Revised: August 8, 2025

Release Notes for Cisco Catalyst 9300 Series Switches, Cisco IOS XE 17.18.x

Document Change History

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

Table 1: Document Change History

Date	Release	Sections Updated
August 08, 2025	17.18.1	• What's New: Software features • Caveats: Open and Resolved Caveats • Compatibility Matrix: Compatibility information for 17.18.1 • Software Images: Software images for 17.18.1 • ROMMON Versions, on page 16: ROMMON Versions for 17.18.1

Introduction

Cisco Catalyst 9300 Series Switches are Cisco's lead stackable access platforms for the next-generation enterprise and have been purpose-built to address emerging trends of Security, IoT, Mobility, and Cloud.

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

Supported Cisco Catalyst 9300 Series Switches Model Numbers

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

Table 2: Cisco Catalyst 9300 Series Switches

Switch Model	Default License Level[1]	Description	Introductory Release
C9300-24H-A	Network Advantage	Stackable 24 10/100/1000 Mbps UPOE+ ports; PoE budget of 830 W with 1100 WAC power supply; supports StackWise-480 and StackPower	Cisco IOS XE Amsterdam 17.2.1
C9300-24H-E	Network Essentials		Cisco IOS XE Amsterdam 17.2.1

Switch Model	Default License Level[1]	Description	Introductory Release
C9300-24P-A	Network Advantage	Stackable 24 10/100/1000 PoE+ ports; PoE budget of 437W; 715 WAC power supply; supports StackWise-480 and StackPower	Cisco IOS XE Everest 16.5.1a
C9300-24P-E	Network Essentials		Cisco IOS XE Everest 16.5.1a
C9300-24S-A	Network Advantage	Stackable 24 1G SFP ports; two power supply slots with 715 WAC power supply installed by default; supports StackWise-480 and StackPower.	Cisco IOS XE Gibraltar 16.11.1
C9300-24S-E	Network Essentials		Cisco IOS XE Gibraltar 16.11.1
C9300-24T-A	Network Advantage	Stackable 24 10/100/1000 Ethernet ports; 350 WAC power supply; supports StackWise-480 and StackPower	Cisco IOS XE Everest 16.5.1a
C9300-24T-E	Network Essentials		Cisco IOS XE Everest 16.5.1a
C9300-24U-A	Network Advantage	Stackable 24 10/100/1000 UPoE ports; PoE budget of 830W; 1100 WAC power supply; supports StackWise-480 and StackPower	Cisco IOS XE Everest 16.5.1a
C9300-24U-E	Network Essentials		Cisco IOS XE Everest 16.5.1a
C9300-24UB-A	Network Advantage	Stackable 24 10/100/1000 Mbps UPOE ports that provide deep buffers and higher scale; PoE budget of 830W with 1100 WAC power supply; supports StackWise-480 and StackPower	Cisco IOS XE Gibraltar 16.12.1
C9300-24UB-E	Network Essentials		Cisco IOS XE Gibraltar 16.12.1
C9300-24UX-A	Network Advantage	Stackable 24 Multigigabit Ethernet 100/1000/2500/5000/10000 UPoE ports; PoE budget of 490 W with 1100 WAC power supply; supports StackWise-480 and StackPower	Cisco IOS XE Everest 16.6.1
C9300-24UX-E	Network Essentials		Cisco IOS XE Everest 16.6.1
C9300-24UXB-A	Network Advantage	Stackable 24 Multigigabit Ethernet (100 Mbps or 1/2.5/5/10 Gbps) UPOE ports that provide deep buffers and higher scale; PoE budget of 560 W with 1100 WAC power supply; supports StackWise-480 and StackPower	Cisco IOS XE Gibraltar 16.12.1
C9300-24UXB-E	Network Essentials		Cisco IOS XE Gibraltar 16.12.1
C9300-48H-A	Network Advantage	Stackable 48 10/100/1000 Mbps UPOE+ ports; PoE budget of 822 W with 1100 WAC power supply; supports StackWise-480 and StackPower	Cisco IOS XE Amsterdam 17.2.1
C9300-48H-E	Network Essentials		Cisco IOS XE Amsterdam 17.2.1

Switch Model	Default License Level[1]	Description	Introductory Release
C9300-48T-A	Network Advantage	Stackable 48 10/100/1000 Ethernet ports; 350 WAC power supply; supports StackWise-480 and StackPower	Cisco IOS XE Everest 16.5.1a
C9300-48T-E	Network Essentials		Cisco IOS XE Everest 16.5.1a
C9300-48P-A	Network Advantage	Stackable 48 10/100/1000 PoE+ ports; PoE budget of 437W; 715 WAC power supply; supports StackWise-480 and StackPower	Cisco IOS XE Everest 16.5.1a
C9300-48P-E	Network Essentials		Cisco IOS XE Everest 16.5.1a
C9300-48S-A	Network Advantage	Stackable 48 1G SFP ports; two power supply slots with 715 WAC power supply installed by default; supports StackWise-480 and StackPower.	Cisco IOS XE Gibraltar 16.11.1
C9300-48S-E	Network Essentials		Cisco IOS XE Gibraltar 16.11.1
C9300-48T-A	Network Advantage	Stackable 48 10/100/1000 Ethernet ports; 350 WAC power supply; supports StackWise-480 and StackPower	Cisco IOS XE Everest 16.5.1a
C9300-48T-E	Network Essentials		Cisco IOS XE Everest 16.5.1a
C9300-48U-A	Network Advantage	Stackable 48 10/100/1000 UPoE ports; PoE budget of 822 W; 1100 WAC power supply; supports StackWise-480 and StackPower	Cisco IOS XE Everest 16.5.1a
C9300-48U-E	Network Essentials		Cisco IOS XE Everest 16.5.1a
C9300-48UB-A	Network Advantage	Stackable 48 10/100/1000 Mbps UPOE ports that provide deep buffers and higher scale; PoE budget of 822 W with 1100 WAC power supply; supports StackWise-480 and StackPower	Cisco IOS XE Gibraltar 16.12.1
C9300-48UB-E	Network Essentials		Cisco IOS XE Gibraltar 16.12.1
C9300-48UN-A	Network Advantage	Stackable 48 Multigigabit Ethernet (100 Mbps or 1/2.5/5 Gbps) UPoE ports; PoE budget of 610 W with 1100 WAC power supply; supports StackWise-480 and StackPower	Cisco IOS XE Fuji 16.8.1a
C9300-48UN-E	Network Essentials		Cisco IOS XE Fuji 16.8.1a
C9300-48UXM-A	Network Advantage	Stackable 48 (36 2.5G Multigigabit Ethernet and 12 10G Multigigabit Ethernet Universal Power Over Ethernet (UPOE) ports)	Cisco IOS XE Everest 16.6.2
C9300-48UXM-E	Network Essentials		Cisco IOS XE Everest 16.6.2

[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 9300L Series Switches

Switch Model	Default License Level[2]	Description	Introductory Release
C9300L-24T-4G-A	Network Advantage	Stackable 24x10/100/1000M Ethernet ports; 4x1G SFP fixed uplink ports; 350 WAC power supply; supports StackWise-320.	Cisco IOS XE Gibraltar 16.11.1c
C9300L-24T-4G-E	Network Essentials		Cisco IOS XE Gibraltar 16.11.1c
C9300L-24P-4G-A	Network Advantage	Stackable 24x10/100/1000M PoE+ ports; 4x1G SFP fixed uplink ports; PoE budget of 505W with 715 WAC power supply; supports StackWise-320.	Cisco IOS XE Gibraltar 16.11.1c
C9300L-24P-4G-E	Network Essentials		Cisco IOS XE Gibraltar 16.11.1c
C9300L-24T-4X-A	Network Advantage	Stackable 24x10/100/1000M Ethernet ports; 4x10G SFP+ fixed uplink ports; 350 WAC power supply; supports StackWise-320.	Cisco IOS XE Gibraltar 16.11.1c
C9300L-24T-4X-E	Network Essentials		Cisco IOS XE Gibraltar 16.11.1c
C9300L-24P-4X-A	Network Advantage	Stackable 24x10/100/1000M PoE+ ports; 4x10G SFP+ fixed uplink ports; PoE budget of 505W with 715 WAC power supply; supports StackWise-320.	Cisco IOS XE Gibraltar 16.11.1c
C9300L-24P-4X-E	Network Essentials		Cisco IOS XE Gibraltar 16.11.1c
C9300L-48T-4G-A	Network Advantage	Stackable 48x10/100/1000M Ethernet ports; 4x1G SFP fixed uplink ports; 350 WAC power supply; supports StackWise-320.	Cisco IOS XE Gibraltar 16.11.1c
C9300L-48T-4G-E	Network Essentials		Cisco IOS XE Gibraltar 16.11.1c
C9300L-48P-4G-A	Network Advantage	Stackable 48x10/100/1000M PoE+ ports; 4x1G SFP fixed uplink ports; PoE budget of 505W with 715 WAC power supply; supports StackWise-320.	Cisco IOS XE Gibraltar 16.11.1c
C9300L-48P-4G-E	Network Essentials		Cisco IOS XE Gibraltar 16.11.1c
C9300L-48T-4X-A	Network Advantage	Stackable 48x10/100/1000M Ethernet ports; 4x10G SFP+ fixed uplink ports; 350 WAC power supply; supports StackWise-320.	Cisco IOS XE Gibraltar 16.11.1c
C9300L-48T-4X-E	Network Essentials		Cisco IOS XE Gibraltar 16.11.1c
C9300L-48P-4X-A	Network Advantage	Stackable 48x10/100/1000M PoE+ ports; 4x10G SFP+ fixed uplink ports; PoE budget of 505W with 715 WAC power supply; supports StackWise-320.	Cisco IOS XE Gibraltar 16.11.1c
C9300L-48P-4X-E	Network Essentials		Cisco IOS XE Gibraltar 16.11.1c

Switch Model	Default License Level[2]	Description	Introductory Release
C9300L-48PF-4G-A	Network Advantage	Stackable 48 10/100/1000 Mbps PoE+ ports; 4x1G SFP+ fixed uplink ports; PoE budget of 890 W with 1100 WAC power supply; supports StackWise-320.	Cisco IOS XE Gibraltar 16.12.2
C9300L-48PF-4G-E	Network Essentials		Cisco IOS XE Gibraltar 16.12.2
C9300L-48PF-4X-A	Network Advantage	Stackable 48 10/100/1000 Mbps PoE+ ports; 4x10G SFP+ fixed uplink ports; PoE budget of 890 W with 1100 WAC power supply; supports StackWise-320.	Cisco IOS XE Gibraltar 16.12.2
C9300L-48PF-4X-E	Network Essentials		Cisco IOS XE Gibraltar 16.12.2
C9300L-24UXG-4X-A	Network Advantage	Stackable 16 10/100/1000 Mbps and 8 Multigigabit Ethernet (100 Mbps or 1/2.5/5/10 Gbps) UPOE ports; 4x10G SFP+ fixed uplink ports; PoE budget of 880 W with 1100 WAC power supply; supports StackWise-320.	Cisco IOS XE Gibraltar 16.12.2
C9300L-24UXG-4X-E	Network Essentials		Cisco IOS XE Gibraltar 16.12.2
C9300L-24UXG-2Q-A	Network Advantage	Stackable 16 10/100/1000 Mbps and 8 Multigigabit Ethernet (100 Mbps or 1/2.5/5/10 Gbps) UPOE ports; 2x40G QSFP+ fixed uplink ports; PoE budget of 722 W with 1100 WAC power supply; supports StackWise-320.	Cisco IOS XE Gibraltar 16.12.2
C9300L-24UXG-2Q-E	Network Essentials		Cisco IOS XE Gibraltar 16.12.2
C9300L-48UXG-4X-A	Network Advantage	Stackable 36 10/100/1000 Mbps and 12 Multigigabit Ethernet (100 Mbps or 1/2.5/5/10 Gbps) UPOE ports; 4x10G SFP+ fixed uplink ports; PoE budget of 675 W with 1100 WAC power supply; supports StackWise-320.	Cisco IOS XE Gibraltar 16.12.2
C9300L-48UXG-4X-E	Network Essentials		Cisco IOS XE Gibraltar 16.12.2
C9300L-48UXG-2Q-A	Network Advantage	Stackable 36 10/100/1000 Mbps and 12 Multigigabit Ethernet (100 Mbps or 1/2.5/5/10 Gbps) UPOE ports; 2x40G QSFP+ fixed uplink ports; PoE budget of 675 W with 1100 WAC power supply; supports StackWise-320.	Cisco IOS XE Gibraltar 16.12.2
C9300L-48UXG-2Q-E	Network Essentials		Cisco IOS XE Gibraltar 16.12.2

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

Table 4: Cisco Catalyst 9300LM Series Switches

Switch Model	Default License Level[3]	Description	Introductory Release
C9300LM-48T-4Y-A	Network Advantage	Stackable 48 x 10/100/1000 M Ethernet ports; 4 x 25 GE SFP28 fixed uplink ports; 600 WAC power supply and fixed fans; supports StackWise-320.	Cisco IOS XE Cupertino 17.9.1
C9300LM-48T-4Y-E	Network Essentials		Cisco IOS XE Cupertino 17.9.1

Switch Model	Default License Level[3]	Description	Introductory Release
C9300LM-24U-4Y-A	Network Advantage	Stackable 24 x 10/100/1000 M UPOE ports; 4 x 25 GE SFP28 fixed uplink ports; PoE budget of 420 W with a single default 600 WAC power supply; supports StackWise-320.	Cisco IOS XE Cupertino 17.9.1
C9300LM-24U-4Y-E	Network Essentials		Cisco IOS XE Cupertino 17.9.1
C9300LM-48U-4Y-A	Network Advantage	Stackable 48 x 10/100/1000 M UPOE ports; 4 x 25 GE SFP28 fixed uplink ports; PoE budget of 790 W with a single default 1000 WAC power supply; supports StackWise-320.	Cisco IOS XE Cupertino 17.9.1
C9300LM-48U-4Y-E	Network Essentials		Cisco IOS XE Cupertino 17.9.1
C9300LM-48UX-4Y-A	Network Advantage	Stackable 40 x 10/100/1000 M and 8 Multigigabit Ethernet (100M/1000M/2.5GE/5GE/10GE) UPOE ports; 4 x 25 GE SFP28 fixed uplink ports; PoE budget of 790 W with a single default 1000 WAC power supply; supports StackWise-320.	Cisco IOS XE Cupertino 17.9.1
C9300LM-48UX-4Y-E	Network Essentials		Cisco IOS XE Cupertino 17.9.1

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

Table 5: Cisco Catalyst 9300X Series Switches

Switch Model	Default License Level[4]	Description	Introductory Release
C9300X-12Y-A	Network Advantage	Stackable 12 1/10/25 GE SFP28 downlink ports; 715 WAC power supply; supports StackPower+, StackWise-1T and C9300X-NM network modules.	Cisco IOS XE Bengaluru 17.5.1
C9300X-12Y-E	Network Essentials		Cisco IOS XE Bengaluru 17.5.1
C9300X-24Y-A	Network Advantage	Stackable 24 1/10/25 GE SFP28 downlink ports; 715 WAC power supply; supports StackPower+, StackWise-1 and C9300X-NM network modules.	Cisco IOS XE Bengaluru 17.5.1
C9300X-24Y-E	Network Essentials		Cisco IOS XE Bengaluru 17.5.1
C9300X-24HX-A	Network Advantage	Stackable 24 Multigigabit Ethernet (100 Mbps or 1/2.5/5/10 Gbps) UPOE+ ports; PoE budget of 735W with 1100WAC power supply; supports StackPower+, StackWise-1T and C9300X-NM network modules.	Cisco IOS XE Cupertino 17.9.1
C9300X-24HX-E	Network Essentials		Cisco IOS XE Cupertino 17.9.1
C9300X-48HX-A	Network Advantage	Stackable 48 Multigigabit Ethernet (100 Mbps or 1/2.5/5/10 Gbps) UPOE+ports; PoE budget of 590W with 1100 WAC power supply; supports StackPower+, StackWise-1T and C9300X-NM network modules.	Cisco IOS XE Bengaluru 17.5.1
C9300X-48HX-E	Network Essentials		Cisco IOS XE Bengaluru 17.5.1

Switch Model	Default License Level[4]	Description	Introductory Release
C9300X-48TX-A	Network Advantage	Stackable 48 Multigigabit Ethernet (100 Mbps or 1/2.5/5/10 Gbps) ports; 715WAC powersupply; supports StackPower+, StackWise-1T and C9300X-NM network modules.	Cisco IOS XE Bengaluru 17.5.1
C9300X-48TX-E	Network Essentials		Cisco IOS XE Bengaluru 17.5.1
C9300X-48HXN-A	Network Advantage	Stackable 40 x 100/1000 M or 2.5/5 GE Multigigabit Ethernet and 8 x 100/1000 M or 2.5/5/10 GE Multigigabit Ethernet UPOE+ ports; PoE budget of 690W with 1100WAC power supply; supports StackPower+, StackWise-1T and C9300X-NM network modules	Cisco IOS XE Cupertino 17.9.3
C9300X-48HXN-E	Network Essentials		Cisco IOS XE Cupertino 17.9.3

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

Supported Network Modules

The following table lists the optional uplink network modules with 1-Gigabit, 10-Gigabit, 25-Gigabit, and 40-Gigabit slots. You should only operate the switch with either a network module or a blank module installed.

Network Module	Description	Introductory Release
C3850-NM-4-1G [1]	Four 1 Gigabit Ethernet SFP module slots	Cisco IOS XE Everest 16.5.1a
C3850-NM-2-10G [1]	Two 10 Gigabit Ethernet SFP module slots	Cisco IOS XE Everest 16.5.1a
C3850-NM-4-10G [1]	Four 10 Gigabit Ethernet SFP module slots	Cisco IOS XE Everest 16.5.1a
C3850-NM-8-10G [1]	Eight 10 Gigabit Ethernet SFP module slots	Cisco IOS XE Everest 16.5.1a
C3850-NM-2-40G [1]	Two 40 Gigabit Ethernet SFP module slots	Cisco IOS XE Everest 16.5.1a
C9300-NM-4G [2]	Four 1 Gigabit Ethernet SFP module slots	Cisco IOS XE Everest 16.5.1a
C9300-NM-4M [2]	Four MultiGigabit Ethernet slots	Cisco IOS XE Fuji 16.8.1a
C9300-NM-8X [2]	Eight 10 Gigabit Ethernet SFP+ module slots	Cisco IOS XE Everest 16.5.1a
C9300-NM-2Q [2]	Two 40 Gigabit Ethernet QSFP+ module slots	Cisco IOS XE Everest 16.5.1a
C9300-NM-2Y [2]	Two 25 Gigabit Ethernet SFP28 module slots	Cisco IOS XE Fuji 16.8.1a

Network Module	Description	Introductory Release
C9300X-NM-2C[3]	Two 40 Gigabit Ethernet/100 Gigabit Ethernet QSFP+ module slots	Cisco IOS XE Bengaluru 17.5.1
C9300X-NM-4C [3]	Four 40 Gigabit Ethernet/100 Gigabit Ethernet slots with a QSFP+ connector ineach slot.	Cisco IOS XE Bengaluru 17.6.1
C9300X-NM-8M[3]	Eight Multigigabit Ethernet slots	Cisco IOS XE Bengaluru 17.5.1
C9300X-NM-8Y[3]	Eight 25 Gigabit Ethernet/10 Gigabit Ethernet/1 Gigabit Ethernet SFP+ module slots	Cisco IOS XE Bengaluru 17.5.1

Note

1. These network modules are supported only on the C3850 and C9300 SKUs of the Cisco Catalyst 3850 Series Switches and Cisco Catalyst 9300 Series Switches respectively.
2. These network modules are supported only on the C9300 SKUs of the Cisco Catalyst 9300 Series Switches.
3. These network modules are supported only on the C9300X SKUs of the Cisco Catalyst 9300 Series Switches.

The following table lists the network modules that are supported on the Cisco Catalyst 9300X-HXN Series Switches and the ports that are usable on each of these network module:

Table 6: Network Modules Supported on Catalyst 9300X-HXN Series Switches

Network Module	Cisco IOS XE Cupertino 17.7.1 and Previous Releases	Cisco IOS XE Cupertino 17.8.1 and Later Releases
C9300X-NM-8Y (8x25G)	Ports 1 to 4 usable.	Ports 1 to 6 usable. Ports 7 and 8 are permanently disabled.
C9300X-NM-8M (8xmGig)	Ports 1 to 4 usable.	Ports 1 to 6 usable. Ports 7 and 8 are permanently disabled.
C9300X-NM-2C (2x100G/2x40G)	Ports 1 to 2 usable. No breakout cable support.	Ports 1 and 2 usable. Breakout cable supported only on port 1. No support for breakout cable on port 2.

Supported Optics Modules

Cisco Catalyst Series Switches support a wide range of optics and the list of supported optics is updated on a regular basis. Use the Transceiver Module Group (TMG) Compatibility Matrix tool, or consult the tables at this URL for the latest transceiver module compatibility information: https://www.cisco.com/en/US/products/hw/modules/ps5455/products_device_support_tables_list.html

What's New in Cisco IOS XE 17.18.x

Hardware Features in Cisco IOS XE 17.18.1

There are no new hardware features in this release.

Software Features in Cisco IOS XE 17.18.1

Feature Name	Description
BGP EVPN VXLAN • BGP EVPN IPv6 Originator ID • Next-hop recursive support with EVPN PBR	The following BGP EVPN VXLAN features are introduced in this release: • BGP EVPN IPv6 originator ID support in Route Type 3 (RT3). • Traffic steering in VXLAN campus fabric using PBR and next-hop recursive support with EVPN PBR (ip2fabric).
BGP neighbors monitoring with SNMP	Introduces the ability to use SNMP to monitor BGP neighbors based on the VRF the neighbor is in. This feature is enabled by default.
Embedded Packet Capture (EPC) support on EtherChannel sub-interfaces	Introduces support for EPC on EtherChannel subinterfaces on Cisco Catalyst 9300X Series Switches.
Maximum number of allowed MAC address moves	Introduces the ability to configure the maximum number of allowed MAC address moves in a given time interval. By default, there is no limit on the number of MAC address moves.
Message authenticator attribute in RADIUS	Introduces support for sending message authenticator attribute in the RADIUS packets which are sent out from the IOS-XE. With this feature, RADIUS packets that do not have the message authenticator attribute are dropped.
Programmability: • YANG Data Models	The following programmability features are introduced in this release: • YANG Data Models: For the list of Cisco IOS XE YANG models available with this release, navigate to: https://github.com/YangModels/yang/tree/main/vendor/cisco/xe/17181.
Resource Manager System (RMS) and Resource Manager Controller (RMC) commands	Introduces support for the following commands: • RMS: show platform software process database fed active details RMS_DB table npi_rms content • RMS IPC (Interprocess Communications Protocol): show platform software resource-manager switch active R0 ipc stats • RMC: show platform software process database fed active details RMC_DB "table npi_rmc" content • RMS and RMC: show platform software resource-manager switch active R0 available-resource RMS

Feature Name	Description
TLS for TACACS+	Introduces support for TACACS+ over Transport Layer Security (TLS). This feature enhances security and provides stronger certificate-based AAA services.

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

Hardware and Software Behavior Changes in Cisco IOS XE 17.18.1

There are no new behavior changes in this release.

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

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

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

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

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

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

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

- **SSHv1**

  Recommendation: Use SSHv2.

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

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

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

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

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

  Recommendation: Do not use this legacy feature.

- **TLS 1.0 and TLS 1.1**

  Recommendation: Use TLS 1.2 or later.

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

  Recommendation: Use ciphers with SHA256 or stronger digital signatures.

- **HTTP**

  Recommendation: Use HTTPS.

- **Telnet**

  Recommendation: Use SSH for remote access.

- **FTP and TFTP**

  Recommendation: Use SFTP or HTTPS for file transfers.

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

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

- **BootP server**

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

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

  Recommendation: Do not use these services on network devices.

- **IP finger**

  Recommendation: Do not use this protocol on network devices.

- **NTP control messages**

  Recommendation: Do not use this feature.

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

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

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

Caveats

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

Open Caveats in Cisco IOS XE 17.18.x

There are no open caveats in this release.

Resolved Caveats in Cisco IOS XE 17.18.1

There are no resolved caveats in this release.

Feature Support

This section lists the supported and unsupported features.

All Supported Features

For the complete list of features supported on a platform, see the Cisco Feature Navigator.

Differences in Feature Support Between Switch Models

For the most part, the list of supported software features is common across Cisco Catalyst 9300, 9300L, 9300LM, and 9300X Series Switches. The following sections list exceptions that are not supported on all PIDs.

For the list of PIDs under the Cisco Catalyst 9300, 9300L, 9300LM, and 9300X Series Switches, see Supported Cisco Catalyst 9300 Series Switches Model Numbers, on page 1.

Table 7: Cisco TrustSec

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

Table 8: Security

Feature	Not Supported On These Variants
MACsec switch-to-host connections in an overlay network.	All
Virtual Routing and Forwarding (VRF)-Aware web authentication	All

Table 9: System Management

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

Limitations and Restrictions

- Control Plane Policing (CoPP): The **show running-config** command does not display information about classes configured under `system-cpp policy`, when they are left at default values. Use the **show policy-map system-cpp-policy** or the **show policy-map control-plane** commands in privileged EXEC mode instead.
- Cisco TrustSec restrictions: Cisco TrustSec can be configured only on physical interfaces, not on logical interfaces.
- Flexible NetFlow limitations
  - You cannot configure NetFlow export using the Ethernet Management port (GigabitEthernet0/0).
  - You can not configure a flow monitor on logical interfaces, such as layer 2 port-channels, loopback, tunnels.

- You can not configure multiple flow monitors of same type (ipv4, ipv6 or datalink) on the same interface for same direction.

- Hardware Limitations (Optics):
  - SFP-10G-T-X supports 100Mbps/1G/10G speeds based on auto negotiation with the peer device. 10Mbps speed is not supported and you cannot force speed settings from the transceiver.
  - PHY Loopback test is not supported on SFP-10G-T-X.

- QoS restrictions
  - When configuring QoS queuing policy, the sum of the queuing buffer should not exceed 100%.
  - Policing and marking policy on sub interfaces is supported.
  - Marking policy on switched virtual interfaces (SVI) is supported.
  - QoS policies are not supported for port-channel interfaces, tunnel interfaces, and other logical interfaces.
  - Stack Queuing and Scheduling (SQS) drops CPU bound packets exceeding 1.4 Gbps.

- 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.

- Stacking:
  - A switch stack supports up to eight stack members.
  - Mixed stacking is supported between C9300 and C9300X SKUs and between C9300L and C9300LM SKUs only.

    This additional restriction applies to the C9300-24UB, C9300-24UXB, and C9300-48UB models of the series: These models can be stacked only with each other. They cannot be stacked with other C9300 SKUs.
  - Auto upgrade for a new member switch is supported only in the install mode.

- 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.
- 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 2000 connections per second (CPS) at less than 50% CPU utilization. Above this rate, AVC service is not guaranteed.
  - Scale: Able to handle up to 20000 bi-directional flows per 24 access ports and 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.
- The File System Check (fsck) utility is not supported in install mode.
- The command **service-routing mdns-sd** is being deprecated. Use the **mdns-sd gateway** command instead.
- Switch Web UI allows configuration of data VLANs only and not voice VLANs. If you remove a voice VLAN configured to an interface using the Web UI, then all data VLANs associated with the interface are also removed by default.

Licensing

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

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

Available Licensing Models and Configuration Information

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

Compatibility Matrix

To view the software compatibility information between Cisco Catalyst 9300 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 17.18.1	CAT9K_IOSXE	cat9k_iosxe.17.18.01.SPA.bin
	No Payload Encryption (NPE)	cat9k_iosxe_npe.17.18.01.SPA.bin

To download software images, visit the software downloads page: Cisco Catalyst 9300 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.

Release	ROMMON Version (C9300 Models)	ROMMON Version (C9300L Models)	ROMMON Version (C9300X Models)	ROMMON Version (C9300LM Models)
17.18.1	17.12.1r	17.14.1r	17.13.1r	17.14.1r
17.17.1	17.12.1r	17.14.1r	17.13.1r	17.14.1r
17.16.1	17.12.1r	17.14.1r	17.13.1r	17.14.1r
17.15.4	17.12.1r	17.15.4r	17.13.1r	17.14.1r
17.15.3	17.12.1r	17.14.1r	17.13.1r	17.14.1r
17.15.2	17.12.1r	17.14.1r	17.13.1r	17.14.1r
17.15.1	17.12.1r	17.14.1r	17.13.1r	17.14.1r
17.14.1	17.12.1r	17.14.1r	17.13.1r	17.14.1r
17.13.1	17.12.1r	17.13.1r	17.13.1r	17.12.1r
Dublin 17.12.4	17.12.1r	17.12.2r	17.12.1r[FC3]	17.12.1r
Dublin 17.12.3	17.12.1r	17.12.2r	17.12.1r[FC3]	17.12.1r
Dublin 17.12.2	17.12.1r	17.12.2r	17.12.1r[FC2]	17.12.1r
Dublin 17.12.1	17.12.1r	17.12.1r	17.12.1r[FC1]	17.12.1r
Dublin 17.11.1	17.11.1r[FC1]	17.10.1r[FC1]	17.11.1r	17.10.1r
Dublin 17.10.1	17.10.1r[FC1]	17.10.1r[FC1]	17.9.1r	17.10.1r
Cupertino 17.9.5	17.9.2r	17.9.2r	17.9.4r	17.9.1r[FC1]
Cupertino 17.9.4	17.9.2r	17.9.1r	17.9.1r	17.9.1r[FC1]
Cupertino 17.9.3	17.9.2r	17.9.1r	17.9.1r	17.9.1r[FC1]
Cupertino 17.9.2	17.9.1r	17.9.1r	17.9.1r	17.9.1r

Release	ROMMON Version (C9300 Models)	ROMMON Version (C9300L Models)	ROMMON Version (C9300X Models)	ROMMON Version (C9300LM Models)
Cupertino 17.9.1	17.9.1r	17.9.1r	17.9.1r	17.9.1r
Cupertino 17.8.1	17.8.1r[FC2]	17.8.1r[FC2]	17.5.1r	-
Cupertino 17.7.1	17.6.1r[FC2]	17.6.1r[FC2]	17.5.1r	-
Bengaluru 17.6.7	17.6.1r[FC2]	17.8.1r[FC2]	17.5.1r	-
Bengaluru 17.6.6a	17.6.6r	17.8.1r[FC2]	17.5.1r	-
Bengaluru 17.6.6	17.6.6r	17.8.1r[FC2]	17.5.1r	-
Bengaluru 17.6.5	17.6.6r	17.8.1r[FC2]	17.5.1r	-
Bengaluru 17.6.4	17.6.1r[FC2]	17.8.1r[FC2]	17.5.1r	-
Bengaluru 17.6.3	17.6.1r[FC2]	17.8.1r[FC2]	17.5.1r	-
Bengaluru 17.6.2	17.6.1r[FC2]	17.6.1r[FC2]	17.5.1r	-
Bengaluru 17.6.1	17.6.1r[FC2]	17.6.1r[FC2]	17.5.1r	-
Bengaluru 17.5.1	17.5.2r	17.4.1r[FC2]	17.5.1r	-
Bengaluru 17.4.1	17.4.1r	17.4.1r[FC2]	-	-
Amsterdam 17.3.8a	17.3.8r	17.8.1r[FC2]	-	-
Amsterdam 17.3.8	17.3.8r	17.8.1r[FC2]	-	-
Amsterdam 17.3.7	17.3.2r	17.8.1r[FC2]	-	-
Amsterdam 17.3.6	17.3.2r	17.8.1r[FC2]	-	-
Amsterdam 17.3.5	17.3.2r	17.8.1r[FC2]	-	-
Amsterdam 17.3.4	17.3.2r	17.3.2r	-	-
Amsterdam 17.3.3	17.3.2r	17.3.2r	-	-
Amsterdam 17.3.2a	17.3.2r	17.3.2r	-	-
Amsterdam 17.3.1	17.3.1r[FC2]	17.1.1r [FC1]	-	-
Amsterdam 17.2.1	17.2.1r[FC1]	17.1.1r[FC1]	-	-
Amsterdam 17.1.1	17.1.1r [FC1]	17.1.1r [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 **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.

Note

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

Upgrading in Install Mode

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

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

When upgrading from ...	Use these commands...	To upgrade to...
Cisco IOS XE Everest 16.5.1a or Cisco IOS XE Everest 16.6.1	Only **request platform software** commands	Cisco IOS XE 17.18.x
Cisco IOS XE Everest 16.6.2 and all later releases	Either **install** commands or **request platform software** commands[5].	

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

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

Step 1 Clean-up

install remove inactive

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

Step 2 Copy new image to flash

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

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

b) **dir flash:**

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

Step 3 Set boot variable

a) **no boot system**

Use this command to reset the boot variable. This command removes the startup system image specification. Otherwise, the switch may boot a previously configured boot image.

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

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

c) **no boot manual**

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

d) **write memory**

Use this command to save boot settings.

e) **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 TFTP server or the flash drive of the *active* switch, if you have copied the image to flash memory. If you point to an image on the flash or USB drive of a member switch (instead of the active), you must specify the exact flash or USB drive - otherwise installation fails. For example, if the image is on the flash drive of member switch 3 (flash-3): `Switch# install add file flash-3:cat9k_iosxe.17.18.01.SPA.bin activate commit`.

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

Step 5 Verify 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 Jul 31 10:02:31 PDT 2025
install_remove: Removing IMG
```

```
Cleaning up unnecessary package files
No path specified, will use booted path /flash/packages.conf

Cleaning /flash
Scanning boot directory for packages ... done.
Preparing packages list to delete ...
[R0]: /flash/packages.conf File is in use, will not delete.
[R1]: /flash/packages.conf File is in use, will not delete.
[R0]: /flash/cat9k-cc_srdriver.17.17.01.SPA.pkg File is in use, will not delete.
[R1]: /flash/cat9k-cc_srdriver.17.17.01.SPA.pkg File is in use, will not delete.
[R0]: /flash/cat9k-espbase.17.17.01.SPA.pkg File is in use, will not delete.
[R1]: /flash/cat9k-espbase.17.17.01.SPA.pkg File is in use, will not delete.
[R0]: /flash/cat9k-guestshell.17.17.01.SPA.pkg File is in use, will not delete.
[R1]: /flash/cat9k-guestshell.17.17.01.SPA.pkg File is in use, will not delete.
[R0]: /flash/cat9k-lni.17.17.01.SPA.pkg File is in use, will not delete.
[R1]: /flash/cat9k-lni.17.17.01.SPA.pkg File is in use, will not delete.
[R0]: /flash/cat9k-rpbase.17.17.01.SPA.pkg File is in use, will not delete.
[R1]: /flash/cat9k-rpbase.17.17.01.SPA.pkg File is in use, will not delete.
[R0]: /flash/cat9k-sipbase.17.17.01.SPA.pkg File is in use, will not delete.
[R1]: /flash/cat9k-sipbase.17.17.01.SPA.pkg File is in use, will not delete.
[R0]: /flash/cat9k-sipspa.17.17.01.SPA.pkg File is in use, will not delete.
[R1]: /flash/cat9k-sipspa.17.17.01.SPA.pkg File is in use, will not delete.
[R0]: /flash/cat9k-srdriver.17.17.01.SPA.pkg File is in use, will not delete.
[R1]: /flash/cat9k-srdriver.17.17.01.SPA.pkg File is in use, will not delete.
[R0]: /flash/cat9k-webui.17.17.01.SPA.pkg File is in use, will not delete.
[R1]: /flash/cat9k-webui.17.17.01.SPA.pkg File is in use, will not delete.
[R0]: /flash/cat9k-wlc.17.17.01.SPA.pkg File is in use, will not delete.
[R1]: /flash/cat9k-wlc.17.17.01.SPA.pkg File is in use, will not delete.
[R0]: /flash/cat9k_iosxe.17.17.01.SPA.conf File is in use, will not delete.
[R1]: /flash/cat9k_iosxe.17.17.01.SPA.conf File is in use, will not delete.
[R0]: /flash/cat9k-rpboot.17.17.01.SPA.pkg File is in use, will not delete.
[R1]: /flash/cat9k-rpboot.17.17.01.SPA.pkg File is in use, will not delete.

The following files will be deleted:
[R0]: /flash/cat9k_iosxe.17.17.01.SPA.bin
[R1]: /flash/cat9k_iosxe.17.17.01.SPA.bin
[R0]: /flash/cat9k-cc_srdriver.17.17.02.SPA.pkg
[R1]: /flash/cat9k-cc_srdriver.17.17.02.SPA.pkg
[R0]: /flash/cat9k-espbase.17.17.02.SPA.pkg
[R1]: /flash/cat9k-espbase.17.17.02.SPA.pkg
[R0]: /flash/cat9k-guestshell.17.17.02.SPA.pkg
[R1]: /flash/cat9k-guestshell.17.17.02.SPA.pkg
[R0]: /flash/cat9k-lni.17.17.02.SPA.pkg
[R1]: /flash/cat9k-lni.17.17.02.SPA.pkg
[R0]: /flash/cat9k-rpbase.17.17.02.SPA.pkg
[R1]: /flash/cat9k-rpbase.17.17.02.SPA.pkg
[R0]: /flash/cat9k-sipbase.17.17.02.SPA.pkg
[R1]: /flash/cat9k-sipbase.17.17.02.SPA.pkg
[R0]: /flash/cat9k-sipspa.17.17.02.SPA.pkg
[R1]: /flash/cat9k-sipspa.17.17.02.SPA.pkg
[R0]: /flash/cat9k-srdriver.17.17.02.SPA.pkg
[R1]: /flash/cat9k-srdriver.17.17.02.SPA.pkg
[R0]: /flash/cat9k-webui.17.17.02.SPA.pkg
[R1]: /flash/cat9k-webui.17.17.02.SPA.pkg
[R0]: /flash/cat9k-wlc.17.17.02.SPA.pkg
[R1]: /flash/cat9k-wlc.17.17.02.SPA.pkg
[R0]: /flash/cat9k_iosxe.17.17.02.SPA.conf
[R1]: /flash/cat9k_iosxe.17.17.02.SPA.conf
[R0]: /flash/cat9k-rpboot.17.17.02.SPA.pkg
[R1]: /flash/cat9k-rpboot.17.17.02.SPA.pkg

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

Deleting file /flash/cat9k_iosxe.17.17.01.SPA.bin ... done.
```

```
Deleting file /flash/cat9k-cc_srdriver.17.17.02.SPA.pkg ... done.
Deleting file /flash/cat9k-espbase.17.17.02.SPA.pkg ... done.
Deleting file /flash/cat9k-guestshell.17.17.02.SPA.pkg ... done.
Deleting file /flash/cat9k-lni.17.17.02.SPA.pkg ... done.
Deleting file /flash/cat9k-rpbase.17.17.02.SPA.pkg ... done.
Deleting file /flash/cat9k-sipbase.17.17.02.SPA.pkg ... done.
Deleting file /flash/cat9k-sipspa.17.17.02.SPA.pkg ... done.
Deleting file /flash/cat9k-srdriver.17.17.02.SPA.pkg ... done.
Deleting file /flash/cat9k-webui.17.17.02.SPA.pkg ... done.
Deleting file /flash/cat9k-wlc.17.17.02.SPA.pkg ... done.
Deleting file /flash/cat9k_iosxe.17.17.02.SPA.conf ... done.
Deleting file /flash/cat9k-rpboot.17.17.02.SPA.pkg ... done.
Deleting /flash/.images/17.17.01.0.1444.1669767962 ... done.
SUCCESS: Files deleted.

--- Starting Post_Remove_Cleanup ---
Performing REMOVE_POSTCHECK on all members
Finished Post_Remove_Cleanup
SUCCESS: install_remove Thu Jul 31 10:02:36 PDT 2025
Switch#
<output truncated>
```

```
Switch# copy tftp://10.8.0.6/image/cat9k_iosxe.17.18.01.SPA.bin flash:

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

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


Switch# dir flash:*.bin

Directory of flash:/*.bin

Directory of flash:/

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


Switch(config)# no boot system

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

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

Switch# write memory

Switch# show boot
Current Boot Variables:
BOOT variable = flash:packages.conf;

Boot Variables on next reload:
BOOT variable = flash:packages.conf;
Manual Boot = no
Enable Break = yes
Boot Mode = DEVICE
iPXE Timeout = 0
```

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

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

install_add_activate_commit: START Thu Jul 31 10:15:02 PDT 2025
install_add: START Thu Jul 31 10:15:02 PDT 2025
install_add: Adding IMG
--- Starting initial file syncing ---
Copying flash:cat9k_iosxe.17.18.01.SPA.bin from Switch 1 to Switch 1 2
Info: Finished copying to the selected Switch
Finished initial file syncing

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

Image added. Version: 17.18.01.0

    Warning: ISSU compatibility check failed for 17.18.01.0
install_activate: START Thu Jul 31 10:17:34 PDT 2025
install_activate: Activating IMG
Following packages shall be activated:
/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-lni.17.18.01.SPA.pkg
/flash/cat9k-rpbase.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/cat9k-rpboot.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 all members
 [1] Activate package(s) on Switch 1
 [2] Activate package(s) on Switch 2
 [2] Finished Activate on Switch 2
 [1] Finished Activate on Switch 1
Checking status of Activate on [1 2]
Activate: Passed on [1 2]
Finished Activate

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

*Jul 31 10:22:00.934: %IOSXEBOOT-4-BOOTLOADER_UPGRADE: (rp/0): Starting boot preupgrade
*Jul 31 10:22:00.937: %IOSXEBOOT-4-BOOTLOADER_UPGRADE: (rp/0): ### Thu Jul 31 10:22:00 PDT 2025 PLEASE DO NOT
 POWER CYCLE ### BOOT LOADER UPGRADING
*Jul 31 10:22:50.808: %IOSXEBOOT-4-flashcp: (rp/0): polaris_adelphi_rommon_sb.bin
*Jul 31 10:22:56.093: %IOSXEBOOT-4-BOOTLOADER_UPGRADE: (rp/0): boot loader upgrade successful
```

```
SUCCESS: install_add_activate_commit Thu Jul 31 10:22:59 PDT 2025
stack-nyqcr3#
Chassis 1 reloading, reason - Reload command
Jul 31 10:23:05.604: %PMAN-5-EXITACTION: F0/0: pvp: Process manager is exiting: reload fp action requested
Jul 31 10:23:07.295: %PMAN-5-EXITACTION: R0/0: pvp: Process manager is exiting: rp processes exit with reload
 switch code



Initializing Hardware......

System Bootstrap, Version 17.18.1r[FC1], RELEASE SOFTWARE (P)
Compiled Wed 03/31/2025 14:36:07.63 by rel

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

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


Waiting for 120 seconds for other switches to boot

Switch number is 1
All switches in the stack have been discovered. Accelerating discovery
<output truncated>
```

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

```
Switch# dir flash:*.pkg

Directory of flash:/
75140 -rw- 2012104     Mar 25 2025 09:52:41 -07:00 cat9k-cc_srdriver.17.17.01.SPA.pkg
475141 -rw- 70333380   Mar 25 2025 09:52:44 -07:00 cat9k-espbase.17.17.01.SPA.pkg
475142 -rw- 13256      Mar 25 2025 09:52:44 -07:00 cat9k-guestshell.17.17.01.SPA.pkg
475143 -rw- 349635524  Mar 25 2025 09:52:54 -07:00 cat9k-rpbase.17.17.01.SPA.pkg
475149 -rw- 24248187   Mar 25 2025 09:53:02 -07:00 cat9k-rpboot.17.17.01.SPA.pkg
475144 -rw- 25285572   Mar 25 2025 09:52:55 -07:00 cat9k-sipbase.17.17.01.SPA.pkg
475145 -rw- 20947908   Mar 25 2025 09:52:55 -07:00 cat9k-sipspa.17.17.01.SPA.pkg
475146 -rw- 2962372    Mar 25 2025 09:52:56 -07:00 cat9k-srdriver.17.17.01.SPA.pkg
475147 -rw- 13284288   Mar 25 2025 09:52:56 -07:00 cat9k-webui.17.17.01.SPA.pkg
475148 -rw- 13248      Mar 25 2025 09:52:56 -07:00 cat9k-wlc.17.17.01.SPA.pkg

491524 -rw- 25711568   Jul 31 2025 11:49:33 -07:00 cat9k-cc_srdriver.17.18.01.SPA.pkg
491525 -rw- 78484428   Jul 31 2025 11:49:35 -07:00 cat9k-espbase.17.18.01.SPA.pkg
491526 -rw- 1598412    Jul 31 2025 11:49:35 -07:00 cat9k-guestshell.17.18.01.SPA.pkg
491527 -rw- 404153288  Jul 31 2025 11:49:47 -07:00 cat9k-rpbase.17.18.01.SPA.pkg
491533 -rw- 31657374   Jul 31 2025 11:50:09 -07:00 cat9k-rpboot.17.18.01.SPA.pkg
491528 -rw- 27681740   Jul 31 2025 11:49:48 -07:00 cat9k-sipbase.17.18.01.SPA.pkg
491529 -rw- 52224968   Jul 31 2025 11:49:49 -07:00 cat9k-sipspa.17.18.01.SPA.pkg
491530 -rw- 31130572   Jul 31 2025 11:49:50 -07:00 cat9k-srdriver.17.18.01.SPA.pkg
491531 -rw- 14783432   Jul 31 2025 11:49:51 -07:00 cat9k-webui.17.18.01.SPA.pkg
491532 -rw- 9160       Jul 31 2025 11:49:51 -07:00 cat9k-wlc.17.18.01.SPA.pkg


11353194496 bytes total (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.17.18.01.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 Jul 31 2025 10:59:16 -07:00 packages.conf
516098 -rw- 7406 Jul 31 2025 10:58:08 -07:00 cat9k_iosxe.17.18.01.SPA.conf
11353194496 bytes total (8963174400 bytes free)
```

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

```
Switch# show version

Cisco IOS XE Software, Version 17.18.01
Cisco IOS Software, Catalyst L3 Switch Software (CAT9K_IOSXE), Version 17.18.1, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2025 by Cisco Systems, Inc.
<output truncated>
```

Downgrading in Install Mode

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

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

When downgrading from ...	Use these commands...	To downgrade to...
Cisco IOS XE 17.18.x	Either **install** commands or **request platform software** command[6].	Cisco IOS XE 17.17.x or earlier releases.

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

Note

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

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

Microcode Downgrade Prerequisite:

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

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

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

Step 1 Clean-up

install remove inactive

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

Step 2 Copy new image to flash

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

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

b) **dir flash:**

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

Step 3 Set boot variable

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

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

b) **no boot manual**

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

c) **write memory**

Use this command to save boot settings.

d) **show boot**

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

Step 4 Downgrade software image

install add file activate commit

Use this command to install the image.

We recommend that you point to the source image on your TFTP server or the flash drive of the *active* switch, if you have copied the image to flash memory. If you point to an image on the flash or USB drive of a member switch (instead of the active), you must specify the exact flash or USB drive - otherwise installation fails. For example, if the image is

on the flash drive of member switch 3 (flash-3): `Switch# install add file flash-3:cat9k_iosxe.17.17.01.SPA.bin activate commit`.

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

Step 5 Verify version

show version

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

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

Example

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

```
Switch# install remove inactive

install_remove: START Thu Jul 31 10:34:24 PDT 2025
install_remove: Removing IMG
Cleaning up unnecessary package files
No path specified, will use booted path /flash/packages.conf

Cleaning /flash
Scanning boot directory for packages ... done.
Preparing packages list to delete ...
[R0]: /flash/packages.conf File is in use, will not delete.
[R1]: /flash/packages.conf File is in use, will not delete.
[R0]: /flash/cat9k-cc_srdriver.17.18.01.SPA.pkg File is in use, will not delete.
[R1]: /flash/cat9k-cc_srdriver.17.18.01.SPA.pkg File is in use, will not delete.
[R0]: /flash/cat9k-espbase.17.18.01.SPA.pkg File is in use, will not delete.
[R1]: /flash/cat9k-espbase.17.18.01.SPA.pkg File is in use, will not delete.
[R0]: /flash/cat9k-guestshell.17.18.01.SPA.pkg File is in use, will not delete.
[R1]: /flash/cat9k-guestshell.17.18.01.SPA.pkg File is in use, will not delete.
[R0]: /flash/cat9k-lni.17.18.01.SPA.pkg File is in use, will not delete.
[R1]: /flash/cat9k-lni.17.18.01.SPA.pkg File is in use, will not delete.
[R0]: /flash/cat9k-rpbase.17.18.01.SPA.pkg File is in use, will not delete.
[R1]: /flash/cat9k-rpbase.17.18.01.SPA.pkg File is in use, will not delete.
[R0]: /flash/cat9k-sipbase.17.18.01.SPA.pkg File is in use, will not delete.
[R1]: /flash/cat9k-sipbase.17.18.01.SPA.pkg File is in use, will not delete.
[R0]: /flash/cat9k-sipspa.17.18.01.SPA.pkg File is in use, will not delete.
[R1]: /flash/cat9k-sipspa.17.18.01.SPA.pkg File is in use, will not delete.
[R0]: /flash/cat9k-srdriver.17.18.01.SPA.pkg File is in use, will not delete.
[R1]: /flash/cat9k-srdriver.17.18.01.SPA.pkg File is in use, will not delete.
[R0]: /flash/cat9k-webui.17.18.01.SPA.pkg File is in use, will not delete.
[R1]: /flash/cat9k-webui.17.18.01.SPA.pkg File is in use, will not delete.
[R0]: /flash/cat9k-wlc.17.18.01.SPA.pkg File is in use, will not delete.
[R1]: /flash/cat9k-wlc.17.18.01.SPA.pkg File is in use, will not delete.
[R0]: /flash/cat9k_iosxe.17.18.01.SPA.conf File is in use, will not delete.
[R1]: /flash/cat9k_iosxe.17.18.01.SPA.conf File is in use, will not delete.
[R0]: /flash/cat9k-rpboot.17.18.01.SPA.pkg File is in use, will not delete.
[R1]: /flash/cat9k-rpboot.17.18.01.SPA.pkg File is in use, will not delete.

The following files will be deleted:
[R0]: /flash/cat9k_iosxe.17.18.01.SPA.bin
[R1]: /flash/cat9k_iosxe.17.18.01.SPA.bin
[R0]: /flash/cat9k-cc_srdriver.17.09.02.SPA.pkg
```

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

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

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

--- Starting Post_Remove_Cleanup ---
Performing REMOVE_POSTCHECK on all members
Finished Post_Remove_Cleanup
SUCCESS: install_remove Thu Jul 31 10:34:32 PDT 2025

Switch# copy tftp://10.8.0.6/image/cat9k_iosxe.17.17.01.SPA.bin flash:
Destination filename [cat9k_iosxe.17.17.01.SPA.bin]?
Accessing tftp://10.8.0.6//cat9k_iosxe.17.17.01.SPA.bin...
Loading /cat9k_iosxe.17.17.01.SPA.bin from 10.8.0.6 (via GigabitEthernet0/0):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 508584771 bytes]
508584771 bytes copied in 101.005 secs (5035244 bytes/sec)


Switch# dir flash:*.bin

Directory of flash:/*.bin

Directory of flash:/

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

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

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

Switch# write memory

Switch# show boot

Current Boot Variables:
BOOT variable = flash:packages.conf;

Boot Variables on next reload:
BOOT variable = flash:packages.conf;
Manual Boot = no
Enable Break = yes
Boot Mode = DEVICE
iPXE Timeout = 0
```

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

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

install_add_activate_commit: START Thu Jul 31 10:55:53 PDT 2025
install_add: START Thu Jul 31 10:55:53 PDT 2025
install_add: Adding IMG
 [2] Switch 2 Warning!!! Image is being downgraded from 17.18.01.0.1186 to 17.17.01.0.1444.
--- Starting initial file syncing ---
Copying flash:cat9k_iosxe.17.17.01.SPA.bin from Switch 1 to Switch 1 2
Info: Finished copying to the selected Switch
Finished initial file syncing

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

Finished Add

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

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

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

```
Activate: Passed on [1 2]
Finished Activate

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

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



Initializing Hardware......

System Bootstrap, Version 17.18.1r[FC1], RELEASE SOFTWARE (P)
Compiled Wed 02/08/2025 14:36:07.63 by rel

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

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


Waiting for 120 seconds for other switches to boot

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

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

```
Switch# show version

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

Upgrading the ROMMON

To know the ROMMON or bootloader version that applies to every major and maintenance release, see ROMMON Versions, on page 16.

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 switch stack, perform the upgrade on the active switch and all members of the stack.

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.

Scaling Information

For information about feature scaling guidelines, see the Cisco Catalyst 9300 Series Switches datasheet at:

http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/datasheet-c78-738977.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 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 9300 Series Switches, visit Cisco Catalyst 9300 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 9300 Series Switches is at this URL: https://www.cisco.com/c/en/us/products/switches/catalyst-9300-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.