPv6 Multicast over Point-to-Point GRE	C9500X
IGMP Proxy	C9500X
Bidirectional PIM	C9500X
mVPN Extranet Support	C9500X
MLDP-Based VPN	C9500X
PIM Snooping	C9500X
PIM Dense Mode	C9500X

IP Routing

Feature	Not Supported On These Variants
PIM Bidirectional Forwarding Detection (PIM BFD), PIM Snooping	C9500X
OSPF NSR	C9500X
OSPFv3 NSR	C9500X
OSPFv2 Loop-Free Alternate IP Fast Reroute	C9500X
Unicast and Multicast over Point-to-Multipoint GRE	C9500H
BFD Multihop Support for IPv4 Static Routes	C9500H

Feature	Not Supported On These Variants
EIGRP Loop-Free Alternate IP Fast Reroute	C9500X
PBR for Object-Group Access Control List (OGACL) Based Matching	C9500X
Multipoint GRE	C9500X
GRE IPv6 Tunnels	C9500X
IP Fast Reroute (IP FRR)	C9500X
Non-stop Routing	C9500X
Policy-based Routing: set ip next-hop recursive and set ip next-hop verify-availability commands	C9500X

Layer 2

Feature	Not Supported On These Variants
Audio Engineering Society: AES67 Timing Profile	C9500X
Q-in-Q on a Trunk Port	C9500X
Resilient Ethernet Protocol	C9500H, C9500X
Multi-VLAN Registration Protocol (MVRP)	C9500X
Loop Detection Guard	C9500X
Cross-Stack UplinkFast	C9500X
Optional Spanning Tree Protocol	C9500X
Precision Time Protocol (PTP)	C9500X
PTPv2 on Cisco StackWise Virtual	C9500X
Fast UniDirectional Link Detection	C9500X
UniDirectional Link Detection (UDLD)	C9500X
IEEE 802.1Q Tunneling	C9500X
One-to-One VLAN Mapping	C9500X
Selective Q-in-Q	C9500X
Audio Video Bridging (AVB): IEEE 802.1BA	C9500X
Flexlink+	C9500H, C9500X
VLAN Load Balancing for FlexLink+	C9500H, C9500X

Feature	Not Supported On These Variants
Preemption for VLAN Load Balancing	C9500H, C9500X
FlexLink+ Dummy Multicast Packets	C9500H, C9500X

Multiprotocol Label Switching

Feature	Not Supported On These Variants
MPLS Label Distribution Protocol (MPLS LDP) VRF-Aware Static Labels	C9500H
VPLS Routed Pseudowire IRB(v4) Unicast	C9500H
LAN MACsec over Multiprotocol Label Switching (MPLS)	C9500X
BGP Multipath Load Sharing for Both eBGP and iBGP in an MPLS VPN	C9500X
MPLS over GRE	C9500X
MPLS Layer 2 VPN over GRE	C9500X
MPLS Layer 3 VPN over GRE	C9500X
Virtual Private LAN Service (VPLS)	C9500X
VPLS Autodiscovery, BGP-based	C9500X
VPLS Layer 2 Snooping: Internet Group Management Protocol or Multicast Listener Discovery	C9500X
Hierarchical VPLS with Multiprotocol Label Switching Access	C9500X
VPLS Routed Pseudowire IRB(v4) Unicast	C9500X
MPLS VPN Inter-AS Options (options B and AB)	C9500X
MPLS VPN Inter-AS IPv4 BGP Label Distribution	C9500X
Seamless Multiprotocol Label Switching	C9500X

Network Management

Feature	Not Supported On These Variants
Flexible NetFlow: TrustSec NetFlow IPv4 Security Group Access Control List (SGACL) Deny and Drop Export	C9500X
Cisco Application Visibility and Control (AVC)	C9500H, C9500X
Flow-Based Switch Port Analyser	C9500X

Feature	Not Supported On These Variants
RSPAN	C9500X
FRSPAN	C9500X
Egress Netflow	C9500X
IP Aware MPLS Netflow	C9500X
NetFlow Version 5	C9500X

Quality of Service

Feature	Not Supported On These Variants
QoS Ingress Shaping	C9500X
VPLS QoS	C9500X
Per VLAN Policy and Per Port Policer	C9500X
Mixed COS/DSCP Threshold in a QoS LAN-queueing Policy	C9500X
Easy QoS: match-all Attributes	C9500X
Classify: Packet Length	C9500X
Class-Based Shaping for DSCP/Prec/COS/MPLS Labels	C9500X
Egress Policing	C9500X
Egress Microflow Destination-Only Policing	C9500X
Ethertype Classification	C9500X
Packet Classification Based on Layer3 Packet-Length	C9500X
PACLs	C9500X
Per IP Session QoS	C9500X
Per Queue Policer	C9500X
QoS Data Export	C9500X
QoS L2 Missed Packets Policing	C9500X

Security

Feature	Not Supported On These Variants
Lawful Intercept	C9500X
Wake-on-LAN (WoL)	C9500H, C9500X

Feature	Not Supported On These Variants
MACsec: • Switch-to-host MACsec • Cisco TrustSec Security Association Protocol • Fallback Key • MACsec EAP-TLS	C9500X
MAC ACLs	C9500X
Port ACLs	C9500X
VLAN ACLs	C9500X
IP Source Guard	C9500X
IPv6 Source Guard	C9500X
Web-based Authentication	C9500X
Port Security	C9500X
Weighted Random Early Detection mechanism (WRED) Based on DSCP, PREC, or COS	C9500X
IEEE 802.1x Port-Based Authentication	C9500X
Dynamic ARP Inspection	C9500X
Dynamic ARP Inspection Snooping	C9500X

System Management

Feature	Not Supported On These Variants
Network-Based Application Recognition (NBAR) and Next-Generation NBAR (NBAR2)	C9500H, C9500X
Unicast MAC Address Filtering	C9500X

VLAN

Feature	Not Supported On These Variants
Wired Dynamic PVLAN	C9500X
Private VLANs	C9500X

Limitations and Restrictions

If a feature is not supported on a switch model, you do not have to factor in any limitations or restrictions that may be listed here. If limitations or restrictions are listed for a feature that is supported, check if model numbers are specified, to know if they apply. If model numbers are not specified, the limitations or restrictions apply to all models in the series.

- Auto negotiation (the **speed auto** command) and half duplex (the **duplex half** command) are not supported on GLC-T or GLC-TE transceivers for 10 Mbps and 100 Mbps speeds. This applies only to the C9500-48Y4C and C9500-24Y4C models of the series.

We recommend not changing Forward Error Correction (FEC) when auto negotiation is ON. This is applicable to 100G/40G/25G CU cables on the C9500-32C, C9500-32QC, C9500-24Y4C and C9500-48Y4C models of the series.

- 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 StackWise Virtual: On Cisco Catalyst 9500 Series Switches - High Performance,
 - When Cisco StackWise Virtual is configured, breakout ports using 4X25G or 4X10G breakout cables can only be used as data ports; they cannot be used to configure SVLs or DAD links.
 - When Cisco StackWise Virtual is configured, Cisco QSA module with 10G SFP modules can be used as data ports and to configure SVLs or DAD links.
 - When Cisco StackWise Virtual is configured, Cisco QSA module with 1G SFP modules can be used as data ports and to configure DAD links; they cannot be used to configure SVLs since SVLs are not supported on 1G interfaces.
 - 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):
 - 1G with Cisco QSA Module (CVR-QSFP-SFP10G) is not supported on the uplink ports of the C9500-24Y4C and C9500-48Y4C models.
 - Installation restriction for SFP-10G-T-X module on C9500-24Y4C and C9500-48Y4C: Only eight SFP-10G-T-X modules are supported at a time. If you insert a ninth SFP-10G-T-X module in a lower numbered port than the existing active eight SFP-10G-T-X module, a reload will bring up the ninth transceiver and moves the last existing port with SFP-10G-T-X module to error disabled state. This happens due to the order of sequence ports link bring up where the lower numbered port brings up the link first. This limitation applies in standalone and in Cisco StackWise Virtual setup with two C9500-24Y4C or C9500-48Y4C switches. Each switch can have eight SFP-10G-T-X modules.
- The following error displays on the console if you insert a ninth module with eight active modules:
- ```
"%IOMD_ETHER_GEIM-4-MAX_LIMIT_XCVR: R0/0: iomd: Number of SFP-10G-T-X that can be supported has reached the max limit of 8, transceiver is err-disabled. Unplug the transceiver in interface TwentyFiveGigE1/0/29"
```
- SFP-10G-T-X supports 100Mbps/1G/10G speeds based on auto negotiation with the peer device. You cannot force speed settings from the transceiver.

- Hardware Limitations:
  - Use the MODE button to switch-off the beacon LED.
  - All port LED behavior is undefined until interfaces are fully initialized.
  - The following limitations apply to Cisco QSA Module (CVR-QSFP-SFP10G) when Cisco 1000Base-T Copper SFP (GLC-T) or Cisco 1G Fiber SFP Module for Multimode Fiber are plugged into the QSA module:
    - 1G Fiber modules over QSA do not support autonegotiation. Auto-negotiation should be disabled on the far-end devices.
    - Although visible in the CLI, the command **[no] speed nonegotiate** is not supported with 1G Fiber modules over QSA.
    - Only GLC-T over QSA supports auto-negotiation.
    - GLC-T supports only port speed of 1000 Mb/s over QSA. Port speeds of 10/100-Mb/s are not supported due to hardware limitation.
  - 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.
  - Autonegotiation is not supported on HundredGigabitEthernet1/0/49 to HundredGigabitEthernet1/0/52 uplink ports of the C9500-48Y4C models, and HundredGigabitEthernet1/0/25 to HundredGigabitEthernet1/0/28 uplink ports of the C9500-24Y4C models. Disable autonegotiation on the peer device if you are using QSFP-H40G-CUxx and QSFP-H40G-ACUxx cables.
  - For QSFP-H100G-CUxx cables, the C9500-48Y4C and C9500-24Y4C models support the cables only if both sides of the connection are either C9500-48Y4C or C9500-24Y4C.
  - For C9500-32C model, the power supply with serial number starting with POG has two fans and the power supply with serial number starting with QCS has a single fan. When you use **show environment status** command, the fan status of one fan is always displayed as N/A when the power supply with single fan is installed into the power supply slot. See [Configuring Internal Power Supplies](#).
- 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 26.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, 26.2.x to 26.2.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.
- On Cisco Catalyst 9500 Series Switches - High Performance (C9500-24Y4C, C9500-32C, C9500-32QC, and C9500-48Y4C), ISSU with Cisco StackWise Virtual is supported only starting from Cisco IOS XE Gibraltar 16.12.1. Therefore, ISSU upgrades can be performed only starting from this release to a later release.
- 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.

#### • QoS restrictions

The following restrictions apply to UADP-powered Catalyst 9500 High Performance models only.

- 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.

#### • 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.
- 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
```

- MACsec switch-to-host connections in EVPN fabric network is not supported. 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.
- Wired Application Visibility and Control limitations:
  - NBAR2 (QoS and Protocol-discovery) configuration is allowed only on wired physical ports. It is not supported on virtual interfaces, for example, VLAN, port channel nor other logical interfaces.
  - NBAR2 based match criteria ‘match protocol’ is allowed only with marking or policing actions. NBAR2 match criteria will not be allowed in a policy that has queuing features configured.
  - ‘Match Protocol’: up to 256 concurrent different protocols in all policies.
  - NBAR2 and Legacy NetFlow cannot be configured together at the same time on the same interface. However, NBAR2 and wired AVC Flexible NetFlow can be configured together on the same interface.
  - Only IPv4 unicast (TCP/UDP) is supported.
  - AVC is not supported on management port (Gig 0/0)
  - NBAR2 attachment should be done only on physical access ports. Uplink can be attached as long as it is a single uplink and is not part of a port channel.
  - Performance: Each switch member is able to handle 500 connections per second (CPS) at less than 50% CPU utilization. Above this rate, AVC service is not guaranteed.
  - Scale: Able to handle up to 5000 bi-directional flows per 24 access ports and 10000 bi-directional flows per 48 access ports.
- 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.
- On the Cisco Catalyst 9500X Series Switches, TCAM space will not be reserved for different features. The available TCAM space will be shared across the features.
- 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.
- Starting from Cisco IOS XE Release 17.10, the following Key Exchange and MAC algorithms are removed from the default list:

Key Exchange algorithm:

- diffie-hellman-group14-sha1

MAC algorithms:

- hmac-sha1
- hmac-sha2-256
- hmac-sha2-512



#### Note

---

You can use the **ip ssh server algorithm kex** command to configure the Key Exchange algorithm and the **ip ssh server algorithm mac** command to configure the MAC algorithms.

---

## 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.



#### Note

---

On the Cisco Catalyst 9500 Series Switches-High Performance, it is from Cisco IOS XE Fuji 16.8.1a to Cisco IOS XE Amsterdam 17.3.1.

---

- 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 9500 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 ROMMON, 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.



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 26.2.1 | CAT9K_IOSXE                 | cat9k_iosxe.26.02.01.SPA.bin     |
|                     | No Payload Encryption (NPE) | cat9k_iosxe_npe.26.02.01.SPA.bin |

To download software images, visit the software downloads page: [Cisco Catalyst 9500 Series 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.

This table provides information about the ROMMON version that is bundled with the Cisco IOS XE releases for Cisco Catalyst 9500 Series Switches. A Cisco IOS XE release is also compatible with a ROMMON version lower or higher than what is specified in this table. For more information, see "Upgrading the ROMMON" section.

For ROMMON version information of Cisco IOS XE 17.x.x releases, refer to the corresponding Cisco IOS XE 17.x.x release notes of the respective platform.

| Release | ROMMON Version (C9500-32C, C9500-32QC, C9500-24Y4C, C9500-48Y4C) | ROMMON Version (C9500X) |
|---------|------------------------------------------------------------------|-------------------------|
| 26.2.1  | 17.8.1r[FC1]                                                     | 17.12.1r                |
| 26.1.2  | 17.8.1r[FC1]                                                     | 17.12.1r                |
| 26.1.1  | 17.8.1r[FC1]                                                     | 17.12.1r                |

## 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. For Cisco Catalyst 9500X Series Switches, enter the **show firmware version all** command in privileged EXEC mode.



### Note

- 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.

## Upgrading and Downgrading the Switch Software

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

### Upgrading in Install Mode

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

| When upgrading from ...                            | Use these commands...                | To upgrade to...    |
|----------------------------------------------------|--------------------------------------|---------------------|
| Cisco IOS XE Everest 16.6.2 and all later releases | Only install commands <sup>3</sup> . | Cisco IOS XE 26.2.x |

<sup>3</sup> Introduced in Cisco IOS XE Fuji 16.8.1a.

This procedure shows the steps to upgrade the Cisco IOS XE software on a switch, from Cisco IOS XE 17.18.1 to Cisco IOS XE 26.2.1 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 sftp:[[/location]/directory]/filename flash:**

Use this command to copy the new image from a SFTP 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 SFTP 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** or **show boot**

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.

We recommend that you point to the source image on your SFTP 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.26.02.01.SPA.bin activate commit.`



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

**Note**

**Step 5** Verify installation

After the software has been successfully installed, use the **dir flash:** command to verify that the flash partition has ten new .pkg files and two .conf files.

a) **dir flash:\*.pkg**

b) **dir flash:\*.conf**

**Step 6** **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 Mar 19 19:51:48 UTC 2026

Cleaning up unnecessary package files

Scanning boot directory for packages ... done.

Preparing packages list to delete ...

cat9k-cc\_srdriver.17.18.01.SPA.pkg

File is in use, will not delete.

cat9k-espbases.17.18.01.SPA.pkg

File is in use, will not delete.

cat9k-guestshell.17.18.01.SPA.pkg

File is in use, will not delete.

cat9k-rpbase.17.18.01.SPA.pkg

File is in use, will not delete.

cat9k-rpboot.17.18.01.SPA.pkg

File is in use, will not delete.

cat9k-sipbase.17.18.01.SPA.pkg

File is in use, will not delete.

cat9k-sipspa.17.18.01.SPA.pkg

File is in use, will not delete.

cat9k-srdriver.17.18.01.SPA.pkg

File is in use, will not delete.

cat9k-webui.17.18.01.SPA.pkg

File is in use, will not delete.

cat9k-wlc.17.18.01.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.17.18.01.SPA.pkg

/flash/cat9k-espbases.17.18.01.SPA.pkg

/flash/cat9k-guestshell.17.18.01.SPA.pkg

/flash/cat9k-rpbase.17.18.01.SPA.pkg

/flash/cat9k-rpboot.17.18.01.SPA.pkg

/flash/cat9k-sipbase.17.18.01.SPA.pkg

/flash/cat9k-sipspa.17.18.01.SPA.pkg

/flash/cat9k-srdriver.17.18.01.SPA.pkg

/flash/cat9k-webui.17.18.01.SPA.pkg

/flash/cat9k-wlc.17.18.01.SPA.pkg

/flash/packages.conf

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

[R0]:

Deleting file flash:cat9k-cc\_srdriver.17.18.01.SPA.pkg ... done.

Deleting file flash:cat9k-espbases.17.18.01.SPA.pkg ... done.

Deleting file flash:cat9k-guestshell.17.18.01.SPA.pkg ... done.

Deleting file flash:cat9k-rpbase.17.18.01.SPA.pkg ... done.

Deleting file flash:cat9k-rpboot.17.18.01.SPA.pkg ... done.

Deleting file flash:cat9k-sipbase.17.18.01.SPA.pkg ... done.

Deleting file flash:cat9k-sipspa.17.18.01.SPA.pkg ... done.

Deleting file flash:cat9k-srdriver.17.18.01.SPA.pkg ... done.

Deleting file flash:cat9k-webui.17.18.01.SPA.pkg ... done.

Deleting file flash:cat9k-wlc.17.18.01.SPA.pkg ... done.

Deleting file flash:packages.conf ... done.

SUCCESS: Files deleted.

--- Starting Post\_Remove\_Cleanup ---

Performing Post\_Remove\_Cleanup on all members

[1] Post\_Remove\_Cleanup package(s) on switch 1

[1] Finished Post\_Remove\_Cleanup on switch 1

Checking status of Post\_Remove\_Cleanup on [1]

Post\_Remove\_Cleanup: Passed on [1]

Finished Post\_Remove\_Cleanup

```

SUCCESS: install_remove Thu Mar 19 19:52:25 UTC 2026
Switch#

Switch# copy sftp://10.8.0.6/image/cat9k_iosxe.26.02.01.SPA.bin flash:
destination filename [cat9k_iosxe.26.02.01.SPA.bin]?
Accessing sftp://10.8.0.6/image/cat9k_iosxe.26.02.01.SPA.bin...
Loading /cat9k_iosxe.26.02.01.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 Mar 19 2026 10:18:11 -07:00 cat9k_iosxe.26.02.01.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 <<on the C9500-24Y4C,C9500-32C, C9500-32QC, and C9500-48Y4C models
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 26.2.1 software image in the flash memory:

```

Switch# install add file flash:cat9k_iosxe.26.02.01.SPA.bin activate commit
install_add_activate_commit: Adding PACKAGE
install_add_activate_commit: Checking whether new add is allowed
--- Starting Add ---
Performing Add on Active/Standby
 [1] Add package(s) on R0
 [1] Finished Add on R0

Checking status of Add on [R0]
Add: Passed on [R0]
Finished Add

Image added. Version: 26.02.01

install_add_activate_commit: Activating PACKAGE
Following packages shall be activated:
/flash/cat9k-wlc.26.02.01.SPA.pkg
/flash/cat9k-webui.26.02.01.SPA.pkg
/flash/cat9k-srdriver.26.02.01.SPA.pkg
/flash/cat9k-sipsa.26.02.01.SPA.pkg

```

```
/flash/cat9k-sipbase.26.02.01.SPA.pkg
/flash/cat9k-rpboot.26.02.01.SPA.pkg
/flash/cat9k-rpbase.26.02.01.SPA.pkg
/flash/cat9k-guestshell.26.02.01.SPA.pkg
/flash/cat9k-espbases.26.02.01.SPA.pkg
/flash/cat9k-cc_srdriver.26.02.01.SPA.pkg
```

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

--- Starting Activate ---

Performing Activate on Active/Standby

[1] Activate package(s) on R0

--- Starting list of software package changes ---

Old files list:

```
Removed cat9k-cc_srdriver.17.18.01.SPA.pkg
Removed cat9k-espbases.17.18.01.SPA.pkg
Removed cat9k-guestshell.17.18.01.SPA.pkg
Removed cat9k-rpbase.17.18.01.SPA.pkg
Removed cat9k-rpboot.17.18.01.SPA.pkg
Removed cat9k-sipbase.17.18.01.SPA.pkg
Removed cat9k-sipspace.17.18.01.SPA.pkg
Removed cat9k-srdriver.17.18.01.SPA.pkg
Removed cat9k-webui.17.18.01.SPA.pkg
Removed cat9k-wlc.17.18.01.SPA.pkg
```

New files list:

```
Added cat9k-cc_srdriver.26.02.01.SSA.pkg
Added cat9k-espbases.26.02.01.SSA.pkg
Added cat9k-guestshell.26.02.01.SSA.pkg
Added cat9k-lni.26.02.01.SSA.pkg
Added cat9k-rpbase.26.02.01.SSA.pkg
Added cat9k-rpboot.26.02.01.SSA.pkg
Added cat9k-sipbase.26.02.01.SSA.pkg
Added cat9k-sipspace.26.02.01.SSA.pkg
Added cat9k-srdriver.26.02.01.SSA.pkg
Added cat9k-webui.26.02.01.SSA.pkg
Added cat9k-wlc.26.02.01.SSA.pkg
```

Finished list of software package changes

[1] Finished Activate on R0

Checking status of Activate on [R0]

Activate: Passed on [R0]

Finished Activate

--- Starting Commit ---

Performing Commit on Active/Standby

[1] Commit package(s) on R0

[1] Finished Commit on R0

Checking status of Commit on [R0]

Commit: Passed on [R0]

Finished Commit

Send model notification for install\_add\_activate\_commit before reload

Install will reload the system now!

SUCCESS: install\_add\_activate\_commit Thu Mar 19 12:13:05 IST 2026

Switch#Mar 19 12:13:11.023: %PMANTACTION: F0/0vp: Process manager is exiting: n requested

Mar 19 12:13:11.028: %PMAN-5-EXITACTION: C1/0: pvp: Process manager is exiting: reload fru action requested

Mar 19 12:13:11.825: %PMAN-5-EXITACTION: R0/0: pvp: Process manager is exiting: reload action requested

Initializing Hardware...

System Bootstrap, Version 17.4.1r[FC2], RELEASE SOFTWARE (P)

Compiled 03-19-2026 12:00:00.00 by rel

Current ROMMON image : Primary Rommon Image

Last reset cause:LocalSoft

```
C9500-32QC platform with 16777216 Kbytes of main memory
Preparing to autoboot. [Press Ctrl-C to interrupt] 5 5 /-\\/-\\/-4 \\/-\\/-\\|3 /-\\/-\\/-2
\\/-\\/-\\|1 /-\\/-\\/-0
```

```
boot: attempting to boot from [bootflash:packages.conf]
```

```
boot: reading file packages.conf
<output truncated>
```

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

```
Switch# dir flash:*.pkg
```

```
Directory of flash:/
475140 -rw- 2012104 Jul 31 2025 09:52:41 -07:00 cat9k-cc_srdriver.17.18.01.SPA.pkg
475141 -rw- 70333380 Jul 31 2025 09:52:44 -07:00 cat9k-esppbase.17.18.01.SPA.pkg
475142 -rw- 13256 Jul 31 2025 09:52:44 -07:00 cat9k-guestshell.17.18.01.SPA.pkg
475143 -rw- 349635524 Jul 31 2025 09:52:54 -07:00 cat9k-rpbase.17.18.01.SPA.pkg
475149 -rw- 24248187 Jul 31 2025 09:53:02 -07:00 cat9k-rpboot.17.18.01.SPA.pkg
475144 -rw- 25285572 Jul 31 2025 09:52:55 -07:00 cat9k-sippbase.17.18.01.SPA.pkg
475145 -rw- 20947908 Jul 31 2025 09:52:55 -07:00 cat9k-sipspa.17.18.01.SPA.pkg
475146 -rw- 2962372 Jul 31 2025 09:52:56 -07:00 cat9k-srdriver.17.18.01.SPA.pkg
475147 -rw- 13284288 Jul 31 2025 09:52:56 -07:00 cat9k-webui.17.18.01.SPA.pkg
475148 -rw- 13248 Jul 31 2025 09:52:56 -07:00 cat9k-wlc.17.18.01.SPA.pkg

491524 -rw- 25711568 Mar 19 2026 11:49:33 -07:00 cat9k-cc_srdriver.26.02.01.SPA.pkg
491525 -rw- 78484428 Mar 19 2026 11:49:35 -07:00 cat9k-esppbase.26.02.01.SPA.pkg
491526 -rw- 1598412 Mar 19 2026 11:49:35 -07:00 cat9k-guestshell.26.02.01.SPA.pkg
491527 -rw- 404153288 Mar 19 2026 11:49:47 -07:00 cat9k-rpbase.26.02.01.SPA.pkg
491533 -rw- 31657374 Mar 19 2026 11:50:09 -07:00 cat9k-rpboot.26.02.01.SPA.pkg
491528 -rw- 27681740 Mar 19 2026 11:49:48 -07:00 cat9k-sippbase.26.02.01.SPA.pkg
491529 -rw- 52224968 Mar 19 2026 11:49:49 -07:00 cat9k-sipspa.26.02.01.SPA.pkg
491530 -rw- 31130572 Mar 19 2026 11:49:50 -07:00 cat9k-srdriver.26.02.01.SPA.pkg
491531 -rw- 14783432 Mar 19 2026 11:49:51 -07:00 cat9k-webui.26.02.01.SPA.pkg
491532 -rw- 9160 Mar 19 2026 11:49:51 -07:00 cat9k-wlc.26.02.01.SPA.pkg
11353194496 bytes total (9544245248 bytes free)
Switch#
```

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:

- packages.conf: the file that has been re-written with the newly installed .pkg files
- cat9k\_iosxe.26.02.01.SPA.conf: a backup copy of the newly installed packages.conf file

```
Switch# dir flash:*.conf
```

```
Directory of flash:/*.conf
Directory of flash:/
434197 -rw- 7406 Mar 19 2026 10:59:16 -07:00 packages.conf
516098 -rw- 7406 Mar 19 2026 10:58:08 -07:00 cat9k_iosxe.26.02.01.SPA.conf
11353194496 bytes total (8963174400 bytes free)
```

The following sample output of the **show version** command displays the Cisco IOS XE 26.2.1 image on the device:

```
Switch# show version
```

```
Cisco IOS XE Software, Version 26.02.01
Cisco IOS Software, Catalyst L3 Switch Software (CAT9K_IOSXE), Version 26.x, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2026 by Cisco Systems, Inc.
<output truncated>
```

## Downgrading in Install Mode

Follow these instructions to downgrade from one release to another, in install mode.

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

| When downgrading from ... | Use these commands...        | To downgrade to...                        |
|---------------------------|------------------------------|-------------------------------------------|
| Cisco IOS XE 26.2.x       | Only <b>install</b> commands | Cisco IOS XE 17.18.x or earlier releases. |

### 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 26.2.1 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 sftp:[[/location]/directory]/filename flash:**

Use this command to copy the new image from a SFTP 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 SFTP 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** or **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 SFTP 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.17.18.01.SPA.bin activate commit**.



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

**Note**

**Step 5**    Verify version  
**show version**

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



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

**Note**

**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 Mar 19 11:42:27 IST 2026

Cleaning up unnecessary package files

No path specified, will use booted path bootflash:packages.conf

Cleaning bootflash:
Scanning boot directory for packages ... done.
Preparing packages list to delete ...
cat9k-cc_srdriver.26.02.01.SSA.pkg
 File is in use, will not delete.
cat9k-espbases.26.02.01.SSA.pkg
 File is in use, will not delete.
cat9k-guestshell.26.02.01.SSA.pkg
 File is in use, will not delete.
cat9k-rpbases.26.02.01.SSA.pkg
 File is in use, will not delete.
cat9k-rpboot.26.02.01.SSA.pkg
 File is in use, will not delete.
cat9k-sipbase.26.02.01.SSA.pkg
 File is in use, will not delete.
cat9k-sipspa.26.02.01.SSA.pkg
 File is in use, will not delete.
cat9k-srdriver.26.02.01.SSA.pkg
 File is in use, will not delete.
cat9k-webui.26.02.01.SSA.pkg
 File is in use, will not delete.
cat9k-wlc.26.02.01.SSA.pkg
 File is in use, will not delete.
packages.conf
 File is in use, will not delete.
done.
SUCCESS: No extra package or provisioning files found on media. Nothing to clean.

SUCCESS: install_remove Thu Mar 19 11:42:39 IST 2026
```

```
Switch# copy sftp://10.8.0.6/image/cat9k_iosxe.17.18.01.SPA.bin flash:
Destination filename [cat9k_iosxe.17.18.01.SPA.bin]?
Accessing sftp://10.8.0.6//cat9k_iosxe.17.18.01.SPA.bin...
Loading /cat9k_iosxe.17.18.01.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 Mar 19 2026 13:35:16 -07:00 cat9k_iosxe.17.18.01.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 bootvar <<on the C9500-24Y4C,C9500-32C, C9500-32QC, and C9500-48Y4C models
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 example displays the installation of the Cisco IOS XE 17.18.1 software image to flash, by using the **install add file activate commit** command.

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

```
install_add_activate_commit: Adding PACKAGE
install_add_activate_commit: Checking whether new add is allowed
--- Starting Add ---
Performing Add on Active/Standby
[1] Add package(s) on R0
[1] Finished Add on R0
Checking status of Add on [R0]
Add: Passed on [R0]
Finished Add
Image added. Version: 17.18.01.0.269
install_add_activate_commit: Activating PACKAGE
```

```
Following packages shall be activated:
/flash/cat9k-wlc.17.18.01.SPA.pkg
/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-espbases.17.18.01.SPA.pkg
/flash/cat9k-cc_srdriver.17.18.01.SPA.pkg
```

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

Performing Activate on Active/Standby

1) Activate package(s) on R0

--- Starting list of software package changes ---

Old files list:

```
Removed cat9k-cc_srdriver.26.02.01.SSA.pkg
Removed cat9k-espbases.26.02.01.SSA.pkg
Removed cat9k-guestshell.26.02.01.SSA.pkg
Removed cat9k-lni.26.02.01.SSA.pkg
Removed cat9k-rpbase.26.02.01.SSA.pkg
Removed cat9k-rpboot.26.02.01.SSA.pkg
Removed cat9k-sipbase.26.02.01.SSA.pkg
Removed cat9k-sipspa.26.02.01.SSA.pkg
Removed cat9k-srdriver.26.02.01.SSA.pkg
Removed cat9k-webui.26.02.01.SSA.pkg
Removed cat9k-wlc.26.02.01.SSA.pkg
```

New files list:

```
Added cat9k-cc_srdriver.17.18.01.SPA.pkg
Added cat9k-espbases.17.18.01.SPA.pkg
Added cat9k-guestshell.17.18.01.SPA.pkg
Added cat9k-rpbase.17.18.01.SPA.pkg
Added cat9k-rpboot.17.18.01.SPA.pkg
Added cat9k-sipbase.17.18.01.SPA.pkg
Added cat9k-sipspa.17.18.01.SPA.pkg
Added cat9k-srdriver.17.18.01.SPA.pkg
Added cat9k-webui.17.18.01.SPA.pkg
Added cat9k-wlc.17.18.01.SPA.pkg
```

Finished list of software package changes

[1] Finished Activate on R0

Checking status of Activate on [R0]

Activate: Passed on [R0]

Finished Activate

--- Starting Commit ---

Performing Commit on Active/Standby

[1] Commit package(s) on R0

[1] Finished Commit on R0

Checking status of Commit on [R0]

Commit: Passed on [R0]

Finished Commit

Send model notification for install\_add\_activate\_commit before reload

Install will reload the system now!

SUCCESS: install\_add\_activate\_commit Thu Mar 19 11:51:01 IST 2026

Mar 19 11:51:07.505: %PMANTvp: Process manager is exiting: ren requested

Mar 19 11:51:07.505: %PMAN-5-EXITACTION: F0/0: pvp: Process manager is exiting: reload fru action requested

Mar 19 11:51:07.834: %PMAN-5-EXITACTION: R0/0: pvp: Process manager is exiting: reload action requested

Initializing Hardware...

System Bootstrap, Version 17.3.1r[FC2], RELEASE SOFTWARE (P)

Compiled 19-03-2026 12:00:00.00 by rel

Current ROMMON image : Primary Rommon Image

Last reset cause:LocalSoft

```
C9500-32QC platform with 16777216 Kbytes of main memory
Preparing to autoboot. [Press Ctrl-C to interrupt] 5 5 /-\\/-\\/-4 \\/-\\/-\\|3 /-\\/-\\/-2
\\/-\\/-\\|1 /-\\/-\\/-0
boot: attempting to boot from [bootflash:packages.conf]
boot: reading file packages.conf
```

<output truncated>

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 [Dublin], Catalyst L3 Switch Software (CAT9K_IOSXE), Version 17.18.1, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2026 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 Versions](#).

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. The manual upgrade applies to all models in the series. Enter the **upgrade rom-monitor capsule golden switch** command in privileged EXEC mode.



### Note

- In case of a Cisco StackWise Virtual setup, upgrade the active and standby switch.

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.

## 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.



---

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 the Cisco Catalyst 9500 Series Switches datasheet at:

<https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9500-series-switches/datasheet-c78-738978.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 9500 Series Switches, visit [Cisco Catalyst 9500 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 9200 Series Switches is at this URL: <https://www.cisco.com/c/en/us/products/switches/catalyst-9500-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 Marketplace](#).
- 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.