



## **Release Notes for Cisco Catalyst 9600 Series Switches, Cisco IOS XE Dublin 17.12.x**

**First Published:** 2023-07-28

**Last Modified:** 2024-03-22

### **Americas Headquarters**

Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
<http://www.cisco.com>  
Tel: 408 526-4000  
800 553-NETS (6387)  
Fax: 408 527-0883



# CONTENTS

---

**CHAPTER 1**

**Introduction 1**

Supported Hardware 1

Cisco Catalyst 9600 Series Switches—Model Numbers 1

Supported Hardware on Cisco Catalyst 9600 Series Switches 2

Optics Modules 4

---

**CHAPTER 2**

**What's New in Cisco IOS XE Dublin 17.12.x 5**

Hardware Features in Cisco IOS XE Dublin 17.12.3 5

Software Features in Cisco IOS XE Dublin 17.12.3 5

Hardware and Software Behavior Changes in Cisco IOS XE Dublin 17.12.3 5

Hardware Features in Cisco IOS XE Dublin 17.12.2 5

Software Features in Cisco IOS XE Dublin 17.12.2 6

Hardware and Software Behavior Changes in Cisco IOS XE Dublin 17.12.2 6

Hardware Features in Cisco IOS XE Dublin 17.12.1 6

Software Features in Cisco IOS XE Dublin 17.12.1 7

Hardware and Software Behavior Changes in Cisco IOS XE Dublin 17.12.1 9

---

**CHAPTER 3**

**Important Notes 11**

Important Notes 11

---

**CHAPTER 4**

**Compatibility Matrix and Web UI System Requirements 17**

Compatibility Matrix 17

Web UI System Requirements 24

---

<b>CHAPTER 5</b>	<b>Licensing and Scaling Guidelines</b>	<b>27</b>
	Licensing	27
	License Levels	27
	Available Licensing Models and Configuration Information	27
	License Levels - Usage Guidelines	28
	Scaling Guidelines	28

---

<b>CHAPTER 6</b>	<b>Limitations and Restrictions</b>	<b>29</b>
	Limitations and Restrictions	29

---

<b>CHAPTER 7</b>	<b>ROMMON Versions</b>	<b>33</b>
	ROMMON Versions	33

---

<b>CHAPTER 8</b>	<b>Upgrading the Switch Software</b>	<b>35</b>
	Finding the Software Version	35
	Software Images	35
	Upgrading the ROMMON	36
	Software Installation Commands	36
	Upgrading in Install Mode	37
	Downgrading in Install Mode	42
	Field-Programmable Gate Array Version Upgrade	47

---

<b>CHAPTER 9</b>	<b>Caveats</b>	<b>49</b>
	Cisco Bug Search Tool	49
	Open Caveats in Cisco IOS XE Dublin 17.12.x	49
	Resolved Caveats in Cisco IOS XE Dublin 17.12.3	50
	Resolved Caveats in Cisco IOS XE Dublin 17.12.2	50
	Resolved Caveats in Cisco IOS XE Dublin 17.12.1	50

---

<b>CHAPTER 10</b>	<b>Additional Information</b>	<b>51</b>
	Troubleshooting	51
	Related Documentation	51

Communications, Services, and Additional Information 51



# CHAPTER 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 Hardware, on page 1](#)

## Supported Hardware

### Cisco Catalyst 9600 Series Switches—Model Numbers

The following table lists the supported switch models. For information about the available license levels, see section *License Levels*.

Switch Model (append with "=" for spares)	Description
C9606R	Cisco Catalyst 9606R Switch <ul style="list-style-type: none"><li>• Redundant supervisor module capability</li><li>• Four linecard slots</li><li>• Hot-swappable fan tray, front and rear serviceable, fan tray assembly with 9 fans.</li><li>• Four power supply module slots</li></ul>

## Supported Hardware on Cisco Catalyst 9600 Series Switches

Product ID (append with "=" for spares)	Description
<b>Supervisor Modules</b>	
C9600-SUP-1	Cisco Catalyst 9600 Series Supervisor 1 Module This supervisor module is supported on the C9606R chassis.
C9600X-SUP-2	Cisco Catalyst 9600 Series Supervisor Engine 2 This supervisor module is supported on the C9606R chassis.
<b>SATA<sup>1</sup> SSD<sup>2</sup> Modules (for the Supervisor)</b>	
C9K-F2-SSD-240GB	Cisco Catalyst 9600 Series 240GB SSD Storage
C9K-F2-SSD-480GB	Cisco Catalyst 9600 Series 480GB SSD Storage
C9K-F2-SSD-960GB	Cisco Catalyst 9600 Series 960GB SSD Storage
<b>Line Cards</b>	
C9600X-LC-32CD	Cisco Catalyst 9600 Series 30-Port QSFP28, 2-Port QSFP-DD line card. <ul style="list-style-type: none"> <li>• C9600X-SUP-2 <ul style="list-style-type: none"> <li>• 30 QSFP28 ports of 100G/40G</li> <li>• 2 QSFP-DD ports of 400G/200G/100G/40G</li> </ul> </li> <li>• C9600-SUP-1 <ul style="list-style-type: none"> <li>• Not supported</li> </ul> </li> </ul>
C9600-LC-40YL4CD	Cisco Catalyst 9600 Series 40-Port SFP56, 2-Port QSFP56, 2-Port QSFP-DD line card. <ul style="list-style-type: none"> <li>• C9600X-SUP-2 <ul style="list-style-type: none"> <li>• 40 SFP56 ports of 50G/25G/10G</li> <li>• 2 QSFP56 ports of 200G/100G/40G</li> <li>• 2 QSFP-DD ports of 400G/200G/100G/40G</li> </ul> </li> <li>• C9600X-SUP-1 <ul style="list-style-type: none"> <li>• 40 SFP28 ports of 25G/10G/1G</li> <li>• 2 QSFP28 ports of 100G/40G</li> </ul> </li> </ul>

<b>Product ID</b> (append with "=" for spares)	<b>Description</b>
C9600-LC-48YL	Cisco Catalyst 9600 Series 48-Port SFP56 line card. <ul style="list-style-type: none"> <li>• C9600X-SUP-2 <ul style="list-style-type: none"> <li>• 48 SFP56 ports of 50G/25G/10G</li> </ul> </li> <li>• C9600X-SUP-1 <ul style="list-style-type: none"> <li>• 48 SFP28 ports of 25G/10G/1G</li> </ul> </li> </ul>
C9600-LC-24C	Cisco Catalyst 9600 Series 24-Port 40G/12-Port 100G line card. <ul style="list-style-type: none"> <li>• C9600X-SUP-2 <ul style="list-style-type: none"> <li>• 24 QSFP28 ports of 100G/40G</li> </ul> </li> <li>• C9600-SUP-1 <ul style="list-style-type: none"> <li>• 12 ports of 100G or 24 ports of 40G</li> </ul> </li> </ul>
C9600-LC-48TX	Cisco Catalyst 9600 Series 48-Port MultiGigabit RJ45 line card. <ul style="list-style-type: none"> <li>• C9600X-SUP-2 <ul style="list-style-type: none"> <li>• 48 ports of 10G/5G/2.5G</li> </ul> </li> <li>• C9600X-SUP-1 <ul style="list-style-type: none"> <li>• 48 ports of 10G/5G/2.5G/1G and 100M/10M</li> </ul> </li> </ul>
C9600-LC-48S	Cisco Catalyst 9600 Series 48-Port SFP line card. <ul style="list-style-type: none"> <li>• C9600X-SUP-2 <ul style="list-style-type: none"> <li>• Not supported</li> </ul> </li> <li>• C9600-SUP-1 <ul style="list-style-type: none"> <li>• 48 SFP ports of 1G</li> </ul> </li> </ul>
<b>AC Power Supply Modules</b>	
C9600-PWR-2KWAC	Cisco Catalyst 9600 Series 2000W AC Power Supply Module <sup>3</sup>
C9600-PWR-3KWAC	Cisco Catalyst 9600 Series 3000W AC Power Supply Module
<b>DC Power Supply Modules</b>	
C9600-PWR-2KWDC	Cisco Catalyst 9600 Series 2000W DC Power Supply Module

<sup>1</sup> Serial Advanced Technology Attachment (SATA)

- <sup>2</sup> Solid State Drive (SSD) Module
- <sup>3</sup> Power supply output capacity is 1050W at 110 VAC.

## 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](https://www.cisco.com/en/US/products/hw/modules/ps5455/products_device_support_tables_list.html)





## CHAPTER 2

# What's New in Cisco IOS XE Dublin 17.12.x

---

- [Hardware Features in Cisco IOS XE Dublin 17.12.3, on page 5](#)
- [Software Features in Cisco IOS XE Dublin 17.12.3, on page 5](#)
- [Hardware and Software Behavior Changes in Cisco IOS XE Dublin 17.12.3, on page 5](#)
- [Hardware Features in Cisco IOS XE Dublin 17.12.2, on page 5](#)
- [Software Features in Cisco IOS XE Dublin 17.12.2, on page 6](#)
- [Hardware and Software Behavior Changes in Cisco IOS XE Dublin 17.12.2, on page 6](#)
- [Hardware Features in Cisco IOS XE Dublin 17.12.1, on page 6](#)
- [Software Features in Cisco IOS XE Dublin 17.12.1, on page 7](#)
- [Hardware and Software Behavior Changes in Cisco IOS XE Dublin 17.12.1, on page 9](#)

## Hardware Features in Cisco IOS XE Dublin 17.12.3

There are no new hardware features in this release.

## Software Features in Cisco IOS XE Dublin 17.12.3

There are no new software features in this release.

## Hardware and Software Behavior Changes in Cisco IOS XE Dublin 17.12.3

There are no behavior changes in this release.

## Hardware Features in Cisco IOS XE Dublin 17.12.2

There are no new hardware features in this release.

## Software Features in Cisco IOS XE Dublin 17.12.2

There are no new software features in this release.

## Hardware and Software Behavior Changes in Cisco IOS XE Dublin 17.12.2

There are no behavior changes in this release.

## Hardware Features in Cisco IOS XE Dublin 17.12.1

Feature Name	Description
Cisco 100GBASE QSFP-100G Modules	<p>Supported transceiver module product numbers:</p> <ul style="list-style-type: none"> <li>• QSFP-100G-SR1.2</li> </ul> <p>Compatible line cards:</p> <ul style="list-style-type: none"> <li>• C9600-LC-24C, C9600-LC-40YL4CD and C9600X-LC-32CD line cards on Cisco Catalyst 9600X Supervisor Module 2 (C9600X-SUP-2)</li> <li>• C9600-LC-24C and C9600-LC-40YL4CD line cards on Cisco Catalyst 9600 Supervisor Module 1 (C9600-SUP-1)</li> </ul> <p>For information about the modules, see <a href="#">Cisco 100GBASE QSFP-100G Modules Data Sheet</a>. For information about device compatibility, see the <a href="#">Transceiver Module Group (TMG) Compatibility Matrix</a>.</p>
	<p>Supported transceiver module product numbers:</p> <ul style="list-style-type: none"> <li>• QSFP-100G-ZR4-S</li> </ul> <p>Compatible line cards:</p> <ul style="list-style-type: none"> <li>• C9600-LC-24C, C9600-LC-40YL4CD and C9600X-LC-32CD line cards on Cisco Catalyst 9600X Supervisor Module 2 (C9600X-SUP-2)</li> </ul> <p>For information about the modules, see <a href="#">Cisco 100GBASE QSFP-100G Modules Data Sheet</a>. For information about device compatibility, see the <a href="#">Transceiver Module Group (TMG) Compatibility Matrix</a>.</p>

## Software Features in Cisco IOS XE Dublin 17.12.1

Feature Name	Description
BGP EVPN VXLAN <ul style="list-style-type: none"> <li>• ARP inspection and DHCP Rogue Server Protection in VXLAN Environment (L2 VNIs)</li> <li>• BGP EVPN VRF Auto RD and Auto RT</li> </ul>	<p>The following BGP EVPN VXLAN features are introduced in this release:</p> <ul style="list-style-type: none"> <li>• ARP inspection and DHCP Rogue Server Protection in VXLAN Environment (L2 VNIs): BGP EVPN VXLAN fabric now supports ARP inspection and DHCP Rogue Server Protection. To configure these features, enable ARP inspection and DHCP Snooping on the VTEPs of the EVPN VXLAN fabric.</li> <li>• BGP EVPN VRF Auto RD and Auto RT: BGP EVPN Layer 3 overlay VRF configuration is simplified with the introduction of new CLIs to auto generate the route distinguisher (RD) and route target (RT) for a VRF.</li> </ul> <p>You can enable the auto generation of RD either at a global level, using the <b>vrf rd-auto</b> command or specifically for a VRF, using the <b>rd-auto [disable]</b> command in the VRF submenu.</p> <p>To enable auto assignment of RT for a VRF, use the <b>vniid vni-id</b> command in the VRF submenu.</p> <p>You can also choose to disable the auto RD and RT features by using the <b>no</b> form of the command.</p>
DSCP marking for RADIUS packets for administrative sessions	Allows you to configure DSCP marking for RADIUS packets for administrative sessions such as SSH and Telnet.
Interface ID Option in DHCPv6 Relay Message	Introduces support for interface ID option in DHCPv6 Relay message. With this, the physical interface details of the client interface are included along with the VLAN number in the message.
Interface Template Support for IPv6 DHCP Guard	Enables you to add the <b>ipv6 dhcp guard attach-policy policy_name</b> global configuration command to an interface template. IPv6 DHCP Guard is then enabled and the policy is applied, wherever the template is applied.
IP DHCP Server Changes to Limit IP Assignment to Next Hop only	Allows you to assign DHCP IP address only to the neighbouring device in an interface using the <b>ip dhcp restrict next hop</b> command. When this command is enabled, the DHCP server in the interface uses the MAC addresses in the DHCP packet and compares it with the addresses in the Cisco Discovery Protocol (CDP) or Link Layer Discovery Protocol (LLDP) cache table. If the MAC addresses match, then the DHCP IP address is assigned to that device.

Feature Name	Description
Modified Trustpoints for Secure Unique Device Identity (SUDI) Certificates	<p>Starting from Cisco IOS XE Dublin 17.12.1, the following changes have been introduced for trustpoints.</p> <ul style="list-style-type: none"> <li>Trustpoint names for existing SUDI certificates</li> </ul> <p>If your device supports Cisco Manufacturing CA III certificate and is not disabled, the trustpoint names are as follows.</p> <ul style="list-style-type: none"> <li>For <i>Cisco Manufacturing CA III</i> certificate, the trustpoint name has changed from CISCO_IDEVID_SUDI to CISCO_IDEVID_CMCA3_SUDI</li> <li>For <i>Cisco Manufacturing CA SHA2</i> certificate, the trustpoint name has changed from CISCO_IDEVID_SUDI_LEGACY to CISCO_IDEVID_CMCA2_SUDI</li> </ul> <p>If your device does not support Cisco Manufacturing CA III certificate or if the certificate is disabled using <b>no platform sudi cmca3</b> command, the trustpoint names are as follows.</p> <ul style="list-style-type: none"> <li>For <i>Cisco Manufacturing CA SHA2</i> certificate, the trustpoint name has changed from CISCO_IDEVID_SUDI to CISCO_IDEVID_CMCA2_SUDI</li> <li>For <i>Cisco Manufacturing CA</i> certificate, the trustpoint name has changed from CISCO_IDEVID_SUDI_LEGACY to CISCO_IDEVID_CMCA_SUDI</li> </ul> <ul style="list-style-type: none"> <li>Hardware SUDI certificates           <ul style="list-style-type: none"> <li>If your device supports <i>High Assurance SUDI CA</i> certificate, this certificate is loaded under CISCO_IDEVID_SUDI trustpoint.</li> <li>If your device does not support <i>High Assurance SUDI CA</i> certificate, <i>ACT2 SUDI CA</i> certificate is loaded under CISCO_IDEVID_SUDI trustpoint.</li> </ul> </li> <li><b>show ip http server status</b> command output           <p>If you configure the trustpoint for the HTTP server as CISCO_IDEVID_SUDI, the output of <b>show ip http server status</b> command displays the operating trustpoint along with the configured trustpoint.</p> <p>The following example shows a sample output of <b>show ip http server status</b> command with both the configured and the operating trustpoint names. Note that if your device does not support Cisco Manufacturing CA III certificate or if the certificate is disabled, the operating trustpoint in the below output displays CISCO_IDEVID_CMCA2_SUDI.</p> <pre>Device# show ip http server status ... HTTP secure server trustpoint: CISCO_IDEVID_SUDI HTTP secure server operating trustpoint: CISCO_IDEVID_CMCA3_SUDI</pre> </li> </ul>
Optimized Layer 2 Overlay Multicast for IPv4 and IPv6 traffic	<p>Optimized Layer 2 Overlay Multicast forwards multicast traffic within the Layer 2 Virtual Network Instance (L2VNI).</p> <p>Support for optimized Layer 2 overlay multicast was introduced on the Cisco Catalyst Series Supervisor 2 Module (C9600X-SUP-2).</p>

Feature Name	Description
Programmability: <ul style="list-style-type: none"> <li>• NETCONF-SSH Algorithms</li> <li>• YANG Data Models</li> </ul>	The following programmability features are introduced in this release: <ul style="list-style-type: none"> <li>• NETCONF-SSH Algorithms: The NETCONF-SSH server configuration file contains the list of all supported algorithms. From this release onwards, you can enable or disable these algorithms at runtime by using Cisco IOS commands or YANG models.</li> <li>• YANG Data Models: For the list of Cisco IOS XE YANG models available with this release, navigate to: <a href="https://github.com/YangModels/yang/tree/master/vendor/cisco/xe/17121">https://github.com/YangModels/yang/tree/master/vendor/cisco/xe/17121</a>.</li> </ul>
<b>show idprom tan</b> command	The <b>show idprom tan</b> command was introduced. It displays the top assembly part number and top assembly part revision number for the identification programmable read-only memory.

#### New on the WebUI

There are no new WebUI features in this release.

## Hardware and Software Behavior Changes in Cisco IOS XE Dublin 17.12.1

Behavior Change	Description
<b>ip mtu</b> command	On the C9600X-SUP-2 Supervisor Module, the <b>ip mtu</b> command has been modified to perform IPv4 and IPv6 fragmentation on the specified IP MTU value.
BDPU Guard and Root Guard Syslogs	The BDPU guard and root guard syslogs have been modified to include client bridge ID information.





## CHAPTER 3

# Important Notes

---

- [Important Notes, on page 11](#)

## Important Notes

- [Unsupported Features: All Models](#)
- [Unsupported Features: Cisco Catalyst 9600 Series Supervisor 2 Module](#)
- [Complete List of Supported Features](#)
- [Accessing Hidden Commands](#)
- [Default Behaviour](#)

### Unsupported Features: All Models

- **Network Management**
  - Cisco Application Visibility and Control (AVC)
- **Security**
  - IPsec VPN
  - MACsec switch-to-host connections in an overlay network.
- **System Management**
  - Network-Based Application Recognition (NBAR) and Next Generation NBAR (NBAR2)
- Network Load Balancing (NLB)

### Unsupported Features: Cisco Catalyst 9600 Series Supervisor 2 Module

- **BGP EVPN VXLAN**
  - Layer 2 Broadcast, Unknown Unicast, and Multicast (BUM) Traffic Forwarding using Ingress Replication
  - BUM Traffic Rate Limiting

- Dynamic ARP inspection (DAI) and DHCP Rogue Server Protection
  - EVPN VXLAN Centralized Default Gateway
  - VXLAN-Aware Flexible Netflow
  - MPLS Layer 3 VPN Border Leaf Handoff
  - MPLS Layer 3 VPN Border Spine Handoff
  - VPLS over MPLS Border Leaf Handoff
  - VPLS over MPLS Border Spine Handoff
  - Interworking of Layer 3 TRM with MVPN Networks for IPv4 Traffic
  - Private VLANs (PVLANS)
  - BGP EVPN VXLAN with IPv6 in the Underlay (VXLANv6)
  - EVPN Microsegmentation
  - VRF aware NAT64 EVPN Fabric
- **Cisco Trustsec**
    - Cisco TrustSec Meta Data Inline Tagging
    - Interface Scalable Group Tag (SGT) Tagging
    - Device SGT Tagging
    - Cisco TrustSec Manual Configuration
    - Cisco TrustSec Security Association Protocol (SAP)
    - Cisco TrustSec Metadata Header Encapsulation
    - SGT Mapping - Local Device SGT and VLAN-based SGT
    - IPv6 Support for SGT and SGACL
    - Cisco TrustSec SGT Caching
    - SGT Inline Tagging
- **High Availability**
    - Quad-Supervisor with Route Processor Redundancy
    - Secure StackWise Virtual
- **Interface and Hardware**
    - Per-port MTU
    - Link Debounce Timer
- **IP Addressing Services**
    - Next Hop Resolution Protocol (NHRP)



- Network Address Translation (NAT)
- Gateway Load Balancing Protocol (GLBP)
- Web Cache Communication Protocol (WCCP)
- Switchport Block Unknown Unicast and Switchport Block Unknown Multicast
- IPv6 over IPv4 GRE Tunnels
- Hot Standby Router Protocol (HSRP)
- Message Session Relay Protocol (MSRP)
- TCP MSS Adjustment
- WCCP IPv4
- GRE IPv6 Tunnels
- **IP Multicast Routing**
  - SDR Listener Support
  - Multicast Routing over GRE Tunnel
  - Multicast VLAN Registration (MVR) for IGMP Snooping
  - IPv6 Multicast over Point-to-Point GRE
  - IGMP Proxy
  - Bidirectional PIM
  - MLD Snooping
  - Multicast VPN
  - MVPNv6
  - mVPN Extranet Support
  - MLDP-Based VPN
  - PIM Snooping
  - PIM Dense Mode
- **IP Routing**
  - OSPFv2 Loop-Free Alternate IP Fast Reroute
  - EIGRP Loop-Free Alternate IP Fast Reroute
  - Policy-Based Routing (PBR)
  - Policy-Based Routing (PBR) for IPv6
  - VRF-Aware PBR
  - Local PBR

- PBR for Object-Group Access Control List (OGACL) Based Matching
- Multipoint GRE
- Web Cache Communication Protocol (WCCP)
- Unicast Reverse Path Forwarding (uRPF)
- Unicast and Multicast over Point-to-Multipoint GRE
  
- **Layer 2**
  - Multi-VLAN Registration Protocol (MVRP)
  - Loop Detection Guard
  
- **Multiprotocol Label Switching**
  - LAN MACsec over Multiprotocol Label Switching (MPLS)
  - BGP Multipath Load Sharing for Both eBGP and iBGP in an MPLS VPN
  - MPLS over GRE
  - MPLS Layer 2 VPN over GRE
  - MPLS Layer 3 VPN over GRE
  - Virtual Private LAN Service (VPLS)
  - VPLS Autodiscovery, BGP-based
  - VPLS Layer 2 Snooping: Internet Group Management Protocol or Multicast Listener Discovery
  - Hierarchical VPLS with MPLS Access
  - VPLS Routed Pseudowire IRB(v4) Unicast
  - MPLS VPN Inter-AS IPv4 BGP Label Distribution
  - Seamless Multiprotocol Label Switching
  
- **Network Management**
  - ERSPAN
  - Flow-Based Switch Port Analyser
  - FRSPAN
  - Ingress Forwarding
  - IP Aware MPLS Netflow
  - NetFlow Version 5
  - VPN ID
  
- **Security**
  - Lawful Intercept

- MACsec:
  - Cisco TrustSec MACsec
  - MACsec EAP-TLS
  - MACsec Downlink
  - The following are not supported on the C9600-LC-40YL4CD line card if used with the C9600X-SUP-2 supervisor:
    - Switch-to-host MACsec
    - Certificate-based MACsec
    - Cisco TrustSec SAP MACsec
  - MACsec is not supported on the C9600-LC-24C and C9600-LC-48YL line cards if used with the C9600X-SUP-2 supervisor
  - WAN MACsec is not supported on the C9600-LC-40YL4CD line card if used with the C9600-SUP-1 supervisor
- MAC ACLs
- Port ACLs
- VLAN ACLs
- IP Source Guard
- Web-based Authentication
- Port Security
- Weighted Random Early Detection mechanism (WRED) Based on DSCP, PREC, or COS
- IEEE 802.1x Port-Based Authentication
- Dynamic ARP Inspection
- Dynamic ARP Inspection Snooping
- **System Management**
  - Unicast MAC Address Filtering
- **VLAN**
  - Wired Dynamic PVLAN
  - Private VLANs

### Complete List of Supported Features

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

## 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 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.

---

## Default Behaviour

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).



# CHAPTER 4

## Compatibility Matrix and Web UI System Requirements

- [Compatibility Matrix](#), on page 17
- [Web UI System Requirements](#), on page 24

### Compatibility Matrix

The following table provides software compatibility information between Cisco Catalyst 9600 Series Switches, Cisco Identity Services Engine, Cisco Access Control Server, and Cisco Prime Infrastructure.

Catalyst 9600	Cisco Identity Services Engine	Cisco Access Control Server	Cisco Prime Infrastructure
Dublin 17.12.3	3.2 3.1 + Patch 3 3.0 + Patch 6 2.7 + Patch 7	-	PI 3.10 + PI 3.10 latest maintenance release + PI 3.10 latest device pack  See <a href="#">Cisco Prime Infrastructure 3.10</a> → <b>Downloads</b> .
Dublin 17.12.2	3.2 3.1 + Patch 3 3.0 + Patch 6 2.7 + Patch 7	-	PI 3.10 + PI 3.10 latest maintenance release + PI 3.10 latest device pack  See <a href="#">Cisco Prime Infrastructure 3.10</a> → <b>Downloads</b> .
Dublin 17.12.1	3.2 3.1 + Patch 3 3.0 + Patch 6 2.7 + Patch 7	-	PI 3.10 + PI 3.10 latest maintenance release + PI 3.10 latest device pack  See <a href="#">Cisco Prime Infrastructure 3.10</a> → <b>Downloads</b> .

Catalyst 9600	Cisco Identity Services Engine	Cisco Access Control Server	Cisco Prime Infrastructure
Dublin 17.11.1	3.2 3.1 + Patch 3 3.0 + Patch 6 2.7 + Patch 7	-	PI 3.10 + PI 3.10 latest maintenance release + PI 3.10 latest device pack  See <a href="#">Cisco Prime Infrastructure 3.10</a> → <b>Downloads.</b>
Dublin 17.10.1	3.2 3.1 + Patch 1 3.0 latest patch 2.7 latest patch 2.6 latest patch 2.4 latest patch	-	PI 3.10 + PI 3.10 latest maintenance release + PI 3.10 latest device pack  See <a href="#">Cisco Prime Infrastructure 3.10</a> → <b>Downloads.</b>
Cupertino 17.9.5	3.2 3.1 + Patch 1 3.0 latest patch 2.7 latest patch 2.6 latest patch 2.4 latest patch	-	PI 3.10 + PI 3.10 latest maintenance release + PI 3.10 latest device pack  See <a href="#">Cisco Prime Infrastructure 3.10</a> → <b>Downloads.</b>
Cupertino 17.9.4	3.2 3.1 + Patch 1 3.0 latest patch 2.7 latest patch 2.6 latest patch 2.4 latest patch	-	PI 3.10 + PI 3.10 latest maintenance release + PI 3.10 latest device pack  See <a href="#">Cisco Prime Infrastructure 3.10</a> → <b>Downloads.</b>
Cupertino 17.9.3	3.2 3.1 + Patch 1 3.0 latest patch 2.7 latest patch 2.6 latest patch 2.4 latest patch	-	PI 3.10 + PI 3.10 latest maintenance release + PI 3.10 latest device pack  See <a href="#">Cisco Prime Infrastructure 3.10</a> → <b>Downloads.</b>

<b>Catalyst 9600</b>	<b>Cisco Identity Services Engine</b>	<b>Cisco Access Control Server</b>	<b>Cisco Prime Infrastructure</b>
Cupertino 17.9.2	3.2 3.1 + Patch 1 3.0 latest patch 2.7 latest patch 2.6 latest patch 2.4 latest patch	-	PI 3.10 + PI 3.10 latest maintenance release + PI 3.10 latest device pack  See <a href="#">Cisco Prime Infrastructure 3.10</a> → <b>Downloads.</b>
Cupertino 17.9.1	3.2 3.1 + Patch 1 3.0 latest patch 2.7 latest patch 2.6 latest patch 2.4 latest patch	-	PI 3.10 + PI 3.10 latest maintenance release + PI 3.10 latest device pack  See <a href="#">Cisco Prime Infrastructure 3.10</a> → <b>Downloads.</b>
Cupertino 17.8.1	3.1 3.0 latest patch 2.7 latest patch 2.6 latest patch 2.4 latest patch	-	PI 3.10 + PI 3.10 latest maintenance release + PI 3.10 latest device pack  See <a href="#">Cisco Prime Infrastructure 3.10</a> → <b>Downloads.</b>
Cupertino 17.7.1	3.1 3.0 latest patch 2.7 latest patch 2.6 latest patch 2.4 latest patch	-	PI 3.10 + PI 3.10 latest maintenance release + PI 3.10 latest device pack  See <a href="#">Cisco Prime Infrastructure 3.10</a> → <b>Downloads.</b>
Bengaluru 17.6.7	3.1 3.0 latest patch 2.7 latest patch 2.6 latest patch 2.4 latest patch	-	PI 3.10 + PI 3.10 latest maintenance release + PI 3.10 latest device pack  See <a href="#">Cisco Prime Infrastructure 3.10</a> → <b>Downloads.</b>

Catalyst 9600	Cisco Identity Services Engine	Cisco Access Control Server	Cisco Prime Infrastructure
Bengaluru 17.6.6a	3.1 3.0 latest patch 2.7 latest patch 2.6 latest patch 2.4 latest patch	-	PI 3.10 + PI 3.10 latest maintenance release + PI 3.10 latest device pack  See <a href="#">Cisco Prime Infrastructure 3.10</a> → <b>Downloads.</b>
Bengaluru 17.6.6	3.1 3.0 latest patch 2.7 latest patch 2.6 latest patch 2.4 latest patch	-	PI 3.10 + PI 3.10 latest maintenance release + PI 3.10 latest device pack  See <a href="#">Cisco Prime Infrastructure 3.10</a> → <b>Downloads.</b>
Bengaluru 17.6.5	3.1 3.0 latest patch 2.7 latest patch 2.6 latest patch 2.4 latest patch	-	PI 3.10 + PI 3.10 latest maintenance release + PI 3.10 latest device pack  See <a href="#">Cisco Prime Infrastructure 3.10</a> → <b>Downloads.</b>
Bengaluru 17.6.4	3.1 3.0 latest patch 2.7 latest patch 2.6 latest patch 2.4 latest patch	-	PI 3.10 + PI 3.10 latest maintenance release + PI 3.10 latest device pack  See <a href="#">Cisco Prime Infrastructure 3.10</a> → <b>Downloads.</b>
Bengaluru 17.6.3	3.1 3.0 latest patch 2.7 latest patch 2.6 latest patch 2.4 latest patch	-	PI 3.10 + PI 3.10 latest maintenance release + PI 3.10 latest device pack  See <a href="#">Cisco Prime Infrastructure 3.10</a> → <b>Downloads.</b>
Bengaluru 17.6.2	3.1 3.0 latest patch 2.7 latest patch 2.6 latest patch 2.4 latest patch	-	PI 3.10 + PI 3.10 latest maintenance release + PI 3.10 latest device pack  See <a href="#">Cisco Prime Infrastructure 3.10</a> → <b>Downloads.</b>



Catalyst 9600	Cisco Identity Services Engine	Cisco Access Control Server	Cisco Prime Infrastructure
Bengaluru 17.6.1	3.1 3.0 latest patch 2.7 latest patch 2.6 latest patch 2.4 latest patch	-	PI 3.9 + PI 3.9 latest maintenance release + PI 3.9 latest device pack  See <a href="#">Cisco Prime Infrastructure 3.9</a> → <b>Downloads.</b>
Bengaluru 17.5.1	3.0 Patch 1 2.7 Patch 2 2.6 Patch 7 2.4 Patch 13	-	PI 3.9 + PI 3.9 latest maintenance release + PI 3.9 latest device pack  See <a href="#">Cisco Prime Infrastructure 3.9</a> → <b>Downloads.</b>
Bengaluru 17.4.1	3.0 2.7 Patch 2	-	PI 3.9 + PI 3.9 latest maintenance release + PI 3.9 latest device pack  See <a href="#">Cisco Prime Infrastructure 3.9</a> → <b>Downloads.</b>
Amsterdam 17.3.8a	2.7	-	PI 3.10 + PI 3.10 latest maintenance release + PI 3.10 latest device pack  See <a href="#">Cisco Prime Infrastructure 3.10</a> → <b>Downloads.</b>
Amsterdam 17.3.8	2.7	-	PI 3.10 + PI 3.10 latest maintenance release + PI 3.10 latest device pack  See <a href="#">Cisco Prime Infrastructure 3.10</a> → <b>Downloads.</b>
Amsterdam 17.3.7	2.7	-	PI 3.10 + PI 3.10 latest maintenance release + PI 3.10 latest device pack  See <a href="#">Cisco Prime Infrastructure 3.10</a> → <b>Downloads.</b>
Amsterdam 17.3.6	2.7	-	PI 3.10 + PI 3.10 latest maintenance release + PI 3.10 latest device pack  See <a href="#">Cisco Prime Infrastructure 3.10</a> → <b>Downloads.</b>
Amsterdam 17.3.5	2.7	-	PI 3.9 + PI 3.9 latest maintenance release + PI 3.9 latest device pack  See <a href="#">Cisco Prime Infrastructure 3.9</a> → <b>Downloads.</b>

Catalyst 9600	Cisco Identity Services Engine	Cisco Access Control Server	Cisco Prime Infrastructure
Amsterdam 17.3.4	2.7	-	PI 3.9 + PI 3.9 latest maintenance release + PI 3.9 latest device pack See <a href="#">Cisco Prime Infrastructure 3.9</a> → <b>Downloads.</b>
Amsterdam 17.3.3	2.7	-	PI 3.9 + PI 3.9 latest maintenance release + PI 3.9 latest device pack See <a href="#">Cisco Prime Infrastructure 3.9</a> → <b>Downloads.</b>
Amsterdam 17.3.2a	2.7	-	PI 3.8 + PI 3.8 latest maintenance release + PI 3.8 latest device pack See <a href="#">Cisco Prime Infrastructure 3.8</a> → <b>Downloads.</b>
Amsterdam 17.3.1	2.7	-	PI 3.8 + PI 3.8 latest maintenance release + PI 3.8 latest device pack See <a href="#">Cisco Prime Infrastructure 3.8</a> → <b>Downloads.</b>
Amsterdam 17.2.1	2.7	-	PI 3.7 + PI 3.7 latest maintenance release + PI 3.7 latest device pack See <a href="#">Cisco Prime Infrastructure 3.7</a> → <b>Downloads.</b>
Amsterdam 17.1.1	2.7	-	-
Gibraltar 16.12.8	2.6	-	-
Gibraltar 16.12.7	2.6	-	-
Gibraltar 16.12.6	2.6	-	-
Gibraltar 16.12.5b	2.6	-	-
Gibraltar 16.12.5	2.6	-	-
Gibraltar 16.12.4	2.6	-	-
Gibraltar 16.12.3a	2.6	-	-
Gibraltar 16.12.3	2.6	-	-
Gibraltar 16.12.2	2.6	-	-
Gibraltar 16.12.1	2.6	-	-

Catalyst 9600	Cisco Identity Services Engine	Cisco Access Control Server	Cisco Prime Infrastructure
Gibraltar 16.11.1	2.6 2.4 Patch 5	5.4 5.5	-
Gibraltar 16.10.1	2.3 Patch 1 2.4 Patch 1	5.4 5.5	PI 3.4 + PI 3.4 latest maintenance release + PI 3.4 latest device pack  See <a href="#">Cisco Prime Infrastructure 3.4</a> → <b>Downloads.</b>
Fuji 16.9.8	2.5 2.1	5.4 5.5	PI 3.9 + PI 3.9 latest maintenance release + PI 3.9 latest device pack  See <a href="#">Cisco Prime Infrastructure 3.9</a> → <b>Downloads.</b>
Fuji 16.9.7	2.5 2.1	5.4 5.5	PI 3.9 + PI 3.9 latest maintenance release + PI 3.9 latest device pack  See <a href="#">Cisco Prime Infrastructure 3.9</a> → <b>Downloads.</b>
Fuji 16.9.6	2.3 Patch 1 2.4 Patch 1	5.4 5.5	PI 3.4 + PI 3.4 latest maintenance release + PI 3.4 latest device pack  See <a href="#">Cisco Prime Infrastructure 3.4</a> → <b>Downloads.</b>
Fuji 16.9.5	2.3 Patch 1 2.4 Patch 1	5.4 5.5	PI 3.4 + PI 3.4 latest maintenance release + PI 3.4 latest device pack  See <a href="#">Cisco Prime Infrastructure 3.4</a> → <b>Downloads.</b>
Fuji 16.9.4	2.3 Patch 1 2.4 Patch 1	5.4 5.5	PI 3.4 + PI 3.4 latest maintenance release + PI 3.4 latest device pack  See <a href="#">Cisco Prime Infrastructure 3.4</a> → <b>Downloads.</b>
Fuji 16.8.1a	2.3 Patch 1 2.4	5.4 5.5	PI 3.3 + PI 3.3 latest maintenance release + PI 3.3 latest device pack  See <a href="#">Cisco Prime Infrastructure 3.3</a> → <b>Downloads.</b>
Everest 16.6.4a	2.2 2.3	5.4 5.5	PI 3.1.6 + Device Pack 13  See <a href="#">Cisco Prime Infrastructure 3.1</a> → <b>Downloads.</b>

Catalyst 9600	Cisco Identity Services Engine	Cisco Access Control Server	Cisco Prime Infrastructure
Everest 16.6.4	2.2 2.3	5.4 5.5	PI 3.1.6 + Device Pack 13 See <a href="#">Cisco Prime Infrastructure 3.1</a> → <b>Downloads</b> .
Everest 16.6.3	2.2 2.3	5.4 5.5	PI 3.1.6 + Device Pack 13 See <a href="#">Cisco Prime Infrastructure 3.1</a> → <b>Downloads</b>
Everest 16.6.2	2.2 2.3	5.4 5.5	PI 3.1.6 + Device Pack 13 See <a href="#">Cisco Prime Infrastructure 3.1</a> → <b>Downloads</b>
Everest 16.6.1	2.2	5.4 5.5	PI 3.1.6 + Device Pack 13 See <a href="#">Cisco Prime Infrastructure 3.1</a> → <b>Downloads</b>
Everest 16.5.1a	2.1 Patch 3	5.4 5.5	-

## Web UI System Requirements

The following subsections list the hardware and software required to access the Web UI:

### Minimum Hardware Requirements

Processor Speed	DRAM	Number of Colors	Resolution	Font Size
233 MHz minimum <sup>4</sup>	512 MB <sup>5</sup>	256	1280 x 800 or higher	Small

<sup>4</sup> We recommend 1 GHz

<sup>5</sup> We recommend 1 GB DRAM

### Software Requirements

#### Operating Systems

- Windows 10 or later
- Mac OS X 10.9.5 or later

#### Browsers

- Google Chrome—Version 59 or later (On Windows and Mac)
- Microsoft Edge

- Mozilla Firefox—Version 54 or later (On Windows and Mac)
- Safari—Version 10 or later (On Mac)





## CHAPTER 5

# Licensing and Scaling Guidelines

---

- [Licensing, on page 27](#)
- [Scaling Guidelines, on page 28](#)

## Licensing

This section provides information about the licensing packages for features available on Cisco Catalyst 9000 Series Switches.

## License Levels

The software features available on Cisco Catalyst 9600 Series Switches fall under these base or add-on license levels.

### Base Licenses

- Network Advantage

### Add-On Licenses

Add-On Licenses require a Network Essentials or Network Advantage as a pre-requisite. The features available with add-on license levels provide Cisco innovations on the switch, as well as on the Cisco Digital Network Architecture Center (Cisco DNA Center).

- DNA Advantage

To find information about platform support and to know which license levels a feature is available with, use Cisco Feature Navigator. To access Cisco Feature Navigator, go to <https://cfng.cisco.com>. An account on cisco.com is not required.

## 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.

In the [software configuration guide](#) of the required release, see **System Management** → **Configuring Smart Licensing**.

- 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.

In the [software configuration guide](#) of the required release (17.3.x onwards), see **System Management** → **Smart Licensing Using Policy**.

For a more detailed overview on Cisco Licensing, go to [cisco.com/go/licensingguide](https://cisco.com/go/licensingguide).

## License Levels - Usage Guidelines

- The duration or term for which a purchased license is valid:

Smart Licensing Using Policy	Smart Licensing
<ul style="list-style-type: none"> <li>• Perpetual: There is no expiration date for such a license.</li> <li>• Subscription: The license is valid only until a certain date (for a three, five, or seven year period).</li> </ul>	<ul style="list-style-type: none"> <li>• Permanent: for a license level, and without an expiration date.</li> <li>• Term: for a license level, and for a three, five, or seven year period.</li> <li>• Evaluation: a license that is not registered.</li> </ul>

- Base licenses (Network-Advantage) are ordered and fulfilled only with a perpetual or permanent license type.
- Add-on licenses (DNA Advantage) are ordered and fulfilled only with a subscription or term license type.
- An add-on license level is included when you choose a network license level. If you use DNA features, renew the license before term expiry, to continue using it, or deactivate the add-on license and then reload the switch to continue operating with the base license capabilities.
- Evaluation licenses cannot be ordered. They are not tracked via Cisco Smart Software Manager and expire after a 90-day period. Evaluation licenses can be used only once on the switch and cannot be regenerated. Warning system messages about an evaluation license expiry are generated only 275 days after expiration and every week thereafter. An expired evaluation license cannot be reactivated after reload. This applies only to *Smart Licensing*. The notion of evaluation licenses does not apply to *Smart Licensing Using Policy*.

## Scaling Guidelines

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>





## CHAPTER 6

# Limitations and Restrictions

- [Limitations and Restrictions](#), on page 29

## 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 run** 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.
- Cisco Catalyst 9600 Series Supervisor 2 Module (C9600X-SUP-2) on a C9606R chassis does not support Quad-Supervisor with RPR.
- 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 18.x ), ISSU is supported between any two EMs that are released not more than 3 years apart.
  - Within a major release train, ISSU is supported from:
    - Any EM (EM1, EM2, EM3) to another EM (EM1, EM2, EM3)  
Example: 16.9.x to 16.12.x, 17.3.x to 17.6.x, 17.6.x to 17.9.x
    - Any release within the same EM  
Example: 16.9.2 to 16.9.3 or 16.9.4 or 16.9.x, 16.12.1 to 16.12.2 or 16.12.3 or 16.12.x, 17.3.1 to 17.3.2 or 17.3.3 or 17.3.x
  - Between major release trains, ISSU is not supported from:
    - An EM of a major release train to an EM of another major release train  
Example: 16.x.x to 17.x.x or 17.x.x to 18.x.x is not supported
    - An SM to EM or EM to SM  
Example: 16.10.x or 16.11.x to 16.12.x is not supported
  - ISSU is not supported on engineering special releases and .s (or similar) images.
  - ISSU is not supported between Licensed Data Payload Encryption (LDPE) and No Payload Encryption (NPE) Cisco IOS XE software images.
  - ISSU downgrades are not supported.
  - While 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
```

- Catalyst 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.





## CHAPTER 7

# ROMMON Versions

- [ROMMON Versions](#), on page 33

## 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.

The following table provides ROMMON version information for the Cisco Catalyst 9600 Series Supervisor Modules. 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)
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 17.9.4	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]

Release	ROMMON Version (C9600-SUP-1)	ROMMON Version (C9600X-SUP-2)
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	-
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]	-



## CHAPTER 8

# Upgrading the Switch Software

- [Finding the Software Version, on page 35](#)
- [Software Images, on page 35](#)
- [Upgrading the ROMMON, on page 36](#)
- [Software Installation Commands, on page 36](#)
- [Upgrading in Install Mode, on page 37](#)
- [Downgrading in Install Mode, on page 42](#)
- [Field-Programmable Gate Array Version Upgrade, on page 47](#)

## 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.

## Software Images

Release	Image Type	File Name
Cisco IOS XE Dublin 17.12.3	CAT9K_IOSXE	cat9k_iosxe.17.12.03.SPA.bin
	No Payload Encryption (NPE)	cat9k_iosxe_npe.17.12.03.SPA.bin
Cisco IOS XE Dublin 17.12.2	CAT9K_IOSXE	cat9k_iosxe.17.12.02.SPA.bin
	No Payload Encryption (NPE)	cat9k_iosxe_npe.17.12.02.SPA.bin

Release	Image Type	File Name
Cisco IOS XE Dublin 17.12.1	CAT9K_IOSXE	cat9k_iosxe.17.12.01.SPA.bin
	No Payload Encryption (NPE)	cat9k_iosxe_npe.17.12.01.SPA.bin

## Upgrading the ROMMON

To know the ROMMON or bootloader version that applies to every major and maintenance release, see [ROMMON Versions, on page 33](#).

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.

## Software Installation Commands

Summary of Software Installation Commands	
To install and activate the specified file, and to commit changes to be persistent across reloads:	
<b>install add file</b> <i>filename</i> [ <b>activate commit</b> ]	
To separately install, activate, commit, cancel, or remove the installation file: <b>install ?</b>	
<b>add file tftp:</b> <i>filename</i>	Copies the install file package from a remote location to the device and performs a compatibility check for the platform and image versions.



Summary of Software Installation Commands	
<b>activate</b> [ <b>auto-abort-timer</b> ]	Activates the file, and reloads the device. The <b>auto-abort-timer</b> keyword automatically rolls back image activation.
<b>commit</b>	Makes changes persistent over reloads.
<b>rollback to committed</b>	Rolls back the update to the last committed version.
<b>abort</b>	Cancels file activation, and rolls back to the version that was running before the current installation procedure started.
<b>remove</b>	Deletes all unused and inactive software installation files.

## 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**.

### Before you begin



**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 Dublin 17.11.x or earlier releases	Cisco IOS XE Dublin 17.12.x

The sample output in this section displays upgrade from Cisco IOS XE Dublin 17.11.1 to Cisco IOS XE Dublin 17.12.1 using **install** commands.

### Procedure

#### 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.

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 Mon Jul 24 19:51:48 UTC 2023
Cleaning up unnecessary package files
Scanning boot directory for packages ... done.
Preparing packages list to delete ...
  cat9k-cc_srdriver.17.11.01.SPA.pkg
    File is in use, will not delete.
  cat9k-espbase.17.11.01.SPA.pkg
    File is in use, will not delete.
  cat9k-guestshell.17.11.01.SPA.pkg
    File is in use, will not delete.
  cat9k-rpbase.17.11.01.SPA.pkg
    File is in use, will not delete.
  cat9k-rpboot.17.11.01.SPA.pkg
    File is in use, will not delete.
  cat9k-sipbase.17.11.01.SPA.pkg
    File is in use, will not delete.
  cat9k-sipspa.17.11.01.SPA.pkg
    File is in use, will not delete.
  cat9k-srdriver.17.11.01.SPA.pkg
    File is in use, will not delete.
  cat9k-webui.17.11.01.SPA.pkg
    File is in use, will not delete.
  cat9k-wlc.17.11.01.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.17.11.01.SPA.pkg
/flash/cat9k-espbase.17.11.01.SPA.pkg
/flash/cat9k-guestshell.17.11.01.SPA.pkg
/flash/cat9k-rpbase.17.11.01.SPA.pkg
/flash/cat9k-rpboot.17.11.01.SPA.pkg
/flash/cat9k-sipbase.17.11.01.SPA.pkg
/flash/cat9k-sipspa.17.11.01.SPA.pkg
/flash/cat9k-srdriver.17.11.01.SPA.pkg
/flash/cat9k-webui.17.11.01.SPA.pkg
/flash/cat9k-wlc.17.11.01.SPA.pkg
/flash/packages.conf

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

[switch 1]:
Deleting file flash:cat9k-cc_srdriver.17.11.01.SPA.pkg ... done.
Deleting file flash:cat9k-espbase.17.11.01.SPA.pkg ... done.
Deleting file flash:cat9k-guestshell.17.11.01.SPA.pkg ... done.
Deleting file flash:cat9k-rpbase.17.11.01.SPA.pkg ... done.
Deleting file flash:cat9k-rpboot.17.11.01.SPA.pkg ... done.
Deleting file flash:cat9k-sipbase.17.11.01.SPA.pkg ... done.
Deleting file flash:cat9k-sipspa.17.11.01.SPA.pkg ... done.
Deleting file flash:cat9k-srdriver.17.11.01.SPA.pkg ... done.
Deleting file flash:cat9k-webui.17.11.01.SPA.pkg ... done.
Deleting file flash:cat9k-wlc.17.11.01.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 Mon Jul 24 19:52:25 UTC 2023
Switch#
```

## Step 2 Copy new image to flash

### a) **copy tftp:[//location]/directory]/filenameflash:**

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.

```
Switch# copy tftp://10.8.0.6/image/cat9k_iosxe.17.12.01.SPA.bin flash:

destination filename [cat9k_iosxe.17.12.01.SPA.bin]?
Accessing tftp://10.8.0.6/image/cat9k_iosxe.17.12.01.SPA.bin...
Loading /cat9k_iosxe.17.12.01.SPA.bin from 10.8.0.6 (via GigabitEthernet0/0):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 601216545 bytes]

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

### b) **dir flash:\*.bin**

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

```
Switch# dir flash:*.bin

Directory of flash:/*.bin

Directory of flash:/

434184 -rw- 601216545 Jul 24 2023 10:18:11 -07:00 cat9k_iosxe.17.12.01.SPA.bin
11353194496 bytes total (8976625664 bytes free)
```

## Step 3 Set boot variable

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

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

```
Switch(config)# boot system 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.

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

### c) **write memory**

Use this command to save boot settings.

```
Switch# write memory
```

### d) **show bootvar**

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

```
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 =
```

#### 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 TFTP server or the flash , if you have copied the image to flash memory.

The following sample output displays installation of the Cisco IOS XE Dublin 17.12.1 software image to flash:

```
Switch# install add file flash:cat9k_iosxe.17.12.01.SPA.bin activate commit
_install_add_activate_commit: START Mon Jul 24 16:37:25 IST 2023

*Jul 24 16:37:26.544 IST: %INSTALL-5-INSTALL_START_INFO: R0/0: install_engine: Started
install one-shot flash:cat9k_iosxe.17.12.01.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.17.12.01.SPA.bin to standby
Info: Finished copying flash:cat9k_iosxe.17.12.01.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: 17.12.01

```
install_add_activate_commit: Activating PACKAGE
Following packages shall be activated:
/flash/cat9k-wlc.17.12.01.SPA.pkg
/flash/cat9k-webui.17.12.01.SPA.pkg
/flash/cat9k-srdriver.17.12.01.SPA.pkg
```

```

/flash/cat9k-sipsa.17.12.01.SPA.pkg
/flash/cat9k-sipbase.17.12.01.SPA.pkg
/flash/cat9k-rpboot.17.12.01.SPA.pkg
/flash/cat9k-rpbase.17.12.01.SPA.pkg
/flash/cat9k-guestshell.17.12.01.SPA.pkg
/flash/cat9k-espbase.17.12.01.SPA.pkg
/flash/cat9k-cc_srdriver.17.12.01.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

\*Jul 24 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

\*Jul 24 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 Mon Jul 24 16:46:18 IST 2023

**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**

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

```

Switch# dir flash:*.pkg
Directory of flash:/*.pkg
Directory of flash:/
475140 -rw- 2012104   Mar 9 2023 09:52:41 -07:00 cat9k-cc_srdriver.17.11.01.SPA.pkg
475141 -rw- 70333380  Mar 9 2023 09:52:44 -07:00 cat9k-espbase.17.11.01.SPA.pkg
475142 -rw- 13256      Mar 9 2023 09:52:44 -07:00 cat9k-guestshell.17.11.01.SPA.pkg
475143 -rw- 349635524   Mar 9 2023 09:52:54 -07:00 cat9k-rpbase.17.11.01.SPA.pkg
475149 -rw- 24248187    Mar 9 2023 09:53:02 -07:00 cat9k-rpboot.17.11.01.SPA.pkg
475144 -rw- 25285572   Mar 9 2023 09:52:55 -07:00 cat9k-sipbase.17.11.01.SPA.pkg
475145 -rw- 20947908  Mar 9 2023 09:52:55 -07:00 cat9k-sipsa.17.11.01.SPA.pkg
475146 -rw- 2962372   Mar 9 2023 09:52:56 -07:00 cat9k-srdriver.17.11.01.SPA.pkg
475147 -rw- 13284288  Mar 9 2023 09:52:56 -07:00 cat9k-webui.17.11.01.SPA.pkg
475148 -rw- 13248     Mar mar9 2023 09:52:56 -07:00 cat9k-wlc.17.11.01.SPA.pkg

491524 -rw- 25711568  Jul 24 2023 11:49:33 -07:00 cat9k-cc_srdriver.17.12.01.SPA.pkg
491525 -rw- 78484428 Jul 24 2023 11:49:35 -07:00 cat9k-espbase.17.12.01.SPA.pkg
491526 -rw- 1598412  Jul 24 2023 11:49:35 -07:00 cat9k-guestshell.17.12.01.SPA.pkg

```

```

491527 -rw- 404153288 Jul 24 2023 11:49:47 -07:00 cat9k-rpbase.17.12.01.SPA.pkg
491533 -rw- 31657374 Jul 24 2023 11:50:09 -07:00 cat9k-rpboot.17.12.01.SPA.pkg
491528 -rw- 27681740 Jul 24 2023 11:49:48 -07:00 cat9k-sipbase.17.12.01.SPA.pkg
491529 -rw- 52224968 Jul 24 2023 11:49:49 -07:00 cat9k-sipsa.17.12.01.SPA.pkg
491530 -rw- 31130572 Jul 24 2023 11:49:50 -07:00 cat9k-srdriver.17.12.01.SPA.pkg
491531 -rw- 14783432 Jul 24 2023 11:49:51 -07:00 cat9k-webui.17.12.01.SPA.pkg
491532 -rw- 9160 Jul 24 2023 11:49:51 -07:00 cat9k-wlc.17.12.01.SPA.pkg

```

```
11353194496 bytes total (8963174400 bytes free)
```

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

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.17.12.01.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 Jul 24 2023 05:39:42 +00:00 packages.conf
16634 -rw- 4882 Jul 24 2023 05:34:06 +00:00 cat9k_iosxe.17.12.01.SPA.conf

```

## Step 6 Verify version

### **show version**

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

The following sample output of the **show version** command displays the Cisco IOS XE Dublin 17.12.1 image on the device:

```
Switch# show version
```

```

Cisco IOS XE Software, Version 17.12.01
Cisco IOS Software [Dublin], Catalyst L3 Switch Software (CAT9K_IOSXE), Version 17.12.1,
RELEASE SOFTWARE (fcl)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2023 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**.

### **Before you begin**

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

When downgrading from ...	To ...
Cisco IOS XE Dublin 17.12.x	Cisco IOS XE Dublin 17.11.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.

The sample output in this section shows downgrade from Cisco IOS XE Dublin 17.12.1 to Cisco IOS XE Dublin 17.11.1, using **install** commands.

## Procedure

### 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.

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 Mon Jul 24 11:42:27 IST 2023

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.17.12.01.SSA.pkg
File is in use, will not delete.
cat9k-espbase.17.12.01.SSA.pkg
File is in use, will not delete.
cat9k-guestshell.17.12.01.SSA.pkg
File is in use, will not delete.
cat9k-rpbase.17.12.01.SSA.pkg
File is in use, will not delete.
cat9k-rpboot.17.12.01.SSA.pkg
File is in use, will not delete.
cat9k-sipbase.17.12.01.SSA.pkg
File is in use, will not delete.
cat9k-sipspa.17.12.01.SSA.pkg
File is in use, will not delete.
cat9k-srdriver.17.12.01.SSA.pkg
File is in use, will not delete.
cat9k-webui.17.12.01.SSA.pkg
File is in use, will not delete.
cat9k-wlc.17.12.01.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 Mon Jul 24 11:42:39 IST 2023

--- 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 Mon Jul 24 19:52:25 UTC 2023
Switch#

```

## Step 2 Copy new image to flash

### a) **copy tftp:[[/location]/directory]/filenameflash:**

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.

```

Switch# copy tftp://10.8.0.6/image/cat9k_iosxe.17.11.01.SPA.bin flash:
Destination filename [cat9k_iosxe.17.11.01.SPA.bin]?
Accessing tftp://10.8.0.6//cat9k_iosxe.17.11.01.SPA.bin...
Loading /cat9k_iosxe.17.11.01.SPA.bin from 10.8.0.6 (via GigabitEthernet0/0):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 508584771 bytes]
508584771 bytes copied in 101.005 secs (5035244 bytes/sec)

```

### b) **dir flash:**

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

```

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

Directory of flash:/

434184 -rw- 508584771 Jul 24 2023 13:35:16 -07:00 cat9k_iosxe.17.11.01.SPA.bin
11353194496 bytes total (9055866880 bytes free)

```

## Step 3 Set boot variable

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

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

```
Switch(config)# boot system 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.

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

### c) **write memory**

Use this command to save boot settings.

```
Switch# write memory
```



d) **show bootvar**

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

```
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 =
```

**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 TFTP server or the flash , if you have copied the image to flash memory.

The following example displays the installation of the Cisco IOS XE Dublin 17.11.1 software image to flash, by using the **install add file activate commit** command.

```
Switch# install add file flash:cat9k_iosxe.17.11.01.SPA.bin activate commit
_install_add_activate_commit: START Mon Jul 24 21:37:25 IST 2023

*Jul 24 16:37:26.544 IST: %INSTALL-5-INSTALL_START_INFO: R0/0: install_engine: Started
install one-shot flash:cat9k_iosxe.17.11.01.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.17.11.01.SPA.bin to standby
Info: Finished copying flash:cat9k_iosxe.17.11.01.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: 17.11.1
install_add_activate_commit: Activating PACKAGE
Following packages shall be activated:
/flash/cat9k-wlc.17.11.01.SPA.pkg
/flash/cat9k-webui.17.11.01.SPA.pkg
```

```

/flash/cat9k-srdriver.17.11.01.SPA.pkg
/flash/cat9k-sipspa.17.11.01.SPA.pkg
/flash/cat9k-sipbase.17.11.01.SPA.pkg
/flash/cat9k-rpboot.17.11.01.SPA.pkg
/flash/cat9k-rpbase.17.11.01.SPA.pkg
/flash/cat9k-guestshell.17.11.01.SPA.pkg
/flash/cat9k-espbases.17.11.01.SPA.pkg
/flash/cat9k-cc_srdriver.17.11.01.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

```

*Jul 24 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

```

```

*Jul 24 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 Mon Jul 24 21:46:18 IST 2023

**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.

The following sample output of the **show version** command displays the Cisco IOS XE Dublin 17.11.1 image on the device:

```

Switch# show version
Cisco IOS XE Software, Version 17.11.01
Cisco IOS Software [Dublin], Catalyst L3 Switch Software (CAT9K_IOSXE), Version 17.11.1,
RELEASE SOFTWARE (fcl)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2023 by Cisco Systems, Inc.
<output truncated>

```

# 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.
-





## CHAPTER 9

### Caveats

---

- [Cisco Bug Search Tool](#), on page 49
- [Open Caveats in Cisco IOS XE Dublin 17.12.x](#), on page 49
- [Resolved Caveats in Cisco IOS XE Dublin 17.12.3](#), on page 50
- [Resolved Caveats in Cisco IOS XE Dublin 17.12.2](#), on page 50
- [Resolved Caveats in Cisco IOS XE Dublin 17.12.1](#), on page 50

### Cisco Bug Search Tool

The Cisco [Bug Search Tool](#) (BST) allows partners and customers to search for software bugs based on product, release, and keyword, and aggregates key data such as bug details, product, and version. The BST is designed to improve the effectiveness in network risk management and device troubleshooting. The tool has a provision to filter bugs based on credentials to provide external and internal bug views for the search input.

To view the details of a caveat, click on the identifier.

### Open Caveats in Cisco IOS XE Dublin 17.12.x

Identifier	Headline
<a href="#">CSCwf67769</a>	9500X/9600X SVL: Support permit/deny ACL logging on 9500X/9600X
<a href="#">CSCwh35728</a>	Need switch to host macsec support in Sda overlay network
<a href="#">CSCwh91946</a>	PBR leak seen on C9600x when PBR is configured
<a href="#">CSCwj38294</a>	C9600X-SUP-2 is dropping IPv6 ND packets
<a href="#">CSCwi74812</a>	STALE mac address is not getting cleared on FED matm table after mac age out on Port-channel

## Resolved Caveats in Cisco IOS XE Dublin 17.12.3

Identifier	Headline
<a href="#">CSCwi83012</a>	SNMP results still contain 4 lanes for 100G optics which do not have multiple lanes
<a href="#">CSCwh45085</a>	C9600X-SUP-2: Unexpected reload during upgrade to 17.12.1 when using C9600-LC-40YL4CD
<a href="#">CSCwh91796</a>	BUM not forwarding while the L2 vni is down
<a href="#">CSCwi28679</a>	9500X/9600X - 224.0.0.1 packets received on a portchannel are sent back through the same portchannel
<a href="#">CSCwi06404</a>	PKI crash after failing a CRL Fetch

## Resolved Caveats in Cisco IOS XE Dublin 17.12.2

Identifier	Headline
<a href="#">CSCwh87343</a>	Cisco IOS XE Software Web UI Privilege Escalation Vulnerability For more information, see Security Advisory: <a href="#">cisco-sa-iosxe-webui-privesc-j22SaA4z</a> .
<a href="#">CSCwf91450</a>	C9500X/C9600X - Stackwise-Virtual: Unexpected Reload with Last reload reason: CPUReset
<a href="#">CSCwe20900</a>	C9500X/C9600X - Stackwise Virtual May Fail to Program Own MAC Address In Hardware
<a href="#">CSCwh01883</a>	C9600X-SUP-2: LCs can't boot from Golden region of IOFPGA when Upgrade/Primary region is corrupted
<a href="#">CSCwh81650</a>	9500X/9600X - memory leak under LEABA_MAIN_DB

## Resolved Caveats in Cisco IOS XE Dublin 17.12.1

Identifier	Headline
<a href="#">CSCwd50137</a>	(C9600X) 9500X/9600X NG-SVL/Standalone: Incorrect reload reason for ISSU/Install upgrade
<a href="#">CSCwf22599</a>	(C9600X) C9500X / C9600X - Routing Traffic to Incorrect Next-Hop MAC Address



## CHAPTER 10

# Additional Information

---

- [Troubleshooting](#), on page 51
- [Related Documentation](#), on page 51
- [Communications, Services, and Additional Information](#), on page 51

## Troubleshooting

For the most up-to-date, detailed troubleshooting information, see the Cisco TAC website at this URL:

<https://www.cisco.com/en/US/support/index.html>

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.

## Related Documentation

Information about Cisco IOS XE at this URL: <https://www.cisco.com/c/en/us/products/ios-nx-os-software/ios-xe/index.html>

All support documentation for Cisco Catalyst 9600 Series Switches is at this URL: <https://www.cisco.com/c/en/us/support/switches/catalyst-9600-series-switches/tsd-products-support-series-home.html>

Cisco Validated Designs documents at this URL: <https://www.cisco.com/go/designzone>

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <https://cfmg.cisco.com/mibs>

## Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at [Cisco Profile Manager](#).
- To get the business impact you're looking for with the technologies that matter, visit [Cisco Services](#).
- To submit a service request, visit [Cisco Support](#).
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit [Cisco Marketplace](#).

- To obtain general networking, training, and certification titles, visit [Cisco Press](#).
- To find warranty information for a specific product or product family, access [Cisco Warranty Finder](#).

### **Cisco Bug Search Tool**

[Cisco Bug Search Tool](#) (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.





