Revised: April 15, 2026

Release Notes for Cisco Catalyst 9600 Series Switches, Cisco IOS XE 26.1.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
April 10, 2026	26.1.1	• What's New: Software features • Caveats: Open and resolved caveats • Compatibility Matrix: Compatibility information for 26.1.1 • Software Images: Software images for 26.1.1 • ROMMON Versions: ROMMON versions for 26.1.1

Introduction

Cisco Catalyst 9600 Series Switches are the next generation purpose-built 40 GigabitEthernet, 50 GigabitEthernet, 100 GigabitEthernet, and 400 GigabitEthernet modular core and aggregation platform providing resiliency at scale with the industry's most comprehensive security while allowing your business to grow at the lowest total operational cost. They have been purpose-built to address emerging trends of Security, IoT, Mobility, and Cloud.

They deliver hardware and software convergence in terms of ASIC architecture with Unified Access Data Plane (UADP) 3.0 and Cisco Silicon One Q200. The platform runs an Open Cisco IOS XE that supports model driven programmability, Serial Advanced Technology Attachment (SATA) Solid State Drive (SSD) local storage, and a higher memory footprint). The series forms the foundational building block for SD-Access, which is Cisco's lead enterprise architecture.

It also supports features that provide high availability, advanced routing and infrastructure services, security capabilities, and application visibility and control.

Supported Cisco Catalyst 9600 Series Switches Model Numbers

The following table lists the supported switch models.

Switch Model (append with “=” for spares)	Description	Introductory Release
C9606R	Cisco Catalyst 9606R Switch • Redundant supervisor module capability • Four linecard slots • Hot-swappable fan tray, front and rear serviceable, fan tray assembly with 9 fans. • Four power supply module slots	Cisco IOS XE Gibraltar 16.11.1

Supported Hardware on Cisco Catalyst 9600 Series Switches

Product ID (append with “=” for spares)	Description	Introductory Release
Supervisor Modules		
C9600-SUP-1	Cisco Catalyst 9600 Series Supervisor 1 Module This supervisor module is supported on the C9606R chassis.	Cisco IOS XE Gibraltar 16.11.1
C9600X-SUP-2	Cisco Catalyst 9600 Series Supervisor Engine 2 This supervisor module is supported on the C9606R chassis.	Cisco IOS XE Cupertino 17.7.1
SATA[1] SSD[2] Modules (for the Supervisor)		
C9K-F2-SSD-240GB	Cisco Catalyst 9600 Series 240GB SSD Storage	Cisco IOS XE Gibraltar 16.11.1
C9K-F2-SSD-480GB	Cisco Catalyst 9600 Series 480GB SSD Storage	Cisco IOS XE Gibraltar 16.11.1
C9K-F2-SSD-960GB	Cisco Catalyst 9600 Series 960GB SSD Storage	Cisco IOS XE Gibraltar 16.11.1
Line Cards		

C9600X-LC-56YL4C	Cisco Catalyst 9600 Series 56-Port SFP56, 4-Port QSFP28 line card.
	• C9600X-SUP-2
	  • 56 SFP56 ports of 50G/25G/10G
	  • 4 QSFP28 ports of 100G/40G
	• C9600-SUP-1
	  • Not supported
		Cisco IOS XE 17.13.1

Product ID (append with “=” for spares)	Description	Introductory Release

C9600X-LC-32CD	Cisco Catalyst 9600 Series 30-Port QSFP28, 2-Port QSFP-DD line card.
	• C9600X-SUP-2
	  • 30 QSFP28 ports of 100G/40G
	  • 2 QSFP-DD ports of 400G/200G/100G/40G
	• C9600-SUP-1
	  • Not supported
		Cisco IOS XE Cupertino 17.9.1

C9600-LC-40YL4CD	Cisco Catalyst 9600 Series 40-Port SFP56, 2-Port QSFP56, 2-Port QSFP-DD line card.
	• C9600X-SUP-2
	  • 40 SFP56 ports of 50G/25G/10G
	  • 2 QSFP56 ports of 200G/100G/40G
	  • 2 QSFP-DD ports of 400G/200G/100G/40G
	• C9600X-SUP-1
	  • 40 SFP28 ports of 25G/10G/1G
	  • 2 QSFP28 ports of 100G/40G
		Cisco IOS XE Cupertino 17.7.1

C9600-LC-48YL	Cisco Catalyst 9600 Series 48-Port SFP56 line card.
	• C9600X-SUP-2
	  • 48 SFP56 ports of 50G/25G/10G
	• C9600X-SUP-1
	  • 48 SFP28 ports of 25G/10G/1G
		Cisco IOS XE Gibraltar 16.11.1

Product ID (append with “=” for spares)	Description	Introductory Release
C9600-LC-24C	Cisco Catalyst 9600 Series 24-Port 40G/12-Port 100G line card. • C9600X-SUP-2 • 24 QSFP28 ports of 100G/40G • C9600-SUP-1 • 12 ports of 100G or 24 ports of 40G	Cisco IOS XE Gibraltar 16.11.1
C9600-LC-48TX	Cisco Catalyst 9600 Series 48-Port MultiGigabit RJ45 line card. • C9600X-SUP-2 • 48 ports of 10G/5G/2.5G • C9600X-SUP-1 • 48 ports of 10G/5G/2.5G/1G and 100M/10M	Cisco IOS XE Amsterdam 17.1.1
C9600-LC-48S	Cisco Catalyst 9600 Series 48-Port SFP line card. • C9600X-SUP-2 • Not supported • C9600-SUP-1 • 48 SFP ports of 1G	Cisco IOS XE Amsterdam 17.2.1
AC Power Supply Modules		
C9600-PWR-2KWAC	Cisco Catalyst 9600 Series 2000W AC Power Supply Module[3]	Cisco IOS XE Gibraltar 16.11.1
C9600-PWR-3KWAC	Cisco Catalyst 9600 Series 3000W AC Power Supply Module	Cisco IOS XE Cupertino 17.8.1
DC Power Supply Modules		
C9600-PWR-2KWDC	Cisco Catalyst 9600 Series 2000W DC Power Supply Module	Cisco IOS XE Gibraltar 16.11.1

[1] Serial Advanced Technology Attachment (SATA)
[2] Solid State Drive (SSD) Module
[3] Power supply output capacity is 1050W at 110 VAC.

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 26.1.x

Hardware Features in Cisco IOS XE 26.1.1

Table 2: Hardware features introduced on Cisco Catalyst 9600 Series Switches

Feature Name	Description and Documentation Link
100GBASE QSFP-100G module	Supported transceiver module product numbers: • QSFP-100G-PSM4-S operating in 4x25G breakout mode Compatible line cards: • C9600-LC-24C line card on Cisco Catalyst 9600 Supervisor Module 1 (C9600-SUP-1) • C9600-LC-24C line card on Cisco Catalyst 9600 Supervisor 2 Module (C9600X-SUP-2) 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 26.1.1

Feature Name	Applicable Models	Description
Clear specific IP translation	All Models	Introduces the ability to selectively remove individual IP translation entries from the NAT translation table. By allowing administrators to clear specific translations rather than the entire table, this functionality reduces network disruption during troubleshooting and provides more precise control over active session management.
CTS policy server list enablement over RADIUS for IPv6	All Models	Network devices can now receive and utilize a list of IPv6-capable policy servers for security group access control list (SGACL) policy downloads, as part of downloading the TrustSec environment data from the ISE server over RADIUS protocol. This enablement ensures that even if the primary connection to ISE changes, the device can continue to fetch security policies using the most appropriate available address type. Prior to this release, server lists of only IPv4 address types were downloaded as part of the environment data.

Feature Name	Applicable Models	Description
Default Recursive next-hop support	All Models	Enhances Policy-Based Routing (PBR) by allowing the configuration of a next-hop that is not directly connected to the device. By enabling recursive lookup, the device can resolve the path to the specified next-hop through the routing table, providing greater flexibility in traffic steering and reducing the requirement for strict, direct-link connectivity in complex network topologies.
Dynamic protocol switching for communication between network devices and policy servers	All Models	Network devices can now switch the transport protocols and seamlessly download the security group access control list (SGACL) policies from the policy server (ISE), without any policy persistence or data traffic issues. This feature introduces the capability to dynamically switch between RADIUS and HTTPS protocols for communication between the policy server and the network device.
High Availability for Security Exchange Protocol	All Models	Introduces the high availability support for the stateful synchronization of IP-Security Group Tag (SGT) bindings in a Security Exchange Protocol (SXP) database between active and standby devices.
PAC download over IPv6	All Models	You can now enable IPv6 for PAC downloads that allows network devices to authenticate and receive credentials from a policy server, such as Identity Services Engine (ISE), using IPv6 addresses. This feature ensures that the TrustSec policy plane can operate in environments where IPv4 is restricted or unavailable.
Programmability: • Service-level ACL support for gNXI services • YANG Data Models	All Models	The following programmability features are introduced in this release: • gRPC Network Management/Operations Interface (gNXI) uses access control lists (ACLs) to restrict clients from using gNMI and gNOI services. ACLs provide a mechanism to define the access rights of clients to a service, and these restrictions are applied at the service-level so that all inbound connections are validated. • 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/2611.
PTP TTL modification	C9600X-SUP-2	Enables the modification of the Time-to-Live (TTL) value in Precision Time Protocol (PTP) packets, allowing them to traverse Layer 3 boundaries and bypass non-PTP-capable devices.

Feature Name	Applicable Models	Description
Resilient Infrastructure	All Models	As part of the ongoing commitment to network security, this release introduces secure alternatives to legacy commands. These updates are designed to mitigate potential risks and assist in establishing a more robust and secure operational baseline. The identified insecure commands are categorized as: • Line transport: Updates to secure remote access methods. • Device server configuration: Hardening of server-side settings. • File transfer protocols: Transitioning to encrypted transfer methods. • SNMP: Enhancements to secure management traffic. • Passwords: Strengthening authentication and credential management. • Miscellaneous: General security improvements for various system functions. The **show system insecure configuration** command introduced in Cisco IOS XE 17.18.2 release lists all insecure commands configured on the device. For all detected insecure configurations during device boot or upgrade, error messages are displayed. In Cisco IOS XE 26.1.1 release, all insecure CLI commands are blocked by default to strengthen your network infrastructure. If your environment requires the use of a legacy command, you must enable the **system mode insecure** command in global configuration mode. • Recommendation: Do not use insecure mode. This mode is temporary and will be removed in a future release. Identify and replace all insecure commands with their secure alternatives. • Upgrade behavior: If you upgrade to Cisco IOS XE 26.1.1 release with insecure commands already present in the running configuration, the **system mode insecure** command is automatically added to your configuration to prevent service disruption. For more information, refer this document Cisco C9000 Switching IOS XE – Resilient Infrastructure Playbook.
Security Service Insertion	C9600	Provides high availability for traffic steering and security service insertion by synchronizing steering policies between active and standby nodes. During a failover event, the standby node assumes the active role while maintaining existing traffic redirection policies, ensuring continuous operation and preventing traffic from bypassing security functions. This capability supports Stateful Switchover (SSO) and In-Service Software upgrade/downgrade to maintain network uptime and fault tolerance.

Feature Name	Applicable Models	Description
SGT Exchange Protocol over IPv6	All Models	SXP propagates the Security Group Tags (SGTs) across network devices that do not have hardware support for Cisco TrustSec. We now facilitate the propagation of SGTs in an IPv6 infrastructure. This feature allows network devices to exchange SGT-to-IP mappings over an IPv6 transport layer, ensuring that identity-based policies are maintained across modern network deployments.

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

Hardware and Software Behavior Changes in Cisco IOS XE 26.1.1

Behavior Change	Description
ASIC drop counters	On Cisco Catalyst 9600 Series Supervisor 2 Module, ASIC drop counters are displayed after Embedded Packet Capture (EPC) stops.
Expanded UDLD port template options	The UDLD port template configuration has been expanded to support additional modes. In addition to *udld port alert*, users can now configure *udld port aggressive*, *udld port aggress-alert*, or *udld port enable* within a template, providing greater flexibility in interface management.
IGMP and MLD snooping for EVPN	IGMP snooping and MLD snooping cannot be disabled for EVPN enabled VLANs if the **multicast advertise** command is enabled or PIM is enabled on the SVI.

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 26.1.x

There are no open caveats in this release.

Resolved Caveats in Cisco IOS XE 26.1.1

There are no resolved caveats in this release.

Feature Support

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

DF Bit Behavior for RADIUS Packets

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).

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 9600 Series Supervisor 1 and 2 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 9600 Series Supervisor Module PIDs, see Supported Cisco Catalyst 9600 Series Switches Model Numbers, on page 1.

BGP EVPN VXLAN

Feature	Not Supported On These Variants
Layer 2 Broadcast, Unknown Unicast, and Multicast (BUM) Traffic Forwarding using Ingress Replication	C9600X-SUP-2
BUM Traffic Rate Limiting	C9600X-SUP-2
Dynamic ARP inspection (DAI) and DHCP Rogue Server Protection	C9600X-SUP-2
EVPN VXLAN Centralized Default Gateway	C9600X-SUP-2
VXLAN-Aware Flexible Netflow	C9600X-SUP-2
MPLS Layer 3 VPN Border Leaf Handoff	C9600X-SUP-2
MPLS Layer 3 VPN Border Spine Handoff	C9600X-SUP-2
VPLS over MPLS Border Leaf Handoff	C9600X-SUP-2
VPLS over MPLS Border Spine Handoff	C9600X-SUP-2
Interworking of Layer 3 TRM with MVPN Networks for IPv4 Traffic	C9600X-SUP-2
Private VLANs (PVLANs)	C9600X-SUP-2
BGP EVPN VXLAN with IPv6 in the Underlay (VXLANv6)	C9600X-SUP-2
EVPN Microsegmentation	C9600X-SUP-2
VRF aware NAT64 EVPN Fabric	C9600X-SUP-2
EVPN VXLAN Multi-Homing	C9600X-SUP-2

Cisco TrustSec

Feature	Not Supported On These Variants
Cisco TrustSec Security Association Protocol (SAP)	C9600X-SUP-2

Feature	Not Supported On These Variants
Cisco TrustSec SGT Caching	C9600X-SUP-2

High Availability

Feature	Not Supported On These Variants
Secure StackWise Virtual	C9600X-SUP-2

Interface and Hardware

Feature	Not Supported On These Variants
EnergyWise	C9600X-SUP-2

IP Addressing Services

Feature	Not Supported On These Variants
Next Hop Resolution Protocol (NHRP)	C9600X-SUP-2
Network Address Translation (NAT)	C9600X-SUP-2
Gateway Load Balancing Protocol (GLBP)	C9600X-SUP-2
Web Cache Communication Protocol (WCCP)	C9600X-SUP-2
Switchport Block Unknown Unicast and Switchport Block Unknown Multicast	C9600X-SUP-2
Message Session Relay Protocol (MSRP)	C9600X-SUP-2
TCP MSS Adjustment	C9600X-SUP-2

IP Multicast Routing

Feature	Not Supported On These Variants
Multicast Routing over GRE Tunnel	C9600X-SUP-2
Multicast VLAN Registration (MVR) for IGMP Snooping	C9600X-SUP-2
IPv6 Multicast over Point-to-Point GRE	C9600X-SUP-2
IGMP Proxy	C9600X-SUP-2
Bidirectional PIM	C9600X-SUP-2
mVPN Extranet Support	C9600X-SUP-2
MLDP-Based VPN	C9600X-SUP-2

Feature	Not Supported On These Variants
PIM Snooping	C9600X-SUP-2
PIM Dense Mode	C9600X-SUP-2

IP Routing

Feature	Not Supported On These Variants
OSPFv2 Loop-Free Alternate IP Fast Reroute	C9600X-SUP-2
EIGRP Loop-Free Alternate IP Fast Reroute	C9600X-SUP-2
PBR for Object-Group Access Control List (OGACL) Based Matching	C9600X-SUP-2
Multipoint GRE	C9600X-SUP-2
Unicast and Multicast over Point-to-Multipoint GRE	C9600X-SUP-2
GRE IPv6 Tunnels	C9600X-SUP-2
IP Fast Reroute (IP FRR)	C9600X-SUP-2
Non-stop Routing	C9600X-SUP-2

Layer 2

Feature	Not Supported On These Variants
Loop Detection Guard	C9600X-SUP-2
Multi-VLAN Registration Protocol (MVRP)	C9600X-SUP-2
Precision Time Protocol (PTP)	C9600X-SUP-2
Resilient Ethernet Protocol	All

Multiprotocol Label Switching

Feature	Not Supported On These Variants
LAN MACsec over Multiprotocol Label Switching (MPLS)	C9600X-SUP-2
BGP Multipath Load Sharing for Both eBGP and iBGP in an MPLS VPN	C9600X-SUP-2
MPLS over GRE	C9600X-SUP-2
MPLS Layer 2 VPN over GRE	C9600X-SUP-2
MPLS Layer 3 VPN over GRE	C9600X-SUP-2

Feature	Not Supported On These Variants
Virtual Private LAN Service (VPLS)	C9600X-SUP-2
VPLS Autodiscovery, BGP-based	C9600X-SUP-2
VPLS Layer 2 Snooping: Internet Group Management Protocol or Multicast Listener Discovery	C9600X-SUP-2
Hierarchical VPLS with MPLS Access	C9600X-SUP-2
VPLS Routed Pseudowire IRB(v4) Unicast	C9600X-SUP-2
MPLS VPN Inter-AS Options (options B and AB)	C9600X-SUP-2
MPLS VPN Inter-AS IPv4 BGP Label Distribution	C9600X-SUP-2
Seamless Multiprotocol Label Switching	C9600X-SUP-2

Network Management

Feature	Not Supported On These Variants
Flow-Based Switch Port Analyser	C9600X-SUP-2
RSPAN	C9600X-SUP-2
FRSPAN	C9600X-SUP-2
Egress Netflow	C9600X-SUP-2
IP Aware MPLS Netflow	C9600X-SUP-2
NetFlow Version 5	C9600X-SUP-2
Cisco Application Visibility and Control (AVC)	All

Quality of Service

Feature	Not Supported On These Variants
QoS Ingress Shaping	C9600X-SUP-2
VPLS QoS	C9600X-SUP-2
Microflow Policers	C9600X-SUP-2
Per VLAN Policy and Per Port Policer	C9600X-SUP-2
Mixed COS/DSCP Threshold in a QoS LAN-queueing Policy	C9600X-SUP-2
Easy QoS: match-all Attributes	C9600X-SUP-2
Classify: Packet Length	C9600X-SUP-2

Feature	Not Supported On These Variants
Class-Based Shaping for DSCP/Prec/COS/MPLS Labels	C9600X-SUP-2
CoPP Microflow Policing	C9600X-SUP-2
Egress Policing	C9600X-SUP-2
Egress Microflow Destination-Only Policing	C9600X-SUP-2
Ethertype Classification	C9600X-SUP-2
Packet Classification Based on Layer3 Packet-Length	C9600X-SUP-2
PACLs	C9600X-SUP-2
Per IP Session QoS	C9600X-SUP-2
Per Queue Policer	C9600X-SUP-2
QoS Data Export	C9600X-SUP-2
QoS L2 Missed Packets Policing	C9600X-SUP-2

Security

Feature	Not Supported On These Variants
Lawful Intercept	C9600X-SUP-2
MACsec: • MACsec EAP-TLS • Switch-to-host MACsec • Certificate-based MACsec • Cisco TrustSec SAP MACsec	C9600X-SUP-2
MAC ACLs	C9600X-SUP-2
Port ACLs	C9600X-SUP-2
VLAN ACLs	C9600X-SUP-2
IP Source Guard	C9600X-SUP-2
IPv6 Source Guard	C9600X-SUP-2
Web-based Authentication	C9600X-SUP-2
Port Security	C9600X-SUP-2
Weighted Random Early Detection mechanism (WRED) Based on DSCP, PREC, or COS	C9600X-SUP-2

Feature	Not Supported On These Variants
IEEE 802.1x Port-Based Authentication	C9600X-SUP-2
Dynamic ARP Inspection	C9600X-SUP-2
Dynamic ARP Inspection Snooping	C9600X-SUP-2

System Management

Feature	Not Supported On These Variants
Unicast MAC Address Filtering	C9600X-SUP-2

VLAN

Feature	Not Supported On These Variants
Wired Dynamic PVLAN	C9600X-SUP-2
Private VLANs	C9600X-SUP-2

Limitations and Restrictions

- Auto negotiation: The SFP+ interface (TenGigabitEthernet0/1) on the Ethernet management port with a 1G transceiver does not support auto negotiation.
- 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.
- Convergence: During SSO, a higher convergence time is observed while removing the active supervisor module installed in slot 3 of a C9606R chassis.
- Hardware Limitations: Optics:
  - Installation restriction for C9600-LC-24C linecard with CVR-QSFP-SFP10G adapter: This adapter must not be installed on an even numbered port where the corresponding odd numbered port is configured as 40GE port. For example, if port 1 is configured as 40GE, CVR-QSFP-SFP10G must not be installed in port 2.

    Installation restriction for C9600-LC-24C linecard with CVR-QSFP-SFP10G adapter: If you insert a 40-Gigabit Ethernet Transceiver Module to odd numbered port, the corresponding even numbered port does not work with CVR-QSFP-SFP10G adapter.
  - GLC-T and GLC-TE operating at 10/100Mbps speed are not supported with Cisco QSA Module (CVR-QSFP-SFP10G).
  - 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: Power Supply Modules:
  - Input voltage for AC power supply modules: All AC-input power supply modules in the chassis must have the same AC-input voltage level.

- Using power supply modules of different types: When mixing AC-input and DC-input power supplies, the AC-input voltage level must be 220 VAC.

- 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, 26.1.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.
  - 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
  - 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
  ```

- 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.

- On the Cisco Catalyst 9600 Series Supervisor 2 Module, 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 Gibraltar 16.11.1 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 9600 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.

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 26.1.1	CAT9K_IOSXE	cat9k_iosxe.26.01.01.SPA.bin
	No Payload Encryption (NPE)	cat9k_iosxe_npe.26.01.01.SPA.bin

To download software images, visit the software downloads page: Cisco Catalyst 9600 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 9600 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 16.x.x releases, refer to the corresponding Cisco IOS XE 16.x.x release notes of the respective platform.

Release	ROMMON Version (C9600-SUP-1)	ROMMON Version (C9600X-SUP-2)
26.1.1	17.8.1r[FC1]	17.10.1r
17.18.3	17.8.1r[FC1]	17.10.1r
17.18.2	17.8.1r[FC1]	17.10.1r
17.18.1	17.8.1r[FC1]	17.10.1r
17.17.1	17.8.1r[FC1]	17.10.1r
17.16.1	17.8.1r[FC1]	17.10.1r
17.15.5	17.8.1r[FC1]	17.10.1r

Release	ROMMON Version (C9600-SUP-1)	ROMMON Version (C9600X-SUP-2)
17.15.4d	17.8.1r[FC1]	17.10.1r
17.15.4b	17.8.1r[FC1]	17.10.1r
17.15.4	17.8.1r[FC1]	17.10.1r
17.15.3	17.8.1r[FC1]	17.10.1r
17.15.2	17.8.1r[FC1]	17.10.1r
17.15.1	17.8.1r[FC1]	17.10.1r
17.14.1	17.8.1r[FC1]	17.10.1r
17.13.1	17.8.1r[FC1]	17.10.1r
Dublin 17.12.4	17.8.1r[FC1]	17.10.1r
Dublin 17.12.3	17.8.1r[FC1]	17.10.1r
Dublin 17.12.2	17.8.1r[FC1]	17.10.1r
Dublin 17.12.1	17.8.1r[FC1]	17.10.1r
Dublin 17.11.1	17.8.1r[FC1]	17.10.1r
Dublin 17.10.1	17.8.1r[FC1]	17.10.1r
Cupertino 17.9.5	17.8.1r[FC1]	17.7.1r[FC3]
Cupertino 17.9.4	17.8.1r[FC1]	17.7.1r[FC3]
Cupertino 17.9.3	17.8.1r[FC1]	17.7.1r[FC3]
Cupertino 17.9.2	17.8.1r[FC1]	17.7.1r[FC3]
Cupertino 17.9.1	17.8.1r[FC1]	17.7.1r[FC3]
Cupertino 17.8.1	17.8.1r[FC1]	17.7.1r[FC3]
Cupertino 17.7.1	17.6.1r	17.7.1r[FC3]
Bengaluru 17.6.7	17.6.1r	-
Bengaluru 17.6.6a	17.6.1r	-
Bengaluru 17.6.6	17.6.1r	-
Bengaluru 17.6.5	17.6.1r	-
Bengaluru 17.6.4	17.6.1r	-
Bengaluru 17.6.3	17.6.1r	-
Bengaluru 17.6.2	17.6.1r	-

Release	ROMMON Version (C9600-SUP-1)	ROMMON Version (C9600X-SUP-2)
Bengaluru 17.6.1	17.6.1r	-
Bengaluru 17.5.1	17.3.1r[FC2]	-
Bengaluru 17.4.1	17.3.1r[FC2]	-
Amsterdam 17.3.8a	17.3.1r[FC2]	-
Amsterdam 17.3.8	17.3.1r[FC2]	-
Amsterdam 17.3.7	17.3.1r[FC2]	-
Amsterdam 17.3.6	17.3.1r[FC2]	-
Amsterdam 17.3.5	17.3.1r[FC2]	-
Amsterdam 17.3.4	17.3.1r[FC2]	-
Amsterdam 17.3.3	17.3.1r[FC2]	-
Amsterdam 17.3.2a	17.3.1r[FC2]	-
Amsterdam 17.3.1	17.3.1r[FC2]	-
Amsterdam 17.2.1	17.1.1[FC2]	-
Amsterdam 17.1.1	17.1.1[FC1]	-

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 **show firmware version all** command in privileged EXEC mode or the **version -v** command in ROMMON 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**.

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 that you can use this procedure for the following upgrade scenarios:

When upgrading from ...	To...
Cisco IOS XE 17.18.x or earlier releases	Cisco IOS XE 26.1.x

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 26.1.1 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:*.bin**

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.

We recommend that you point to the source image on a SFTP server or the flash , if you have copied the image to flash memory.

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

Step 6 Verify version

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-espbase.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:
[switch 1]:
/flash/cat9k-cc_srdriver.17.18.01.SPA.pkg
```

```
/flash/cat9k-espbase.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]y

[switch 1]:
Deleting file flash:cat9k-cc_srdriver.17.18.01.SPA.pkg ... done.
Deleting file flash:cat9k-espbase.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.26.01.01.SPA.bin flash:

destination filename [cat9k_iosxe.26.01.01.SPA.bin]?
Accessing sftp://10.8.0.6/image/cat9k_iosxe.26.01.01.SPA.bin...
Loading /cat9k_iosxe.26.01.01.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.26.01.01.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 26.1.1 software image to flash:

```
Switch# install add file flash:cat9k_iosxe.26.01.01.SPA.bin activate commit
_install_add_activate_commit: START Thu Mar 19 16:37:25 IST 2026

*Mar 19 16:37:26.544 IST: %INSTALL-5-INSTALL_START_INFO: R0/0: install_engine: Started install one-shot
flash:cat9k_iosxe.26.01.01.SPA.bin
install_add_activate_commit: Adding PACKAGE
install_add_activate_commit: Checking whether new add is allowed ....

This operation requires a reload of the system. Do you want to proceed?
Please confirm you have changed boot config to flash:packages.conf [y/n]y

--- Starting initial file syncing ---
Copying image file: flash:cat9k_iosxe.26.01.01.SPA.bin to standby
Info: Finished copying flash:cat9k_iosxe.26.01.01.SPA.bin to standby
Finished initial file syncing

--- Starting Add ---
Performing Add on Active/Standby
  [R0] Add package(s) on R0
  [R0] Finished Add on R0
  [R1] Add package(s) on R1
  [R1] Finished Add on R1
Checking status of Add on [R0 R1]
Add: Passed on [R0 R1]
Finished Add

Image added. Version: 26.01.01

install_add_activate_commit: Activating PACKAGE
Following packages shall be activated:
/flash/cat9k-wlc.26.01.01.SPA.pkg
/flash/cat9k-webui.26.01.01.SPA.pkg
/flash/cat9k-srdriver.26.01.01.SPA.pkg
/flash/cat9k-sipspa.26.01.01.SPA.pkg
/flash/cat9k-sipbase.26.01.01.SPA.pkg
/flash/cat9k-rpboot.26.01.01.SPA.pkg
/flash/cat9k-rpbase.26.01.01.SPA.pkg
/flash/cat9k-guestshell.26.01.01.SPA.pkg
/flash/cat9k-espbase.26.01.01.SPA.pkg
/flash/cat9k-cc_srdriver.26.01.01.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
```

```
*Mar 19 16:45:21.695 IST: %INSTALL-5-INSTALL_AUTO_ABORT_TIMER_PROGRESS: R0/0: rollback_timer: Install auto
abort timer will expire in 7200 seconds  [R0] Activate package(s) on R0
  [R0] Finished Activate on R0
  [R1] Activate package(s) on R1
  [R1] Finished Activate on R1
Checking status of Activate on [R0 R1]
Activate: Passed on [R0 R1]
Finished Activate

*Mar 19 16:45:25.233 IST: %INSTALL-5-INSTALL_AUTO_ABORT_TIMER_PROGRESS: R1/0: rollback_timer: Install auto
abort timer will expire in 7200 seconds--- Starting Commit ---
Performing Commit on Active/Standby
  [R0] Commit package(s) on R0
  [R0] Finished Commit on R0
  [R1] Commit package(s) on R1
  [R1] Finished Commit on R1
Checking status of Commit on [R0 R1]
Commit: Passed on [R0 R1]
Finished Commit

Install will reload the system now!
SUCCESS: install_add_activate_commit  Thu Mar 19 16:46:18 IST 2026
```

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    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-espbase.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-sipbase.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.26.01.01.SPA.pkg
491525 -rw- 78484428   Mar 19 2026 11:49:35 -07:00  cat9k-espbase.26.01.01.SPA.pkg
491526 -rw- 1598412    Mar 19 2026 11:49:35 -07:00  cat9k-guestshell.26.01.01.SPA.pkg
491527 -rw- 404153288  Mar 19 2026 11:49:47 -07:00  cat9k-rpbase.26.01.01.SPA.pkg
491533 -rw- 31657374   Mar 19 2026 11:50:09 -07:00  cat9k-rpboot.26.01.01.SPA.pkg
491528 -rw- 27681740   Mar 19 2026 11:49:48 -07:00  cat9k-sipbase.26.01.01.SPA.pkg
491529 -rw- 52224968   Mar 19 2026 11:49:49 -07:00  cat9k-sipspa.26.01.01.SPA.pkg
491530 -rw- 31130572   Mar 19 2026 11:49:50 -07:00  cat9k-srdriver.26.01.01.SPA.pkg
491531 -rw- 14783432   Mar 19 2026 11:49:51 -07:00  cat9k-webui.26.01.01.SPA.pkg
491532 -rw- 9160       Mar 19 2026 11:49:51 -07:00  cat9k-wlc.26.01.01.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:

- `packages.conf`: the file that has been re-written with the newly installed .pkg files.
- `cat9k_iosxe.26.01.01.SPA.conf`: a backup copy of the newly installed packages.conf file.

```
Switch# dir flash:*.conf

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

```
16631  -rw- 4882 Mar 19 2026 05:39:42 +00:00  packages.conf
16634  -rw- 4882 Mar 19 2026 05:34:06 +00:00  cat9k_iosxe.26.01.01.SPA.conf
```

The following sample output of the **show version** command displays the Cisco IOS XE 26.1.1 image on the device:

```
Switch# show version

Cisco IOS XE Software, Version 26.01.01
Cisco IOS Software, Catalyst L3 Switch Software (CAT9K_IOSXE), Version 26.x, RELEASE SOFTWARE (fc1)
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. 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 ...	To ...
Cisco IOS XE 26.1.x	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 module is introduced is the minimum software version for that model. We recommend upgrading all existing hardware to the same release as the latest hardware.

This procedure shows the steps to downgrade the Cisco IOS XE software on a switch, from Cisco IOS XE 26.1.1 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**

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 a SFTP server or the flash , if you have copied the image to flash memory.

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 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.26.01.01.SSA.pkg
      File is in use, will not delete.
    cat9k-espbase.26.01.01.SSA.pkg
      File is in use, will not delete.
    cat9k-guestshell.26.01.01.SSA.pkg
      File is in use, will not delete.
    cat9k-rpbase.26.01.01.SSA.pkg
      File is in use, will not delete.
    cat9k-rpboot.26.01.01.SSA.pkg
      File is in use, will not delete.
    cat9k-sipbase.26.01.01.SSA.pkg
      File is in use, will not delete.
    cat9k-sipspa.26.01.01.SSA.pkg
      File is in use, will not delete.
    cat9k-srdriver.26.01.01.SSA.pkg
```

```
      File is in use, will not delete.
    cat9k-webui.26.01.01.SSA.pkg
      File is in use, will not delete.
    cat9k-wlc.26.01.01.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

--- 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.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
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: START Thu Mar 19 21:37:25 IST 2026

*Mar 19 16:37:26.544 IST: %INSTALL-5-INSTALL_START_INFO: R0/0: install_engine: Started install one-shot
flash:cat9k_iosxe.17.18.01.SPA.bin
install_add_activate_commit: Adding PACKAGE
install_add_activate_commit: Checking whether new add is allowed ....

This operation requires a reload of the system. Do you want to proceed?
Please confirm you have changed boot config to flash:packages.conf [y/n]y

--- Starting initial file syncing ---
Copying image file: flash:cat9k_iosxe.17.18.01.SPA.bin to standby
Info: Finished copying flash:cat9k_iosxe.17.18.01.SPA.bin to standby
Finished initial file syncing

--- Starting Add ---
Performing Add on Active/Standby
  [R0] Add package(s) on R0
  [R0] Finished Add on R0
  [R1] Add package(s) on R1
  [R1] Finished Add on R1
Checking status of Add on [R0 R1]
Add: Passed on [R0 R1]
Finished Add

Image added. Version: 17.18.1
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-espbase.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

--- Starting Activate ---
Performing Activate on Active/Standby

*Mar 19 21:45:21.695 IST: %INSTALL-5-INSTALL_AUTO_ABORT_TIMER_PROGRESS: R0/0: rollback_timer: Install auto
abort timer will expire in 7200 seconds  [R0] Activate package(s) on R0
  [R0] Finished Activate on R0
  [R1] Activate package(s) on R1
  [R1] Finished Activate on R1
Checking status of Activate on [R0 R1]
Activate: Passed on [R0 R1]
Finished Activate


*Mar 19 21:45:25.233 IST: %INSTALL-5-INSTALL_AUTO_ABORT_TIMER_PROGRESS: R1/0: rollback_timer: Install auto
abort timer will expire in 7200 seconds--- Starting Commit ---
Performing Commit on Active/Standby
  [R0] Commit package(s) on R0
  [R0] Finished Commit on R0
```

```
  [R1] Commit package(s) on R1
  [R1] Finished Commit on R1
Checking status of Commit on [R0 R1]
Commit: Passed on [R0 R1]
Finished Commit

Install will reload the system now!
SUCCESS: install_add_activate_commit  Thu Mar 19 21:46:18 IST 2026
```

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, on page 18.

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

  - 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.

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 the Cisco Catalyst 9600 Series Switches datasheets at:

https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9600-series-switches/nb-06-cat9600-series-data-sheet-cte-en.html

https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9600-series-switches/nb-06-cat9600-series-line-data-sheet-cte-en.html

https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9600-series-switches/nb-06-cat9600-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

This section provides information about hidden commands in Cisco IOS XE and the security measures that are in place, when they are accessed. These commands are only meant to assist Cisco TAC in advanced troubleshooting and are not documented.

Hidden commands are available under:

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

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

- The commands have CLI help. Enter enter a question mark (?) at the system prompt to display the list of available commands.

  Note: For Category 1, enter the **service internal** command before you enter the question mark; you do not have to do this for Category 2.

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

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

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

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

Important

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

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

Related Documentation

For 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 9600 Series Switches, visit Cisco Catalyst 9606R Switch.

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 9600 Series Switches is at this URL: https://www.cisco.com/c/en/us/products/switches/catalyst-9600-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.