Release Notes for Cisco Catalyst 9500 Series Switches, Cisco IOS XE Gibraltar 16.12.x

First Published: 2019-07-31

Last Modified: 2022-09-22

Release Notes for Cisco Catalyst 9500 Series Switches, Cisco IOS XE Gibraltar 16.12.x

Introduction

Cisco Catalyst 9500 Series Switches and Cisco Catalyst 9500 Series Switches - High Performance are leading, fixed, core and aggregation enterprise switching platforms and have been purpose-built to address emerging trends in security, IoT, mobility, and cloud.

These switches deliver complete convergence in terms of ASIC architecture with Unified Access Data Plane (UADP) 2.0 on Cisco Catalyst 9500 Series Switches and UADP 3.0 on Cisco Catalyst 9500 Series Switches - High Performance. The platform runs an open Cisco IOS XE that supports model-driven programmability. This series forms the foundational building block for Software-Defined Access (SD-Access), which is Cisco's lead enterprise architecture.

Note With the introduction of the High Performance models in the series, there may be differences in the supported and unsupported features, limitations, and caveats that apply to the Cisco Catalyst 9500 Series Switches and Cisco Catalyst 9500 Series Switches - High Performance models. Throughout this release notes document, any such differences are expressly called out. If they are not, the information applies to all the models in the series.

Whats New in Cisco IOS XE Gibraltar 16.12.8

There are no new hardware or software features in this release. For the list of open and resolved caveats in this release, see Caveats.

Whats New in Cisco IOS XE Gibraltar 16.12.7

There are no new hardware or software features in this release. For the list of open and resolved caveats in this release, see Caveats.

Whats New in Cisco IOS XE Gibraltar 16.12.6

There are no new hardware or software features in this release. For the list of open and resolved caveats in this release, see Caveats.

Whats New in Cisco IOS XE Gibraltar 16.12.5b

There are no new hardware or software features in this release. For the list of open and resolved caveats in this release, see Caveats.

Whats New in Cisco IOS XE Gibraltar 16.12.5

There are no new hardware or software features in this release. For the list of open and resolved caveats in this release, see Caveats.

Whats New in Cisco IOS XE Gibraltar 16.12.4

There are no new hardware or software features in this release. For the list of open and resolved caveats in this release, see Caveats.

Whats New in Cisco IOS XE Gibraltar 16.12.3a

There are no new hardware or software features in this release. For the list of open and resolved caveats in this release, see Caveats.

Whats New in Cisco IOS XE Gibraltar 16.12.3

There are no new hardware or software features in this release. For the list of open and resolved caveats in this release, see Caveats.

Whats New in Cisco IOS XE Gibraltar 16.12.2

Hardware Features in Cisco IOS XE Gibraltar 16.12.2

There are no new hardware features in this release for C9500-12Q, C9500-16X, C9500-24Q and C9500-40X switch models of the Cisco Catalyst 9500 Series Switches.

Table 1: Hardware Features Introduced on Cisco Catalyst 9500 Series Switches-High Performance (C9500-24Y4C, C9500-32C, C9500-32QC, C9500-48Y4C)

Feature Name	Description and Documentation Link
Direct-Attach Active Optical Cables	• Supported cable product numbers: • SFP-10G-AOC1M, SFP-10G-AOC2M, SFP-10G-AOC3M, SFP-10G-AOC5M, SFP-10G-AOC7M, SFP-10G-AOC10M • Compatible switch models—C9500-24Y4C, C9500-32C, C9500-32QC, C9500-48Y4C For information about the module, see Cisco 10GBASE SFP+ Modules Data Sheet. For information about device compatibility, see the Transceiver Module Group (TMG) Compatibility Matrix.

Software Features in Cisco IOS XE Gibraltar 16.12.2

There are no new software features in this release. For the list of open and resolved caveats in this release, see Caveats.

Whats New in Cisco IOS XE Gibraltar 16.12.1c

Cisco IOS XE Gibraltar 16.12.1c release applies only to Cisco Catalyst 9500 Series Switches - High Performance. There are no new hardware or software features in this release. For the list of open and resolved caveats in this release, see Caveats, on page 51.

Whats New in Cisco IOS XE Gibraltar 16.12.1

Hardware Features in Cisco IOS XE Gibraltar 16.12.1

- Hardware Features Introduced on Cisco Catalyst 9500 Series Switches
- Hardware Features Introduced on Cisco Catalyst 9500 Series Switches-High Performance

Table 2: Hardware Features Introduced on Cisco Catalyst 9500 Series Switches (C9500-12Q, C9500-16X, C9500-24Q, C9500-40X)

Feature Name	Description and Documentation Link
Direct-Attach Copper Cable	• Supported cable product number: QSFP-H40G-CU0-5M. • Compatible switch model numbers: C9500-12Q, C9500-16X, C9500-24Q, C9500-40X. • Compatible network modules: C9500-NM-2Q. For information about the module, see Cisco 40GBASE QSFP Modules Data Sheet. For information about device compatibility, see the Transceiver Module Group (TMG) Compatibility Matrix.

Table 3: Hardware Features Introduced on Cisco Catalyst 9500 Series Switches-High Performance (C9500-24Y4C, C9500-32C, C9500-32QC, and C9500-48Y4C

Feature Name	Description and Documentation Link
Cisco SFP Modules for Gigabit Ethernet	• Supported transceiver module product numbers—GLC-T and GLC-TE (10 and 100 Mbps supported). • Compatible switch models— C9500-48Y4C, C9500-24Y4C. For information about the module, see Cisco SFP Modules for Gigabit Ethernet Applications Data Sheet. For information about device compatibility, see the Transceiver Module Group (TMG) Compatibility Matrix.
Cisco 100BASE-X Small Form-Factor Pluggable (SFP) Modules	• Supported transceiver module product number— GLC-GE-100FX. • Compatible switch models—C9500-48Y4C, C9500-24Y4C. For information about the module, see Cisco 100BASE-X Small Form-Factor Pluggable Modules for Fast Ethernet Applications Data Sheet. For information about device compatibility, see the Transceiver Module Group (TMG) Compatibility Matrix.
Cisco 100GBASE QSFP-100G Modules	• Supported transceiver module product number—QSFP-40/100-SRBD. 40G and 100G modes are supported. By default, the 100G mode is effective. For 40G, configure the **speed** command, in the interface configuration mode. • Compatible switch models—C9500-32C, C9500-32QC, C9500-48Y4C, C9500-24Y4C. For information about the module, see Cisco 100GBASE QSFP-100G Modules Data Sheet. For information about device compatibility, see the Transceiver Module Group (TMG) Compatibility Matrix.
Direct-Attach Copper Cable	• Supported cable product number: QSFP-H40G-CU0-5M. • Compatible switch model numbers: C9500-32C, C9500-32QC, C9500-48Y4C, C9500-24Y4C. For information about the module, see Cisco 40GBASE QSFP Modules Data Sheet. For information about device compatibility, see the Transceiver Module Group (TMG) Compatibility Matrix.

Software Features in Cisco IOS XE Gibraltar 16.12.1

- Software Features Introduced on All Models, on page 5
- Software Features Introduced on Cisco Catalyst 9500 Series Switches, on page 8
- Software Features Introduced on Cisco Catalyst 9500 Series Switches-High Performance, on page 12

Software Features Introduced on All Models

Feature Name	Description, Documentation Link, and License Level Information
Autoconf Device Granularity to PID of Cisco Switch	Introduces the **platform type** filter option for class map and parameter map configurations. Use the **map platform-type** command in parameter map filter configuration mode, to set the parameter map attribute and the **match platform-type** command in control class-map filter configuration mode, to evaluate control classes. See Network Management → Configuring Autoconf. (Network Essentials and Network Advantage)
Border Gateway Protocol (BGP) Ethernet VPN (EVPN) Route Target (RT) Autonomous System Number (ASN) Rewrite	Introduces support for the **rewrite-evpn-rt-asn** command in address-family configuration mode. This command enables the rewrite of the ASN portion of the EVPN route target that originates from the current autonomous system, with the ASN of the target eBGP EVPN peer. See IP Routing Commands → rewrite-evpn-rt-asn. (Network Advantage)
Bidirectional Protocol Independent Multicast (PIM)	Introduces support for bidirectional PIM. This feature is an extension of the PIM suite of protocols that implements shared sparse trees with bidirectional data flow. In contrast to PIM-sparse mode, bidirectional PIM avoids keeping source-specific state in a router and allows trees to scale to an arbitrary number of sources. See IP Multicast Routing → Configuring Protocol Independent Multicast (PIM). (Network Advantage)
Ethernet over MPLS (EoMPLS) Xconnect on Subinterfaces	Transports Ethernet traffic from a source 802.1Q VLAN to a destination 802.1Q VLAN through a single virtual circuit over an Multiprotocol Label Switching (MPLS) network. See Multiprotocol Label Switching → Configuring Ethernet-over-MPLS and Pseudowire Redundancy. (Network Advantage)
High Availability support for MACsec Key Agreement (MKA)	Support for high availability for MKA sessions is introduced. MKA sessions are now SSO-aware. In the event of failure of the active switch, the standby switch takes over the existing MKA sessions in a minimally disruptive switchover. Since high availability for MKA MACSec is introduced in this release, existing MKA MACSec sessions must be cleared once using **clear mka sessions** if software image is upgraded from older releases using ISSU. See Security → MACsec Encryption. (Network Advantage)

Feature Name	Description, Documentation Link, and License Level Information
IEEE 1588v2, Precision Time Protocol (PTP) support	Introduces support for PTP Version 2 (PTPv2) on the Cisco Catalyst 9500 Series Switches - High Performance. PTP is defined in IEEE 1588 as Precision Clock Synchronization for Networked Measurements and Control Systems, and was developed to synchronize the clocks in packet-based networks that include distributed device clocks of varying precision and stability. A PTP profile is the set of allowed PTP features applicable to a device. Introduces PTP support on native Layer 3 ports on all the variants of the Cisco Catalyst 9500 Series Switches. See Configuring Precision Time Protocol (PTP). (Network Advantage)
IPv4 and IPv6: Object Groups for access control lists (ACLs)	Enables you to classify users, devices, or protocols into groups and apply them to ACLs, to create access control policies for these groups. With this feature, you use object groups instead of individual IP addresses, protocols, and ports, which are used in conventional ACLs. It allows multiple access control entries (ACEs), and you can use each ACE to allow or deny an entire group of users the access to a group of servers or services. See Security → Object Groups for ACLs. (Network Essentials and Network Advantage)
MPLS Layer 2 VPN over GRE	Provides a mechanism for tunneling Layer 2 MPLS packets over a non-MPLS network. See Multiprotocol Label Switching → Configuring MPLS Layer 2 VPN over GRE. (Network Advantage)
MPLS Layer 3 VPN over Generic Routing Encapsulation (GRE)	Provides a mechanism for tunneling Layer 3 MPLS packets over a non-MPLS network. See Multiprotocol Label Switching → Configuring MPLS Layer 3 VPN over GRE. (Network Advantage)
MPLS Subinterface Support	MPLS is now supported on Layer 3 subinterfaces. See VLAN → Configuring Layer 3 Subinterfaces. (Network Advantage)
Network Address Translation (NAT) license level change	The NAT feature is now available with the Network Advantage license. See IP Addressing Services → Configuring Network Address Translation. (Network Advantage)
Port Channel with Subinterface	Subinterfaces can now be created on Layer 3 port channels. See VLAN → Configuring Layer 3 Subinterfaces. (Network Essentials and Network Advantage)

Feature Name	Description, Documentation Link, and License Level Information
Programmability • IoX Support of Docker • Model-Driven Telemetry gNMI Dial-In • NETCONF-YANG SSH Server Support • YANG Data Models	The following programmability features are introduced in this release: • Model-Driven Telemetry gNMI Dial-In—Support for telemetry subscriptions and updates over a gRPC Network Management Interface (gNMI). • NETCONF-YANG SSH Server Support—NETCONF-YANG supporting the use of IOS Secure Shell (SSH) public keys (RSA) to authenticate users as an alternative to password-based authentication. • YANG Data Models—For the list of Cisco IOS XE YANG models available with this release, navigate to: https://github.com/YangModels/yang/tree/master/vendor/cisco/xe/16121. Some of the models introduced in this release are not backward compatible. For the complete list, navigate to: https://github.com/YangModels/yang/tree/master/vendor/cisco/xe/16121/BIC. Revision statements embedded in the YANG files indicate if there has been a model revision. The *README.md* file in the same GitHub location highlights changes that have been made in the release. See Programmability. (Network Essentials and Network Advantage)
Seamless MPLS	Integrates multiple networks into a single MPLS domain. It removes the need for service specific configurations in network transport nodes. See Multiprotocol Label Switching → Configuring Seamless MPLS. (Network Advantage)
Simplified Factory Reset for Removable Storage	Performing a factory reset now also erases the contents of removable storage devices such as Serial Advanced Technology Attachment (SATA), Solid State Drive (SSD), and USB. See System Management → Performing Factory Reset. (Network Advantage)
Source Group Tag (SGT), Destination Group Tag (DGT) over FNF for IPv6 traffic	Introduces support for SGT and DGT fields over FNF, for IPv6 traffic. See Network Management → Configuring Flexible NetFlow. (Network Advantage)
VPN Routing and Forwarding-aware Policy Based Routing (VRF-aware PBR)	The PBR feature is now VRF-aware and can be configured on VRF lite interfaces. You can enable policy based routing of packets for a VRF instance. See IP Routing → Configuring VRF aware PBR. (Network Advantage)

New on the Web UI	
• 802.1X Port-Based Authentication • Audio Video Bridging	Use the WebUI for: • 802.1X Port-Based Authentication—Supports IEEE 802.1X authentication configuration at the interface level. This type of access control and authentication protocol restricts unauthorized clients from connecting to a LAN through publicly accessible ports • Audio Video Bridging—Supports configuration and monitoring of Ethernet based audio/video deployments using the IEEE 802.1BA standard. This enables low latency and high dedicated bandwidth for time-sensitive audio and video streams for a professional grade experience.

Software Features Introduced on Cisco Catalyst 9500 Series Switches

Feature Name	Description, Documentation Link, and License Level Information
Bluetooth Dongle	Introduces support for external USB Bluetooth dongles. The connected dongle acts as a Bluetooth host and serves as a management port connection on the device. See Interface and Hardware Components → Configuring an External USB Bluetooth Dongle. (Network Essentials and Network Advantage)
Flexlink+	Configures a pair of Layer 2 interfaces - one interface is configured to act as a backup for the other interface. See Layer 2 → Configuring Flexlink+. (Network Essentials and Network Advantage)

Feature Name	Description, Documentation Link, and License Level Information
IPv6: BGP	IPv6 support is introduced for the following features: • IPv6: BGP Hide Local Autonomous System • IPv6: BGP Named Community Lists • IPv6: BGP Neighbor Policy • IPv6: BGP Prefix-Based Outbound Route Filtering • IPv6: BGP Restart Neighbor Session After Max-Prefix Limit Reached • IPv6: BGP Support for Fast Peering Session Deactivation • IPv6: BGP Selective Address Tracking • IPv6: BGP IPv6 PIC Edge and Core for IP/MPLS • IPv6: Multiprotocol BGP Link-local Address Peering • IPv6: BGP Route-Map Continue • IPv6: BGP Route-Map Continue Support for Outbound Policy • IPv6: BGP Support for IP Prefix Import from Global Table into a VRF Table • IPv6: BGP Named Community Lists • IPv6: BGP Support for Sequenced Entries in Extended Community Lists • IPv6: BGP Support for TTL Security Check • IPv6: BGP Support for BFD (Network Advantage)
IPv6: Intermediate System to Intermediate System (IS-IS)	IPv6 support is introduced for the following IS-IS features: • Integrated ISIS Point to Point Adjacency over Broadcast Media • Integrated ISIS Protocol Shutdown Support Maintaining Configuration Parameters
IPv6: IP Enhanced IGRP Route Authentication	IPv6 support is introduced for IP Enhanced IGRP Route Authentication. (Network Advantage and Network Essentials)

Feature Name	Description, Documentation Link, and License Level Information
IPv6: IP Service Level Agreements (SLAs)	IPv6 support is introduced for the following IP SLA features: • IPv6: IP SLAs - Multi Operation Scheduler • IPv6: IP SLAs - One Way Measurement • IPv6: IP SLAs - VoIP Threshold Traps • IPv6: IP SLAs - Additional Threshold Traps • IPv6: IP SLAs - Random Scheduler • IPv6: IP SLAs - Sub-millisecond Accuracy Improvements (Network Advantage and Network Essentials)
IPv6: MIBs for IPv6 Traffic	Introduces IPv6 support for the following MIBs: • IP Forwarding Table MIB (RFC4292) • Management Information Base for the Internet Protocol (IP) (RFC4293 (Network Advantage and Network Essentials)
IPv6: Multicast Routing	IPv6 support is introduced for the following multicast routing features: • IPv6: Address Family Support for Multiprotocol BGP • IPv6: Address Group Range Support • IPv6: PIMv6 Anycast RP solution (Network Advantage)
IPv6: Multiprotocol Label Switching (MPLS)	IPv6 support is introduced for the following MPLS features: • IPv6: MPLS VPN VRF CLI for IPv4 and IPv6 VPNs • IPv6: EIGRP IPv6 NSF/GR • IPv6: EIGRP MPLS VPN PE-CE • IPv6: Route Target Rewrite • IPv6: eiBGP Multipath (Network Advantage)
IPv6: Neighbor Discovery	IPv6 support is introduced for the following Neighbor Discovery features: • IPv6: Global IPv6 entries for unsolicited NA • IPv6: HA support (Network Advantage and Network Essentials)

Feature Name	Description, Documentation Link, and License Level Information
IPv6: Open Shortest Path First (OSPF)	IPv6 support is introduced for the following OSPF features: • IPv6: NSF - OSPF • IPv6: OSPF Flooding Reduction • IPv6: OSPF Link State Database Overload Protection • IPv6: OSPF On Demand Circuit (RFC 1793) • IPv6: OSPF Packet Pacing • IPv6: OSPF Support for Multi-VRF on CE Routers • IPv6: OSPFv3 NSR • IPv6: OSPFv3 Retransmission Limits • IPv6: OSPF for IPv6 (OSPFv3) Authentication Support with IPsec • IPv6: OSPFv3 Graceful Restart • IPv6: VRF aware OSPFv3, EIGRPv6, BGPv6 • IPv6: OSPFv3 Fast Convergence - LSA and SPF throttling (Network Advantage and Network Essentials)
IPv6: Proxy Mobile	IPv6 support is introduced for PMIPv6 Hybrid Access.
IPv6: Services	IPv6 support is introduced for AAAA DNS Lookups over an IPv6 Transport. (Network Advantage and Network Essentials)
IPv6: Time-Based Access Lists Using Time Ranges	IPv6 support is introduced for Time-Based Access Lists using time ranges. (Network Advantage and Network Essentials)
IPv6: Triggered RIP	IPv6 support is introduced for Triggered Extensions to RIP.
IPv6-based Posture Validation	Introduces IPv6 support for Posture Validation. (Network Advantage and Network Essentials)
Layer 3 Subinterface	Layer 3 interfaces forward IPv4 and IPv6 packets to another device using static or dynamic routing protocols. You can use Layer 3 interfaces for IP routing and inter-VLAN routing of Layer 2 traffic. See VLAN → Configuring Layer 3 Subinterfaces.
MPLS VPN-Inter-AS Option B	Allows an MPLS Virtual Private Network (VPN) service provider to interconnect different autonomous systems to provide VPN services. In an Inter-AS Option B network, autonomous system boundary router (ASBR) peers are connected by one or more interfaces that are enabled to receive MPLS traffic. See Multiprotocol Label Switching → Configuring MPLS InterAS Option B. (Network Advantage)

Feature Name	Description, Documentation Link, and License Level Information
Stack troubleshooting optimization	The output of the **show tech-support stack** command has been enhanced to include more stack-related information. See High Availability Commands → show tech-support stack. (A license level does not apply)

Software Features Introduced on Cisco Catalyst 9500 Series Switches-High Performance

Feature Name	Description, Documentation Link, and License Level Information
Cisco StackWise Virtual—Cisco QSFP to SFP or SFP+ Adapter (QSA module)	Introduces support for QSA module with Cisco StackWise Virtual. • Cisco QSA module with 10G SFP modules can be used as data ports and to configure StackWise Virtual links (SVLs) or Dual-Active Detection (DAD) links. • Cisco QSA module with 1G SFP modules can be used as data ports and to configure DAD links; they cannot be used to configure SVLs since SVLs are not supported on 1G interfaces. See High Availability → Configuring Cisco StackWise Virtual. (Network Advantage)
In-Service Software Upgrade (ISSU) with Cisco StackWise Virtual	Introduces support for ISSU with Cisco StackWise Virtual. See High Availability → Configuring ISSU. (Network Advantage)

Important Notes

- Cisco StackWise Virtual - Supported and Unsupported Features
- Unsupported Features—All Models
- Unsupported Features—Cisco Catalyst 9500 Series Switches
- Unsupported Features—Cisco Catalyst 9500 Series Switches - High Performance
- Complete List of Supported Features
- Accessing Hidden Commands
- Default Behaviour—All Models

- Default Interface Behaviour on Cisco Catalyst 9500 Series Switches - High Performance Only

Cisco StackWise Virtual - Supported and Unsupported Features

When you enable Cisco StackWise Virtual on the device

- Layer 2, Layer 3, Security, Quality of Service, Multicast, Application Monitoring and Management, Multiprotocol Label Switching, High Availability, BGP EVPN VXLAN, Remote Switched Port Analyzer, and Sofware Defined Access are supported.

  Contact the Cisco Technical Support Centre for the specific list of features that are supported under each one of these technologies.

- Resilient Ethernet Protocol is *not* supported.

Unsupported Features—All Models

- IPsec VPN
- Performance Monitoring (PerfMon)
- Virtual Routing and Forwarding (VRF)-Aware web authentication

Unsupported Features—Cisco Catalyst 9500 Series Switches

- Border Gateway Protocol (BGP) Additional Paths
- Cisco TrustSec Network Device Admission Control (NDAC) on Uplinks
- Flexible NetFlow—NetFlow v5 Export Protocol, 4-byte (32-bit) AS Number Support, TrustSec NetFlow IPv4 Security Group Access Control List (SGACL) Deny and Drop Export
- Lawful Intercept (LI)
- Network-Powered Lighting (including COAP Proxy Server, 2-event Classification, Perpetual POE, Fast PoE)
- PIM Bidirectional Forwarding Detection (PIM BFD), PIM Snooping.
- Quality of Service—Classification (Layer 3 Packet Length, Time-to-Live (TTL)), per queue policer support, sharped profile enablement for egress per port queues, L2 Miss, Ingress Packet FIFO (IPF)
- Unicast over Point to Multipoint (P2MP) Generic Routing Encapsulation (GRE), Multicast over P2MP GRE.
- VLAN Translation—One-to-One Mapping

Unsupported Features—Cisco Catalyst 9500 Series Switches - High Performance

- Cisco Application Visibility and Control (AVC)
- Flexlink+
- VLAN Load Balancing for FlexLink+
- Preemption for VLAN Load Balancing

- FlexLink+ Dummy Multicast Packets
- MPLS Label Distribution Protocol (MPLS LDP) VRF-Aware Static Labels
- Next Generation Network-Based Application Recognition (NBAR) and Next Generation NBAR (NBAR2)
- QoS Options on GRE Tunnel Interfaces

Complete List of Supported Features

For the complete list of features supported on a platform, see the Cisco Feature Navigator at https://www.cisco.com/go/cfn.

When you search for the list of features by platform select

- CAT9500—to see all the features supported on the C9500-12Q, C9500-16X, C9500-24Q, C9500-40X models
- CAT9500 HIGH PERFORMANCE (32C; 32QC; 48Y4C; 24Y4C)—to see all the features supported on the C9500-24Y4C, C9500-32C, C9500-32QC, and C9500-48Y4C models

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. This means that entering enter a question mark (?) at the system prompt did not display the list of available commands. For information about CLI help, see Understanding the Help System. Such hidden commands are only meant to assist Cisco TAC in advanced troubleshooting and are therefore not documented.

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. Entering enter a question mark (?) at the system prompt displays 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 the 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—All Models

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

Default Interface Behaviour on Cisco Catalyst 9500 Series Switches - High Performance Only

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

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

Supported Hardware

Cisco Catalyst 9500 Series Switches—Model Numbers

The following table lists the supported hardware models and the default license levels they are delivered with. For more information about the available license levels, see section *License Levels*.

Base PIDs are the model numbers of the switch.

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

Table 4: Cisco Catalyst 9500 Series Switches

Switch Model	Default License Level	Description
Base PIDs		
C9500-12Q-E	Network Essentials	12 40-Gigabit Ethernet QSFP+ ports and two power supply slots
C9500-12Q-A	Network Advantage	
C9500-16X-E	Network Essentials	16 1/10-Gigabit Ethernet SFP/SFP+ ports and two power supply slots
C9500-16X-A	Network Advantage	

Switch Model	Default License Level	Description
C9500-24Q-E	Network Essentials	24-Port 40-Gigabit Ethernet QSFP+ ports and two power supply slots
C9500-24Q-A	Network Advantage	
C9500-40X-E	Network Essentials	40 1/10-Gigabit Ethernet SFP/SFP+ ports and two power supply slots
C9500-40X-A	Network Advantage	
Bundled PIDs		
C9500-16X-2Q-E	Network Essentials	16 10-Gigabit Ethernet SFP+ port switch and a 2-Port 40-Gigabit Ethernet (QSFP) network module on uplink ports
C9500-16X-2Q-A	Network Advantage	
C9500-24X-E	Network Essentials	16 10-Gigabit Ethernet SFP+ port switch and an 8-Port 10-Gigabit Ethernet (SFP) network module on uplink ports
C9500-24X-A	Network Advantage	
C9500-40X-2Q-E	Network Essentials	40 10-Gigabit Ethernet SFP+ port switch and a 2-Port 40-Gigabit Ethernet (QSFP) network module on uplink ports
C9500-40X-2Q-A	Network Advantage	
C9500-48X-E	Network Essentials	40 10-Gigabit Ethernet SFP+ port switch and an 8-Port 10-Gigabit Ethernet (SFP) network module on uplink ports
C9500-48X-A	Network Advantage	

Table 5: Cisco Catalyst 9500 Series Switches-High Performance

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

Network Modules

The following table lists optional network modules for uplink ports available with some configurations .

Network Module	Description
C9500-NM-8X	Cisco Catalyst 9500 Series Network Module 8-port 1/10 Gigabit Ethernet with SFP/SFP+ Note the supported switch models (Base PIDs): • C9500-40X • C9500-16X
C9500-NM-2Q	Cisco Catalyst 9500 Series Network Module 2-port 40 Gigabit Ethernet with QSFP+ Note the supported switch models (Base PIDs): • C9500-40X • C9500-16X

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

Compatibility Matrix

The following table provides software compatibility information between Cisco Catalyst 9500 Series Switches, Cisco Identity Services Engine, Cisco Access Control Server, and Cisco Prime Infrastructure.

Catalyst 9500, 9500-High Performance and 9500X	Cisco Identity Services Engine	Cisco Access Control Server	Cisco Prime Infrastructure
Gibraltar 16.12.8	2.6	-	PI 3.9 + PI 3.9 latest maintenance release + PI 3.9 latest device pack See Cisco Prime Infrastructure 3.9 → Downloads.
Gibraltar 16.12.7	2.6	-	PI 3.9 + PI 3.9 latest maintenance release + PI 3.9 latest device pack See Cisco Prime Infrastructure 3.9 → Downloads.

Catalyst 9500, 9500-High Performance and 9500X	Cisco Identity Services Engine	Cisco Access Control Server	Cisco Prime Infrastructure
Gibraltar 16.12.6	2.6	-	PI 3.9 + PI 3.9 latest maintenance release + PI 3.9 latest device pack See Cisco Prime Infrastructure 3.9 → Downloads.
Gibraltar 16.12.5b	2.6	-	PI 3.9 + PI 3.9 latest maintenance release + PI 3.9 latest device pack See Cisco Prime Infrastructure 3.9 → Downloads.
Gibraltar 16.12.5	2.6	-	PI 3.9 + PI 3.9 latest maintenance release + PI 3.9 latest device pack See Cisco Prime Infrastructure 3.9 → Downloads.
Gibraltar 16.12.4	2.6	-	PI 3.8 + PI 3.8 latest maintenance release + PI 3.8 latest device pack See Cisco Prime Infrastructure 3.8 → Downloads.
Gibraltar 16.12.3a	2.6	-	PI 3.5 + PI 3.5 latest maintenance release + PI 3.5 latest device pack See Cisco Prime Infrastructure 3.5 → **Downloads**.
Gibraltar 16.12.3	2.6	-	PI 3.5 + PI 3.5 latest maintenance release + PI 3.5 latest device pack See Cisco Prime Infrastructure 3.5 → **Downloads**.
Gibraltar 16.12.2	2.6	-	PI 3.5 + PI 3.5 latest maintenance release + PI 3.5 latest device pack See Cisco Prime Infrastructure 3.5 → **Downloads**.
Gibraltar 16.12.1	2.6	-	PI 3.5 + PI 3.5 latest maintenance release + PI 3.5 latest device pack See Cisco Prime Infrastructure 3.5 → **Downloads**.

Catalyst 9500, 9500-High Performance and 9500X	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	PI 3.4 + PI 3.4 latest maintenance release + PI 3.4 latest device pack See Cisco Prime Infrastructure 3.4 → **Downloads**.
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 Cisco Prime Infrastructure 3.4→ **Downloads**.
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 Cisco Prime Infrastructure 3.9 → **Downloads**.
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 Cisco Prime Infrastructure 3.9 → **Downloads**.
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 Cisco Prime Infrastructure 3.4→ **Downloads**.
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 Cisco Prime Infrastructure 3.4→ **Downloads**.
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 Cisco Prime Infrastructure 3.4→ **Downloads**.
Fuji 16.9.3	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 Cisco Prime Infrastructure 3.4→ **Downloads**.

Catalyst 9500, 9500-High Performance and 9500X	Cisco Identity Services Engine	Cisco Access Control Server	Cisco Prime Infrastructure
Fuji 16.9.2	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 Cisco Prime Infrastructure 3.4→ **Downloads**.
Fuji 16.9.1	2.3 Patch 1 2.4 Patch 1	5.4 5.5	PI 3.4 + PI 3.4 latest device pack See Cisco Prime Infrastructure 3.4→ **Downloads**.
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 Cisco Prime Infrastructure 3.3→ **Downloads**.
Everest 16.6.4a	2.2 2.3	5.4 5.5	PI 3.1.6 + Device Pack 13 See Cisco Prime Infrastructure 3.1 → **Downloads**.
Everest 16.6.4	2.2 2.3	5.4 5.5	PI 3.1.6 + Device Pack 13 See Cisco Prime Infrastructure 3.1 → **Downloads**.
Everest 16.6.3	2.2 2.3	5.4 5.5	PI 3.1.6 + Device Pack 13 See Cisco Prime Infrastructure 3.1 → **Downloads**
Everest 16.6.2	2.2 2.3	5.4 5.5	PI 3.1.6 + Device Pack 13 See Cisco Prime Infrastructure 3.1 → **Downloads**
Everest 16.6.1	2.2	5.4 5.5	PI 3.1.6 + Device Pack 13 See Cisco Prime Infrastructure 3.1 → **Downloads**
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[1]	512 MB[2]	256	1280 x 800 or higher	Small

[1] We recommend 1 GHz
[2] 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)

Upgrading 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.

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

(C9500-12Q, C9500-16X, C9500-24Q, C9500-40X)

Release	Image Type	File Name
Cisco IOS XE Gibraltar 16.12.8	CAT9K_IOSXE	cat9k_iosxe.16.12.08.SPA.bin
	No Payload Encryption (NPE)	cat9k_iosxe_npe.16.12.08.SPA
Cisco IOS XE Gibraltar 16.12.7	CAT9K_IOSXE	cat9k_iosxe.16.12.07.SPA.bin
	No Payload Encryption (NPE)	cat9k_iosxe_npe.16.12.07.SPA
Cisco IOS XE Gibraltar 16.12.6	CAT9K_IOSXE	cat9k_iosxe.16.12.06.SPA.bin
	No Payload Encryption (NPE)	cat9k_iosxe_npe.16.12.06.SPA
Cisco IOS XE Gibraltar 16.12.5b	CAT9K_IOSXE	cat9k_iosxe.16.12.05b.SPA.bi
	No Payload Encryption (NPE)	cat9k_iosxe_npe.16.12.05b.SP
Cisco IOS XE Gibraltar 16.12.5	CAT9K_IOSXE	cat9k_iosxe.16.12.05.SPA.bin
	No Payload Encryption (NPE)	cat9k_iosxe_npe.16.12.05.SPA
Cisco IOS XE Gibraltar 16.12.4	CAT9K_IOSXE	cat9k_iosxe.16.12.04.SPA.bin
	No Payload Encryption (NPE)	cat9k_iosxe_npe.16.12.04.SPA
Cisco IOS XE Gibraltar 16.12.3a	CAT9K_IOSXE	cat9k_iosxe.16.12.03a.SPA.bi
	No Payload Encryption (NPE)	cat9k_iosxe_npe.16.12.03a.SP
Cisco IOS XE Gibraltar 16.12.3	CAT9K_IOSXE	cat9k_iosxe.16.12.03.SPA.bin
	No Payload Encryption (NPE)	cat9k_iosxe_npe.16.12.03.SPA
Cisco IOS XE Gibraltar 16.12.2	CAT9K_IOSXE	cat9k_iosxe.16.12.02.SPA.bin
	No Payload Encryption (NPE)	cat9k_iosxe_npe.16.12.02.SPA
Cisco IOS XE Gibraltar 16.12.1	CAT9K_IOSXE	cat9k_iosxe.16.12.01.SPA.bin
	No Payload Encryption (NPE)	cat9k_iosxe_npe.16.12.01.SPA

(C9500-24Y4C, C9500-32C, C9500-32QC, and C9500-48Y4C)

Release	Image Type	File Name
Cisco IOS XE Gibraltar 16.12.8	CAT9K_IOSXE	cat9k_iosxe.16.12.08.SPA.bin
	No Payload Encryption (NPE)	cat9k_iosxe_npe.16.12.08.SPA
Cisco IOS XE Gibraltar 16.12.7	CAT9K_IOSXE	cat9k_iosxe.16.12.07.SPA.bin
	No Payload Encryption (NPE)	cat9k_iosxe_npe.16.12.07.SPA

Release	Image Type	File Name
Cisco IOS XE Gibraltar 16.12.6	CAT9K_IOSXE	cat9k_iosxe.16.12.06.SPA.
	No Payload Encryption (NPE)	cat9k_iosxe_npe.16.12.06.
Cisco IOS XE Gibraltar 16.12.5b	CAT9K_IOSXE	cat9k_iosxe.16.12.05b.SPA
	No Payload Encryption (NPE)	cat9k_iosxe_npe.16.12.05b
Cisco IOS XE Gibraltar 16.12.5	CAT9K_IOSXE	cat9k_iosxe.16.12.05.SPA.
	No Payload Encryption (NPE)	cat9k_iosxe_npe.16.12.05.
Cisco IOS XE Gibraltar 16.12.4	CAT9K_IOSXE	cat9k_iosxe.16.12.04.SPA.
	No Payload Encryption (NPE)	cat9k_iosxe_npe.16.12.04.
Cisco IOS XE Gibraltar 16.12.3a	CAT9K_IOSXE	cat9k_iosxe.16.12.03a.SPA
	No Payload Encryption (NPE)	cat9k_iosxe_npe.16.12.03a
Cisco IOS XE Gibraltar 16.12.3	CAT9K_IOSXE	cat9k_iosxe.16.12.03.SPA.
	No Payload Encryption (NPE)	cat9k_iosxe_npe.16.12.03.
Cisco IOS XE Gibraltar 16.12.2	CAT9K_IOSXE	cat9k_iosxe.16.12.02.SPA.
	No Payload Encryption (NPE)	cat9k_iosxe_npe.16.12.02.
Cisco IOS XE Gibraltar 16.12.1c	CAT9K_IOSXE	cat9k_iosxe.16.12.01c.SPA
	No Payload Encryption (NPE)	cat9k_iosxe_npe.16.12.01c

ROMMON Upgrades

The ROM monitor (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 the Serial Peripheral Interface (SPI) flash devices in 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. To know the ROMMON or bootloader version that applies to every major and maintenance release, refer to the corresponding subsections and tables below.

- ROMMON Upgrades for C9500-12Q, C9500-16X, C9500-24Q, C9500-40X, on page 24
- ROMMON Upgrades for C9500-24Y4C, C9500-32C, C9500-32QC, and C9500-48Y4C, on page 25

ROMMON Upgrades for C9500-12Q, C9500-16X, C9500-24Q, C9500-40X

This subsection applies only to the C9500-12Q, C9500-16X, C9500-24Q, C9500-40X models of the series.

Note Cisco IOS XE Gibraltar 16.12.1: automatic ROMMON upgrade; no action required

Cisco IOS XE Gibraltar 16.12.2 and later releases: manual upgrade of both ROMMONs is required – if there is a new ROMMON version.

If you are upgrading *from* Cisco IOS XE Gibraltar 16.12.1 or a later release, and a new ROMMON version is available for the software version you are upgrading to, you must *manually upgrade* both ROMMONs. To know if there is a new ROMMON version for the software version you are upgrading to, see the table below:

Caution Do not power cycle your switch during the upgrade.

(C9500-12Q, C9500-16X, C9500-24Q, C9500-40X)

Scenario	ROMMON Version for C9500-12Q, C9500-16X, C9500-24Q, C9500-40X

If you boot Cisco IOS XE Gibraltar 16.12.3a
or
Cisco IOS XE Gibraltar 16.12.3
or
Cisco IOS XE Gibraltar 16.12.2 for the first time
	On Cisco Catalyst 9500 Series Switches, the ROMMON version is `16.12.2r`
	`ROM: IOS-XE ROMMON`
	`BOOTLDR: System Bootstrap, Version 16.12.2r, RELEASE SOFTWARE (P)`

If you boot Cisco IOS XE Gibraltar 16.12.1 for the first time	On Cisco Catalyst 9500 Series Switches, the ROMMON version may be automatically upgraded to `16.12.1r[FC1]`.
	`ROM: IOS-XE ROMMON`
	`BOOTLDR: System Bootstrap, Version 16.12.1r, RELEASE SOFTWARE (P)`
	You will see the following on the console, during the install operation , if you use install commands to upgrade software:
	`!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!`
	`%IOSXEBOOT-4-BOOTLOADER_UPGRADE: (rp/0): ### Wed Jul 31 18:03:28 Universal 2019 PLEASE DO NOT POWER CYCLE`
	`### BOOT LOADER UPGRADING`
	`waiting for upgrades to complete...`

You can upgrade the ROMMON before, or, after upgrading the software version. If you go back to an older release after this, the ROMMON is not downgraded. The updated ROMMON supports all previous releases.

- To upgrade the ROMMON in the primary SPI flash device, enter the **upgrade rom-monitor capsule primary switch** command in privileged EXEC mode.
- To upgrade the ROMMON in the golden SPI flash device, enter the **upgrade rom-monitor capsule golden switch** command in privileged EXEC mode.

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

ROMMON Upgrades for C9500-24Y4C, C9500-32C, C9500-32QC, and C9500-48Y4C

This subsection applies only to the C9500-24Y4C, C9500-32C, C9500-32QC, and C9500-48Y4C models of the series.

When you upgrade from the existing release on your switch to a later or newer release for the first time, the primary ROMMON may be automatically upgraded, based on the hardware version of the switch. If the ROMMON is automatically upgraded, it will take effect on the next reload. If you go back to the older release after this, the ROMMON is not downgraded. The updated ROMMON supports all previous releases. For subsequent Cisco IOS XE 16.x.x, releases, if there is a new ROMMON in that release, it may be automatically upgraded based on the hardware version of the switch when you boot up your switch with the new image for the first time.

On Cisco Catalyst 9500 Series Switches - High Performance, ROMMON upgrades do not happen during the install operation. The upgrade happens when the image starts booting.

Caution Do not power cycle your switch during the upgrade.

(C9500-24Y4C, C9500-32C, C9500-32QC, and C9500-48Y4C)

Scenario	Automatic ROMMON Upgrade Respoonse for C9500-24Y4C, C9500-32C, C9500-32QC, and C9500-48Y4C

If you boot Cisco IOS XE Gibraltar 16.12.3a
or
Cisco IOS XE Gibraltar 16.12.3
or
Cisco IOS XE Gibraltar 16.12.2 for the first time
	On Cisco Catalyst 9500 Series Switches - High Performance, the boot loader may be automatically upgraded to version `17.1.1[FC2]`.
	`ROM: IOS-XE ROMMON`
	`BOOTLDR: System Bootstrap, Version 17.1.1[FC2], RELEASE SOFTWARE (P)`

If you boot Cisco IOS XE Gibraltar 16.12.1c for the first time	On Cisco Catalyst 9500 Series Switches - High Performance, the boot loader may be automatically upgraded to version `16.12.1r[FC1]`.
	`ROM: IOS-XE ROMMON`
	`BOOTLDR: System Bootstrap, Version 16.12.1r, RELEASE SOFTWARE (P)`

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.

On Cisco Catalyst 9500 Series Switches, the FPGA upgrade process is part of the software image upgrade. On Cisco Catalyst 9500 Series Switches – High Performance, the FPGA upgrade happens automatically when the software image for Cisco IOS XE Gibraltar 16.12.1 boots the first time. The FPGA version does not downgrade when you downgrade the software image.

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.

After completing the upgrade procedure, you can verify the FPGA version against the value in the table below. Enter the **version -v** command in ROMMON mode.

Platform	FPGA Version in Cisco IOS XE Gibraltar 16.12.1
Cisco Catalyst 9500 Series Switches	Secure Boot FPGA - 0x216 0x19032516
Cisco Catalyst 9500 Series Switches – High Performance	Secure Boot FPGA - 0x19031223

Software Installation Commands

Summary of Software Installation Commands **Supported starting from Cisco IOS XE Everest 16.6.2 and later releases**	
To install and activate the specified file, and to commit changes to be persistent across reloads: **`install add file`** *`filename`* [**`activate commit`**] To separately install, activate, commit, cancel, or remove the installation file: **`install ?`**	
add file tftp: *filename*	Copies the install file package from a remote location to the device and performs a compatibility check for the platform and image versions.
activate [**auto-abort-timer**]	Activates the file, and reloads the device. The **auto-abort-timer** keyword automatically rolls back image activation.
commit	Makes changes persistent over reloads.
rollback to committed	Rolls back the update to the last committed version.
abort	Cancels file activation, and rolls back to the version that was running before the current installation procedure started.
remove	Deletes all unused and inactive software installation files.

Note The **request platform software** commands are deprecated starting from Cisco IOS XE Gibraltar 16.10.1. The commands are visible on the CLI in this release and you can configure them, but we recommend that you use the **install** commands to upgrade or downgrade.

Summary of request platform software Commands **Note** **This table of commands is not supported on Cisco Catalyst 9500 Series Switches - High Performance.**	
`Device# request platform software package ?`	
clean	Cleans unnecessary package files from media
copy	Copies package to media
describe	Describes package content
expand	Expands all-in-one package to media
install	Installs the package
uninstall	Uninstalls the package
verify	Verifies In Service Software Upgrade (ISSU) software package compatibility

Upgrading with In Service Software Upgrade (ISSU) with Cisco StackWise Virtual

Follow these instructions to perform In Service Software Upgrade (ISSU) to Cisco IOS XE Gibraltar 16.12.1 with Cisco StackWise Virtual, in install mode.

Before you begin

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

When upgrading from ...	To...
Cisco IOS XE Fuji 16.9.3 or Cisco IOS XE Fuji 16.9.4	Cisco IOS XE Gibraltar 16.12.x

Note Downgrade with ISSU is not supported. To downgrade, follow the instructions in the Downgrading in Install Mode, on page 40 section.

For more information about ISSU release support and recommended releases, see Technical References → In-Service Software Upgrade (ISSU).

Procedure

Step 1 **enable**

Enables privileged EXEC mode. Enter your password if prompted.

```
Switch# enable
```

Step 2 **show version | in INSTALL** or **show version | in System image**

On the Catalyst 9500 Series Switches, use **show version | in INSTALL** command to check the boot mode. ISSU is supported only in install mode. You cannot perform ISSU if the switch is booted in bundle mode.

```
Switch# show version | in INSTALL
Switch Ports Model              SW Version        SW Image              Mode
------ ----- -----              ----------        ----------            ----
*    1 12    C9500-12Q          16.12.1             CAT9K_IOSXE         INSTALL
     2 12    C9500-12Q          16.12.1             CAT9K_IOSXE         INSTALL
```

On Catalyst 9500 Series Switches - High Performance, use **show version | in System image** to check if the switch booted into IOS via " boot flash:packages.conf ". The output should display the following:

```
Switch# show version | in System image
System image file is "flash:packages.conf"
```

You cannot perform ISSU if the switch is booted in bundle mode. If you perform ISSU in bundle mode, you will see the following error.

```
*Nov 13 14:55:57.338: %INSTALL-5-INSTALL_START_INFO: Chassis 1 R1/0: install_engine: Started
 install one-shot ISSU flash:cat9k_iosxe.16.12.02.SPA.bininstall_add_activate_commit: Adding
 ISSU
ERROR: install_add_activate_commit: One-Shot ISSU operation is not supported in bundle boot
 mode
FAILED: install_add_activate_commit  exit(1) Tue Nov 13 14:56:03 UTC 2018
```

Step 3 **dir flash: | in free**

Use this command to check if there is sufficient available memory on flash. Ensure that you have at least 1GB of space in flash to expand a new image.

```
Switch# dir flash: | in free
11353194496 bytes total (8565174272 bytes free)
```

Step 4 **show redundancy**

Use this command to check if the switch is in SSO mode.

```
Switch# show redundancy
Redundant System Information :
------------------------------
       Available system uptime = 4 minutes
Switchovers system experienced = 0
              Standby failures = 0
        Last switchover reason = none

                 Hardware Mode = Duplex
    Configured Redundancy Mode = sso
     Operating Redundancy Mode = sso
              Maintenance Mode = Disabled
                Communications = Up
<output truncated>
```

Step 5 **show boot system**

Use this command to verify that the manual boot variable is set to **no**.

```
Switch# show boot system
Current Boot Variables:
BOOT variable = flash:packages.conf;
MANUAL_BOOT variable = no

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

If the manual boot variable is set to **yes**, use the **no boot manual** command in global configuration mode to set the switch for autoboot.

Step 6 **show issu state** [*detail*]

Use this command to verify that no other ISSU process is in progress.

```
Switch# show issu state detail
--- Starting local lock acquisition on chassis 2 ---
Finished local lock acquisition on chassis 2

No ISSU operation is in progress

Switch#
```

Step 7 **show install summary**

Use this command to verify that the state of the image is *Activated & Committed*. Clear the install state if the state is not *Activated & Committed*.

```
Switch# show install summary
[ Switch 1 2 ] Installed Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted,
            C - Activated & Committed, D - Deactivated & Uncommitted
--------------------------------------------------------------------------------
Type  St   Filename/Version
--------------------------------------------------------------------------------
IMG   C    16.12.2.0.2433
```

Step 8 **install add file activate issu commit**

Use this command to automate the sequence of all the upgrade procedures, including downloading the images to both the switches, expanding the images into packages, and upgrading each switch as per the procedures.

```
Switch# install add file tftp:cat9k_iosxe.16.12.01.SPA.bin activate issu commit
```

The following sample output displays installation of Cisco IOS XE Gibraltar 16.12.1 software image with ISSU procedure.

```
Switch# install add file tftp:cat9k_iosxe.16.12.01.SPA.bin activate issu commit
install_add_activate_commit: START Thu Jul 21 06:16:32 UTC 2019
Downloading file tftp://172.27.18.5//cat9k_iosxe.16.12.01.SPA.bin

*Jul 21 06:16:34.064: %INSTALL-5-INSTALL_START_INFO: Switch 1 R0/0: install_engine: Started
 install one-shot ISSU tftp://172.27.18.5//cat9k_iosxe.16.12.01.SPA.binFinished downloading
 file tftp://172.27.18.5//cat9k_iosxe.16.12.01.SPA.bin to flash:cat9k_iosxe.16.12.01.SPA.bin
install_add_activate_commit: Adding ISSU

--- Starting initial file syncing ---
```

```
[1]: Copying flash:cat9k_iosxe.16.12.01.SPA.bin from switch 1 to switch 2
[2]: Finished copying to switch 2
Info: Finished copying flash:cat9k_iosxe.16.12.01.SPA.bin to the selected switch(es)
Finished initial file syncing

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

install_add_activate_commit: Activating ISSU

NOTE: Going to start Oneshot ISSU install process

STAGE 0: Initial System Level Sanity Check before starting ISSU
================================================
--- Verifying install_issu supported ---
--- Verifying standby is in Standby Hot state ---
--- Verifying booted from the valid media ---
--- Verifying AutoBoot mode is enabled ---
Finished Initial System Level Sanity Check


STAGE 1: Installing software on Standby
================================================
--- Starting install_remote ---
Performing install_remote on Chassis remote
[2] install_remote package(s) on switch 2
[2] Finished install_remote on switch 2
install_remote: Passed on [2]
Finished install_remote


STAGE 2: Restarting Standby
================================================
--- Starting standby reload ---
Finished standby reload

--- Starting wait for Standby to reach terminal redundancy state ---

*Jul 21 06:24:16.426: %SMART_LIC-5-EVAL_START: Entering evaluation period
*Jul 21 06:24:16.426: %SMART_LIC-5-EVAL_START: Entering evaluation period
*Jul 21 06:24:16.466: %HMANRP-5-CHASSIS_DOWN_EVENT: Chassis 2 gone DOWN!
*Jul 21 06:24:16.497: %REDUNDANCY-3-STANDBY_LOST: Standby processor fault (PEER_NOT_PRESENT)
*Jul 21 06:24:16.498: %REDUNDANCY-3-STANDBY_LOST: Standby processor fault (PEER_DOWN)
*Jul 21 06:24:16.498: %REDUNDANCY-3-STANDBY_LOST: Standby processor fault
(PEER_REDUNDANCY_STATE_CHANGE)
*Jul 21 06:24:16.674: %RF-5-RF_RELOAD: Peer reload. Reason: EHSA standby down
*Jul 21 06:24:16.679: %IOSXE_REDUNDANCY-6-PEER_LOST: Active detected switch 2 is no longer
 standby
*Jul 21 06:24:16.416: %NIF_MGR-6-PORT_LINK_DOWN: Switch 1 R0/0: nif_mgr: Port 1 on front
side stack link 0 is DOWN.
*Jul 21 06:24:16.416: %NIF_MGR-6-PORT_CONN_DISCONNECTED: Switch 1 R0/0: nif_mgr: Port 1 on
 front side stack link 0 connection has DISCONNECTED: CONN_ERR_PORT_LINK_DOWN_EVENT
*Jul 21 06:24:16.416: %NIF_MGR-6-STACK_LINK_DOWN: Switch 1 R0/0: nif_mgr: Front side stack
 link 0 is DOWN.
*Jul 21 06:24:16.416: %STACKMGR-6-STACK_LINK_CHANGE: Switch 1 R0/0: stack_mgr: Stack port
1 on Switch 1 is down
```

```
<output truncated>

*Jul 21 06:29:36.393: %IOSXE_REDUNDANCY-6-PEER: Active detected switch 2 as standby.
*Jul 21 06:29:36.392: %STACKMGR-6-STANDBY_ELECTED: Switch 1 R0/0: stack_mgr: Switch 2 has
been elected STANDBY.
*Jul 21 06:29:41.397: %REDUNDANCY-5-PEER_MONITOR_EVENT: Active detected a standby insertion
 (raw-event=PEER_FOUND(4))
*Jul 21 06:29:41.397: %REDUNDANCY-5-PEER_MONITOR_EVENT: Active detected a standby insertion
 (raw-event=PEER_REDUNDANCY_STATE_CHANGE(5))
*Jul 21 06:29:42.257: %REDUNDANCY-3-IPC: IOS versions do not match.
*Jul 21 06:30:24.323: %HA_CONFIG_SYNC-6-BULK_CFGSYNC_SUCCEED: Bulk Sync succeededFinished
wait for Standby to reach terminal redundancy state


*Jul 21 06:30:25.325: %RF-5-RF_TERMINAL_STATE: Terminal state reached for (SSO)
STAGE 3: Installing software on Active
================================================
--- Starting install_active ---
Performing install_active on Chassis 1

<output truncated>

[1] install_active package(s) on switch 1
[1] Finished install_active on switch 1
install_active: Passed on [1]
Finished install_active


STAGE 4: Restarting Active (switchover to standby)
================================================
--- Starting active reload ---
New software will load after reboot process is completed
SUCCESS: install_add_activate_commit  Thu Jul 21 23:06:45 UTC 2019
Jul 21 23:06:45.731: %INSTALL-5-INSTALL_COMPLETED_INFO: R0/0: install_engine: Completed
install one-shot ISSU flash:cat9k_iosxe.16.12.01.SPA.bin
Jul 21 23:06:47.509: %PMAN-5-EXITACTION: F0/0: pvp: Process manager is exiting: reload fp
action requested
Jul 21 23:06:48.776: %PM

Initializing Hardware...

System Bootstrap, Version 16.12.1r, RELEASE SOFTWARE (P)
Compiled Fri 08/17/2018 10:48:42.68 by rel

Current ROMMON image : Primary
Last reset cause     : PowerOn
C9500-40X platform with 16777216 Kbytes of main memory

boot: attempting to boot from [flash:packages.conf]
boot: reading file packages.conf
#
################################################################################################################################


Jul 21 23:08:30.238: %PMAN-5-EXITACTION: C0/0: pvp: Process manager is exiting:

Waiting for 120 seconds for other switches to boot
######################
Switch number is 1
All switches in the stack have been discovered. Accelerating discovery
```

```
Switch console is now available


Press RETURN to get started.




Jul 21 23:14:17.080: %INSTALL-5-INSTALL_START_INFO: R0/0: install_engine: Started install
commit
Jul 21 23:15:48.445: %INSTALL-5-INSTALL_COMPLETED_INFO: R0/0: install_engine: Completed
install commit ISSU
```

Step 9 **show version**

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 Gibraltar 16.12.1 image on the device:

```
Switch# show version
Cisco IOS XE Software, Version 16.12.01
Cisco IOS Software [Gibraltar], Catalyst L3 Switch Software (CAT9K_IOSXE), Version 16.12.1,
 RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2019 by Cisco Systems, Inc.
<output truncated>
```

Step 10 **show issu state** [*detail*]

Use this command to verify that no ISSU process is in pending state.

```
Switch# show issu state detail
--- Starting local lock acquisition on chassis 2 ---
Finished local lock acquisition on chassis 2

No ISSU operation is in progress

Switch#
```

Step 11 **exit**

Exits privileged EXEC mode and returns to user EXEC mode.

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**

Before you begin

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 Gibraltar 16.12.1 (for Cisco Catalyst 9500 Series Switches) Cisco IOS XE Gibraltar 16.12.1c (for Cisco Catalyst 9500 Series Switches - High Performance)
Cisco IOS XE Everest 16.6.2 or later releases	On Cisco Catalyst 9500 Series Switches use either **install** commands or **request platform software** commands	
Cisco IOS XE Gibraltar 16.11.x	On Cisco Catalyst 9500 Series Switches - High Performance use **install** commands	

The sample output in this section displays upgrade from

- Cisco IOS XE Everest 16.5.1a to Cisco IOS XE Gibraltar 16.12.1 using **request platform software** commands.
- Cisco IOS XE Everest 16.6.3 to Cisco IOS XE Gibraltar 16.12.1 using **install** commands.

Procedure

Step 1 Clean Up

Ensure that you have at least 1GB of space in flash to expand a new image. Clean up old installation files in case of insufficient space.

- **request platform software package clean**
- **install remove inactive**

The following sample output displays the cleaning up of unused files, by using the **request platform software package clean** command for upgrade scenario Cisco IOS XE Everest 16.5.1a to Cisco IOS XE Gibraltar 16.12.1.

```
Switch# request platform software package clean
Running command on switch 1
Cleaning up unnecessary package files
No path specified, will use booted path flash:packages.conf
Cleaning flash:
Scanning boot directory for packages ... done.
Preparing packages list to delete ...
cat9k-cc_srdriver.16.05.01a.SPA.pkg
File is in use, will not delete.
cat9k-espbase.16.05.01a.SPA.pkg
File is in use, will not delete.
cat9k-guestshell.16.05.01a.SPA.pkg
File is in use, will not delete.
cat9k-rpbase.16.05.01a.SPA.pkg
File is in use, will not delete.
cat9k-rpboot.16.05.01a.SPA.pkg
File is in use, will not delete.
cat9k-sipbase.16.05.01a.SPA.pkg
File is in use, will not delete.
cat9k-sipspa.16.05.01a.SPA.pkg
File is in use, will not delete.
cat9k-srdriver.16.05.01a.SPA.pkg
File is in use, will not delete.
```

```
cat9k-webui.16.05.01a.SPA.pkg
File is in use, will not delete.
cat9k-wlc.16.05.01a.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:
[1]:
/flash/cat9k-cc_srdriver.16.06.01..SPA.pkg
/flash/cat9k-espbase.16.06.01.SPA.pkg
/flash/cat9k-guestshell.16.06.01.SPA.pkg
/flash/cat9k-rpbase.16.06.01.SPA.pkg
/flash/cat9k-rpboot.16.06.01.SPA.pkg
/flash/cat9k-sipbase.16.06.01.SPA.pkg
/flash/cat9k-sipspa.16.06.01.SPA.pkg
/flash/cat9k-srdriver.16.06.01.SPA.pkg
/flash/cat9k-webui.16.06.01.SPA.pkg
/flash/cat9k_iosxe.16.05.01a.SPA.conf
/flash/cat9k_iosxe.16.06.01.SPA.bin
/flash/packages.conf.00-

Do you want to proceed? [y/n]y
[1]:
Deleting file flash:cat9k-cc_srdriver.16.06.01.SPA.pkg ... done.
Deleting file flash:cat9k-espbase.16.06.01.SPA.pkg ... done.
Deleting file flash:cat9k-guestshell.16.06.01.SPA.pkg ... done.
Deleting file flash:cat9k-rpbase.16.06.01.SPA.pkg ... done.
Deleting file flash:cat9k-rpboot.16.06.01.SPA.pkg ... done.
Deleting file flash:cat9k-sipbase.16.06.01.SPA.pkg ... done.
Deleting file flash:cat9k-sipspa.16.06.01.SPA.pkg ... done.
Deleting file flash:cat9k-srdriver.16.06.01.SPA.pkg ... done.
Deleting file flash:cat9k-webui.16.06.01.SPA.pkg ... done.
Deleting file flash:cat9k_iosxe.16.05.01a.SPA.conf ... done.
Deleting file flash:cat9k_iosxe.16.06.01.SPA.bin ... done.
Deleting file flash:packages.conf.00- ... done.
SUCCESS: Files deleted.
Switch#
```

The following sample output displays the cleaning up of unused files, by using the **install remove inactive** command, for upgrade scenario Cisco IOS XE Everest 16.6.3 to Cisco IOS XE Gibraltar 16.12.1:

```
Switch# install remove inactive

install_remove: START Mon Jul 22 19:51:48 UTC 2019
Cleaning up unnecessary package files
Scanning boot directory for packages ... done.
Preparing packages list to delete ...
done.

The following files will be deleted:
[switch 1]:
/flash/cat9k-cc_srdriver.16.06.03.SPA.pkg
/flash/cat9k-espbase.16.06.03.SPA.pkg
/flash/cat9k-guestshell.16.06.03.SPA.pkg
/flash/cat9k-rpbase.16.06.03.SPA.pkg
/flash/cat9k-rpboot.16.06.03.SPA.pkg
/flash/cat9k-sipbase.16.06.03.SPA.pkg
/flash/cat9k-sipspa.16.06.03.SPA.pkg
/flash/cat9k-srdriver.16.06.03.SPA.pkg
/flash/cat9k-webui.16.06.03.SPA.pkg
/flash/cat9k-wlc.16.06.03.SPA.pkg
```

```
/flash/packages.conf

Do you want to remove the above files? [y/n]y
[switch 1]:
Deleting file flash:cat9k-cc_srdriver.16.06.03.SPA.pkg ... done.
Deleting file flash:cat9k-espbase.16.06.03.SPA.pkg ... done.
Deleting file flash:cat9k-guestshell.16.06.03.SPA.pkg ... done.
Deleting file flash:cat9k-rpbase.16.06.03.SPA.pkg ... done.
Deleting file flash:cat9k-rpboot.16.06.03.SPA.pkg ... done.
Deleting file flash:cat9k-sipbase.16.06.03.SPA.pkg ... done.
Deleting file flash:cat9k-sipspa.16.06.03.SPA.pkg ... done.
Deleting file flash:cat9k-srdriver.16.06.03.SPA.pkg ... done.
Deleting file flash:cat9k-webui.16.06.03.SPA.pkg ... done.
Deleting file flash:cat9k-wlc.16.06.03.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 22 19:52:25 UTC 2019
Switch#
```

Step 2 Copy new image to flash

a) **copy tftp: flash:**

Use this command to copy the new image to flash: (or skip this step if you want to use the new image from your TFTP server)

```
Switch# copy tftp://10.8.0.6//cat9k_iosxe.16.12.01.SPA.bin flash:

Destination filename [cat9k_iosxe.16.12.01.SPA.bin]?
Accessing tftp://10.8.0.6//cat9k_iosxe.16.12.01.SPA.bin...
Loading /cat9k_iosxe.16.12.01.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**

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 22 2019 10:18:11 -07:00 cat9k_iosxe.16.12.01.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
Switch(config)# exit
```

b) **write memory**

Use this command to save boot settings.

```
Switch# write memory
```

c) **show boot system**

Use this command to verify that the boot variable is set to **flash:packages.conf** and the manual boot variable is set to **no**.

The output should display the following values of these variables:

BOOT variable = flash:packages.conf

MANUAL_BOOT variable = no

```
Switch# show boot system
```

Step 4 Software install image to flash

- **request platform software package install**
- **install add file activate commit**

The following sample output displays installation of the Cisco IOS XE Gibraltar 16.12.1 software image to flash, by using the **request platform software package install** command, for upgrade scenario Cisco IOS XE Everest 16.5.1a to Cisco IOS XE Gibraltar 16.12.1.

```
Switch# request platform software package install switch all file
flash:cat9k_iosxe.16.12.01.SPA.bin

--- Starting install local lock acquisition on switch 1 ---
Finished install local lock acquisition on switch 1

Expanding image file: flash:cat9k_iosxe.16.12.01.SPA.bin
[]: Finished copying to switch
[1]: Expanding file
[1]: Finished expanding all-in-one software package in switch 1
SUCCESS: Finished expanding all-in-one software package.
[1]: Performing install
SUCCESS: install finished
[1]: install package(s) on switch 1
--- Starting list of software package changes ---
Old files list:
Removed cat9k-cc_srdriver.16.05.01a.SPA.pkg
Removed cat9k-espbase.16.05.01a.SPA.pkg
Removed cat9k-guestshell.16.05.01a.SPA.pkg
Removed cat9k-rpbase.16.05.01a.SPA.pkg
Removed cat9k-rpboot.16.05.01a.SPA.pkg
Removed cat9k-sipbase.16.05.01a.SPA.pkg
Removed cat9k-sipspa.16.05.01a.SPA.pkg
Removed cat9k-srdriver.16.05.01a.SPA.pkg
Removed cat9k-webui.16.05.01a.SPA.pkg
Removed cat9k-wlc.16.05.01a.SPA.pkg
New files list:
Added cat9k-cc_srdriver.16.12.01.SPA.pkg
Added cat9k-espbase.16.12.01.SPA.pkg
Added cat9k-guestshell.16.12.01.SPA.pkg
Added cat9k-rpbase.16.12.01.SPA.pkg
Added cat9k-rpboot.16.12.01.SPA.pkg
Added cat9k-sipbase.16.12.01.SPA.pkg
```

```
Added cat9k-sipspa.16.12.01.SPA.pkg
Added cat9k-srdriver.16.12.01.SPA.pkg
Added cat9k-webui.16.12.01.SPA.pkg
Finished list of software package changes
SUCCESS: Software provisioned. New software will load on reboot.
[1]: Finished install successful on switch 1
Checking status of install on [1]
[1]: Finished install in switch 1
SUCCESS: Finished install: Success on [1]
```

Note
Old files listed in the logs are not removed from flash.

The following sample output displays installation of the Cisco IOS XE Gibraltar 16.12.1 software image to flash, by using the **install add file activate commit** command, for upgrade scenario Cisco IOS XE Everest 16.6.3 to Cisco IOS XE Gibraltar 16.12.1:

```
Switch# install add file flash:cat9k_iosxe.16.12.01.SPA.bin activate commit

install_add_activate_commit: START Mon Jul 22 19:54:51 UTC 2019

System configuration has been modified.
Press Yes(y) to save the configuration and proceed.
Press No(n) for proceeding without saving the configuration.
Press Quit(q) to exit, you may save configuration and re-enter the command. [y/n/q]yBuilding
 configuration...

[OK]Modified configuration has been saved

*Mar 06 19:54:55.633: %IOSXE-5-PLATFORM: Switch 1 R0/0: Mar 06 19:54:55 install_engine.sh:

%INSTALL-5-INSTALL_START_INFO: Started install one-shot
flash:cat9k_iosxe.16.12.01.SPA.bininstall_add_activate_commit: Adding PACKAGE

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 ---
Info: Finished copying flash:cat9k_iosxe.16.12.01.SPA.bin to the selected switch(es)
Finished initial file syncing

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

install_add_activate_commit: Activating PACKAGE
Following packages shall be activated:
/flash/cat9k-wlc.16.12.01.SPA.pkg
/flash/cat9k-webui.16.12.01.SPA.pkg
/flash/cat9k-srdriver.16.12.01.SPA.pkg
/flash/cat9k-sipspa.16.12.01.SPA.pkg
/flash/cat9k-sipbase.16.12.01.SPA.pkg
/flash/cat9k-rpboot.16.12.01.SPA.pkg
/flash/cat9k-rpbase.16.12.01.SPA.pkg
/flash/cat9k-guestshell.16.12.01.SPA.pkg
/flash/cat9k-espbase.16.12.01.SPA.pkg
/flash/cat9k-cc_srdriver.16.12.01.SPA.pkg

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

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

--- Starting Commit ---
Performing Commit on all members

*Mar 06 19:57:41.145: %IOSXE-5-PLATFORM: Switch 1 R0/0: Mar 06 19:57:41 rollback_timer.sh:

%INSTALL-5-INSTALL_AUTO_ABORT_TIMER_PROGRESS: Install auto abort timer will expire in 7200
 seconds [1] Commit package(s) on switch 1
[1] Finished Commit on switch 1
Checking status of Commit on [1]
Commit: Passed on [1]
Finished Commit

Install will reload the system now!
SUCCESS: install_add_activate_commit Mon Jul 22 19:57:48 UTC 2019
Switch#
```

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 **dir flash:**

After the software has been successfully installed, use this command to verify that the flash partition has ten new `.pkg` files and three `.conf` files.

The following is sample output of the **dir flash:** command for upgrade scenario Cisco IOS XE Everest 16.5.1a to Cisco IOS XE Gibraltar 16.12.1:

```
Switch# dir flash:*.pkg

Directory of flash:/*.pkg
Directory of flash:/
475140 -rw- 2012104   Jul 26 2017 09:52:41 -07:00 cat9k-cc_srdriver.16.05.01a.SPA.pkg
475141 -rw- 70333380  Jul 26 2017 09:52:44 -07:00 cat9k-espbase.16.05.01a.SPA.pkg
475142 -rw- 13256     Jul 26 2017 09:52:44 -07:00 cat9k-guestshell.16.05.01a.SPA.pkg
475143 -rw- 349635524 Jul 26 2017 09:52:54 -07:00 cat9k-rpbase.16.05.01a.SPA.pkg
475149 -rw- 24248187  Jul 26 2017 09:53:02 -07:00 cat9k-rpboot.16.05.01a.SPA.pkg
475144 -rw- 25285572  Jul 26 2017 09:52:55 -07:00 cat9k-sipbase.16.05.01a.SPA.pkg
475145 -rw- 20947908  Jul 26 2017 09:52:55 -07:00 cat9k-sipspa.16.05.01a.SPA.pkg
475146 -rw- 2962372   Jul 26 2017 09:52:56 -07:00 cat9k-srdriver.16.05.01a.SPA.pkg
475147 -rw- 13284288  Jul 26 2017 09:52:56 -07:00 cat9k-webui.16.05.01a.SPA.pkg
475148 -rw- 13248     Jul 26 2017 09:52:56 -07:00 cat9k-wlc.16.05.01a.SPA.pkg

491524 -rw- 25711568  Jul 22 2019 11:49:33 -07:00 cat9k-cc_srdriver.16.12.01.SPA.pkg
491525 -rw- 78484428  Jul 22 2019 11:49:35 -07:00 cat9k-espbase.16.12.01.SPA.pkg
491526 -rw- 1598412   Jul 22 2019 11:49:35 -07:00 cat9k-guestshell.16.12.01.SPA.pkg
491527 -rw- 404153288 Jul 22 2019 11:49:47 -07:00 cat9k-rpbase.16.12.01.SPA.pkg
491533 -rw- 31657374  Jul 22 2019 11:50:09 -07:00 cat9k-rpboot.16.12.01.SPA.pkg
491528 -rw- 27681740  Jul 22 2019 11:49:48 -07:00 cat9k-sipbase.16.12.01.SPA.pkg
491529 -rw- 52224968  Jul 22 2019 11:49:49 -07:00 cat9k-sipspa.16.12.01.SPA.pkg
491530 -rw- 31130572  Jul 22 2019 11:49:50 -07:00 cat9k-srdriver.16.12.01.SPA.pkg
491531 -rw- 14783432  Jul 22 2019 11:49:51 -07:00 cat9k-webui.16.12.01.SPA.pkg
491532 -rw- 9160      Jul 22 2019 11:49:51 -07:00 cat9k-wlc.16.12.01.SPA.pkg
```

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

The following is sample output of the **dir flash:** command for the Cisco IOS XE Everest 16.6.3 to Cisco IOS XE Gibraltar 16.12.1 upgrade scenario:

```
Switch# dir flash:

Directory of flash:/
475140 -rw- 2012104   Jul 26 2017 09:52:41 -07:00 cat9k-cc_srdriver.16.06.03.SPA.pkg
475141 -rw- 70333380  Jul 26 2017 09:52:44 -07:00 cat9k-espbase.16.06.03.SPA.pkg
475142 -rw- 13256     Jul 26 2017 09:52:44 -07:00 cat9k-guestshell.16.06.03.SPA.pkg
475143 -rw- 349635524 Jul 26 2017 09:52:54 -07:00 cat9k-rpbase.16.06.03.SPA.pkg
475149 -rw- 24248187  Jul 26 2017 09:53:02 -07:00 cat9k-rpboot.16.06.03.SPA.pkg
475144 -rw- 25285572  Jul 26 2017 09:52:55 -07:00 cat9k-sipbase.16.06.03.SPA.pkg
475145 -rw- 20947908  Jul 26 2017 09:52:55 -07:00 cat9k-sipspa.16.06.03.SPA.pkg
475146 -rw- 2962372   Jul 26 2017 09:52:56 -07:00 cat9k-srdriver.16.06.03.SPA.pkg
475147 -rw- 13284288  Jul 26 2017 09:52:56 -07:00 cat9k-webui.16.06.03.SPA.pkg
475148 -rw- 13248     Jul 26 2017 09:52:56 -07:00 cat9k-wlc.16.06.03.SPA.pkg

491524 -rw- 25711568  Jul 22 2019 11:49:33 -07:00 cat9k-cc_srdriver.16.12.01.SPA.pkg
491525 -rw- 78484428  Jul 22 2019 11:49:35 -07:00 cat9k-espbase.16.12.01.SPA.pkg
491526 -rw- 1598412   Jul 22 2019 11:49:35 -07:00 cat9k-guestshell.16.12.01.SPA.pkg
491527 -rw- 404153288 Jul 22 2019 11:49:47 -07:00 cat9k-rpbase.16.12.01.SPA.pkg
491533 -rw- 31657374  Jul 22 2019 11:50:09 -07:00 cat9k-rpboot.16.12.01.SPA.pkg
491528 -rw- 27681740  Jul 22 2019 11:49:48 -07:00 cat9k-sipbase.16.12.01.SPA.pkg
491529 -rw- 52224968  Jul 22 2019 11:49:49 -07:00 cat9k-sipspa.16.12.01.SPA.pkg
491530 -rw- 31130572  Jul 22 2019 11:49:50 -07:00 cat9k-srdriver.16.12.01.SPA.pkg
491531 -rw- 14783432  Jul 22 2019 11:49:51 -07:00 cat9k-webui.16.12.01.SPA.pkg
491532 -rw- 9160      Jul 22 2019 11:49:51 -07:00 cat9k-wlc.16.12.01.SPA.pkg

11353194496 bytes total (9544245248 bytes free)
Switch#
```

The following sample output 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.16.12.01.SPA.conf`— a backup copy of the newly installed packages.conf file

```
Switch# dir flash:*.conf

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

434197 -rw- 7406 Jul 22 2019 10:59:16 -07:00 packages.conf
516098 -rw- 7406 Jul 22 2019 10:58:08 -07:00 cat9k_iosxe.16.12.01.SPA.conf
11353194496 bytes total (8963174400 bytes free)
```

Step 6 Reload

This step is required only if you install the software image to flash by using the **request platform software package install** command.

a) **reload**

Use this command to reload the switch.

```
Switch# reload
```

b) **boot flash:**

If your switches are configured with auto boot, then the stack will automatically boot up with the new image. If not, you can manually boot flash:packages.conf

```
Switch: boot flash:packages.conf
```

c) **show version**

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

Note
When you boot the new image, the boot loader is automatically updated, but the new bootloader version is not displayed in the output until the next reload.

The following sample output of the **show version** command displays the Cisco IOS XE Gibraltar 16.12.1 image on the Cisco Catalyst 9500 Series Switches:

```
Switch# show version
Cisco IOS XE Software, Version 16.12.01
Cisco IOS Software [Gibraltar], Catalyst L3 Switch Software (CAT9K_IOSXE), Version
16.12.1, RELEASE SOFTWARE (fc4)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2019 by Cisco Systems, Inc.
Compiled Tue 30-Jul-19 19:26 by mcpre

<output truncated>
```

The following sample output of the **show version** command displays the Cisco IOS XE Gibraltar 16.12.1c image on the Cisco Catalyst 9500 Series Switches - High Performance:

```
Switch# show version
Cisco IOS XE Software, Version 16.12.01c
Cisco IOS Software [Gibraltar], Catalyst L3 Switch Software (CAT9K_IOSXE), Version
16.12.1c, RELEASE SOFTWARE (fc4)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2019 by Cisco Systems, Inc.
Compiled Tue 30-Jul-19 19:26 by mcpre

<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 via " boot flash:packages.conf ."

Before you begin

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

When downgrading from ...	Use these commands...	To downgrade to...
Cisco IOS XE Gibraltar 16.12.1 (for Cisco Catalyst 9500 Series Switches)	On Cisco Catalyst 9500 Series Switches, either **install** commands or **request platform software** commands	Cisco IOS XE Gibraltar 16.11.x or an earlier release.
Cisco IOS XE Gibraltar 16.12.1c (for Cisco Catalyst 9500 Series Switches - High Performance)	On Cisco Catalyst 9500 Series Switches - High Performance use **install** commands	Cisco IOS XE Gibraltar 16.11.x

The sample output in this section shows downgrade from Cisco IOS XE Gibraltar 16.12.1 to Cisco IOS XE Everest 16.6.1, by using the **install** commands.

Important 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.

Procedure

Step 1 Clean Up

Ensure that you have at least 1GB of space in flash to expand a new image. Clean up old installation files in case of insufficient space.

- **install remove inactive**
- **request platform software package clean**

The following sample output displays the cleaning up of Cisco IOS XE Gibraltar 16.12.1 files using the **install remove inactive** command:

```
Switch# install remove inactive

install_remove: START Mon Jul 22 19:51:48 UTC 2019
Cleaning up unnecessary package files
Scanning boot directory for packages ... done.
Preparing packages list to delete ...
done.

The following files will be deleted:
[switch 1]:
/flash/cat9k-cc_srdriver.16.12.01.SPA.pkg
/flash/cat9k-espbase.16.12.01.SPA.pkg
/flash/cat9k-guestshell.16.12.01.SPA.pkg
/flash/cat9k-rpbase.16.12.01.SPA.pkg
/flash/cat9k-rpboot.16.12.01.SPA.pkg
/flash/cat9k-sipbase.16.12.01.SPA.pkg
/flash/cat9k-sipspa.16.12.01.SPA.pkg
/flash/cat9k-srdriver.16.12.01.SPA.pkg
/flash/cat9k-webui.16.12.01.SPA.pkg
/flash/cat9k-wlc.16.12.01.SPA.pkg
/flash/packages.conf

Do you want to remove the above files? [y/n]y
[switch 1]:
```

```
Deleting file flash:cat9k-cc_srdriver.16.12.01.SPA.pkg ... done.
Deleting file flash:cat9k-espbase.16.12.01.SPA.pkg ... done.
Deleting file flash:cat9k-guestshell.16.12.01.SPA.pkg ... done.
Deleting file flash:cat9k-rpbase.16.12.01.SPA.pkg ... done.
Deleting file flash:cat9k-rpboot.16.12.01.SPA.pkg ... done.
Deleting file flash:cat9k-sipbase.16.12.01.SPA.pkg ... done.
Deleting file flash:cat9k-sipspa.16.12.01.SPA.pkg ... done.
Deleting file flash:cat9k-srdriver.16.12.01.SPA.pkg ... done.
Deleting file flash:cat9k-webui.16.12.01.SPA.pkg ... done.
Deleting file flash:cat9k-wlc.16.12.01.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 22 19:52:25 UTC 2019
Switch#
```

Step 2 Copy new image to flash

a) **copy tftp: flash:**

Use this command to copy the new image to flash: (or skip this step if you want to use the new image from your TFTP server)

```
Switch# copy tftp://10.8.0.6//cat9k_iosxe.16.06.01.SPA.bin flash:

Destination filename [cat9k_iosxe.16.06.01.SPA.bin]?
Accessing tftp://10.8.0.6//cat9k_iosxe.16.06.01.SPA.bin...
Loading /cat9k_iosxe.16.06.01.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 22 2019 13:35:16 -07:00 cat9k_iosxe.16.06.01.SPA.bin
11353194496 bytes total (9055866880 bytes free)
```

Step 3 Downgrade software image

- **install add file activate commit**
- **request platform software package install**

The following example displays the installation of the Cisco IOS XE Everest 16.6.1 software image to flash, by using the **install add file activate commit** command.

```
Switch# install add file flash:cat9k_iosxe.16.06.01.SPA.bin activate commit

install_add_activate_commit: START Mon Jul 22 19:54:51 UTC 2019
```

```
System configuration has been modified.
Press Yes(y) to save the configuration and proceed.
Press No(n) for proceeding without saving the configuration.
Press Quit(q) to exit, you may save configuration and re-enter the command. [y/n/q]yBuilding
 configuration...

[OK]Modified configuration has been saved

*Jul 22 19:54:55.633: %IOSXE-5-PLATFORM: Switch 1 R0/0: Jul 22 19:54:55 install_engine.sh:
 %INSTALL-
5-INSTALL_START_INFO: Started install one-shot flash:cat9k_iosxe.16.06.01.SPA.bin
install_add_activate_commit: Adding PACKAGE

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 ---
Info: Finished copying flash:cat9k_iosxe.16.06.01.SPA.bin to the selected switch(es)
Finished initial file syncing

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

install_add_activate_commit: Activating PACKAGE
Following packages shall be activated:
/flash/cat9k-wlc.16.06.01.SPA.pkg
/flash/cat9k-webui.16.06.01.SPA.pkg
/flash/cat9k-srdriver.16.06.01.SPA.pkg
/flash/cat9k-sipspa.16.06.01.SPA.pkg
/flash/cat9k-sipbase.16.06.01.SPA.pkg
/flash/cat9k-rpboot.16.06.01.SPA.pkg
/flash/cat9k-rpbase.16.06.01.SPA.pkg
/flash/cat9k-guestshell.16.06.01.SPA.pkg
/flash/cat9k-espbase.16.06.01.SPA.pkg
/flash/cat9k-cc_srdriver.16.06.01.SPA.pkg

This operation requires a reload of the system. Do you want to proceed? [y/n]y
--- Starting Activate ---
Performing Activate on all members
[1] Activate package(s) on switch 1
[1] Finished Activate on switch 1
Checking status of Activate on [1]
Activate: Passed on [1]
Finished Activate

--- Starting Commit ---
Performing Commit on all members

*Jul 22 19:57:41.145: %IOSXE-5-PLATFORM: Switch 1 R0/0: Jul 22 19:57:41 rollback_timer.sh:
 %INSTALL-
5-INSTALL_AUTO_ABORT_TIMER_PROGRESS: Install auto abort timer will expire in 7200 seconds
[1] Commit package(s) on switch 1
[1] Finished Commit on switch 1
Checking status of Commit on [1]
Commit: Passed on [1]
Finished Commit

Install will reload the system now!
```

```
SUCCESS: install_add_activate_commit Mon Jul 22 19:57:48 UTC 2019
Switch#
```

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

Step 4 Reload

a) **reload**

Use this command to reload the switch.

```
Switch# reload
```

b) **boot flash:**

If your switches are configured with auto boot, then the stack will automatically boot up with the new image. If not, you can manually boot flash:packages.conf

```
Switch: boot flash:packages.conf
```

Note
When you downgrade the software image, the boot loader does not automatically downgrade. It remains updated.

c) **show version**

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

Note
When you boot the new image, the boot loader is automatically updated, but the new bootloader version is not displayed in the output until the next reload.

The following sample output of the **show version** command displays the Cisco IOS XE Everest 16.6.1 image on the device:

```
Switch# show version
Cisco IOS XE Software, Version 16.06.01
Cisco IOS Software [Everest], Catalyst L3 Switch Software (CAT9K_IOSXE), Version 16.6.1,
 RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2017 by Cisco Systems, Inc.
Compiled Fri 16-Mar-18 06:38 by mcpre
<output truncated>
```

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 9500 Series Switches and Cisco Catalyst 9500 Series Switches - High Performance fall under these base or add-on license levels.

Base Licenses

- Network Essentials
- Network Advantage—Includes features available with the Network Essentials license and more.

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 Essentials
- DNA Advantage— Includes features available with the DNA Essentials license and more.

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://cfnng.cisco.com. An account on cisco.com is not required.

License Types

The following license types are available:

- Permanent—for a license level, and without an expiration date.
- Term—for a license level, and for a three, five, or seven year period.
- Evaluation—a license that is not registered.

License Levels - Usage Guidelines

- Base licenses (Network Essentials and Network-Advantage) are ordered and fulfilled only with a permanent license type.
- Add-on licenses (DNA Essentials and DNA Advantage) are ordered and fulfilled only with a 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.
- When ordering an add-on license with a base license, note the combinations that are permitted and those that are not permitted:

Table 6: Permitted Combinations

	DNA Essentials	DNA Advantage
Network Essentials	Yes	No

Network Advantage	Yes[3]	Yes

[3] You will be able to purchase this combination only at the time of the DNA license renewal and not when you purchase DNA-Essentials the first time.

- 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*.

Cisco Smart Licensing

Cisco Smart Licensing is a flexible licensing model that provides you with an easier, faster, and more consistent way to purchase and manage software across the Cisco portfolio and across your organization. And it's secure – you control what users can access. With Smart Licensing you get:

- Easy Activation: Smart Licensing establishes a pool of software licenses that can be used across the entire organization—no more PAKs (Product Activation Keys).
- Unified Management: Cisco License Central provides a complete view into all of your Cisco products and services in an easy-to-use portal, so you always know what you have and what you are using.
- License Flexibility: Your software is not node-locked to your hardware, so you can easily use and transfer licenses as needed.

To use Smart Licensing, you must first set up a Smart Account on Cisco License Central. For a more detailed overview on Cisco Licensing, visit the Licensing Hub.



Important Cisco Smart Licensing is the default and the only available method to manage licenses.

Deploying Smart Licensing

The following provides a process overview of a day 0 to day N deployment directly initiated from a device that is running Cisco IOS XE Fuji 16.9.1 or later releases. Links to the configuration guide provide detailed information to help you complete each one of the smaller tasks.

Procedure

Step 1 Begin by establishing a connection from your network to Cisco Smart Software Manager on cisco.com.

In the software configuration guide of the required release, see *System Management* → *Configuring Smart Licensing* → *Connecting to CSSM*

Step 2 Create and activate your Smart Account, or login if you already have one.

To create and activate Smart Account, go to Cisco Software Central → Create Smart Accounts. Only authorized users can activate the Smart Account.

Step 3 Complete the Cisco Smart Software Manager set up.

a) Accept the Smart Software Licensing Agreement.

b) Set up the required number of Virtual Accounts, users and access rights for the virtual account users.

Virtual accounts help you organize licenses by business unit, product type, IT group, and so on.

c) Generate the registration token in the Cisco Smart Software Manager portal and register your device with the token.

In the software configuration guide of the required release, see *System Management → Configuring Smart Licensing → Registering the Device in CSSM*

With this,

- The device is now in an authorized state and ready to use.
- The licenses that you have purchased are displayed in your Smart Account.

Using Smart Licensing on an Out-of-the-Box Device

Starting from Cisco IOS XE Fuji 16.9.1, if an out-of-the-box device has the software version factory-provisioned, all licenses on such a device remain in evaluation mode until registered in Cisco Smart Software Manager.

In the software configuration guide of the required release, see *System Management → Configuring Smart Licensing → Registering the Device in CSSM*

How Upgrading or Downgrading Software Affects Smart Licensing

Starting from Cisco IOS XE Fuji 16.9.1, Smart Licensing is the default and only license management solution; all licenses are managed as Smart Licenses.



Important Starting from Cisco IOS XE Fuji 16.9.1, the Right-To-Use (RTU) licensing mode is deprecated, and the associated **license right-to-use** command is no longer available on the CLI.

Note how upgrading to a release that supports Smart Licensing or moving to a release that does not support Smart Licensing affects licenses on a device:

- **When you upgrade from an earlier release to one that supports Smart Licensing**—all existing licenses remain in evaluation mode until registered in Cisco Smart Software Manager. After registration, they are made available in your Smart Account.

  In the software configuration guide of the required release, see *System Management → Configuring Smart Licensing → Registering the Device in CSSM*

- **When you downgrade to a release where Smart Licensing is not supported**—all smart licenses on the device are converted to traditional licenses and all smart licensing information on the device is removed.

Scaling Guidelines

For information about feature scaling guidelines, see the Cisco Catalyst 9500 Series Switches datasheet at:

https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9500-series-switches/datasheet-c78-738978.html

Limitations and Restrictions

With Cisco Catalyst 9500 Series Switches and Cisco Catalyst 9500 Series Switches - High Performance—If a feature is not supported on a switch model, you do not have to factor in any limitations or restrictions that may be listed here. If limitations or restrictions are listed for a feature that is supported, check if model numbers are specified, to know if they apply. If model numbers are not specified, the limitations or restrictions apply to all models in the series.

- Auto negotiation

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

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

- Control Plane Policing (CoPP)—The **show 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.

- Cisco StackWise Virtual

  - On Cisco Catalyst 9500 Series Switches, when Cisco StackWise Virtual is configured, breakout ports using 4X10G breakout cables, or the Cisco QSFP to SFP or SFP+ Adapter (QSA) module can only be used as data ports; they cannot be used to configure StackWise Virtual links (SVLs) or dual-active detective (DAD) links.

  - On Cisco Catalyst 9500 Series Switches - High Performance,

    - When Cisco StackWise Virtual is configured, breakout ports using 4X25G or 4X10G breakout cables can only be used as data ports; they cannot be used to configure SVLs or DAD links.

    - When Cisco StackWise Virtual is configured, Cisco QSA module with 10G SFP modules can be used as data ports and to configure SVLs or DAD links.

    - When Cisco StackWise Virtual is configured, Cisco QSA module with 1G SFP modules can be used as data ports and to configure DAD links; they cannot be used to configure SVLs since SVLs are not supported on 1G interfaces.

- Cisco TrustSec restrictions—Cisco TrustSec can be configured only on physical interfaces, not on logical interfaces.

- Flexible NetFlow limitations

  - You cannot configure NetFlow export using the Ethernet Management port (GigabitEthernet0/0).

- You can not configure a flow monitor on logical interfaces, such as layer 2 port-channels, loopback, tunnels.
- You can not configure multiple flow monitors of same type (ipv4, ipv6 or datalink) on the same interface for same direction.

- Hardware Limitations:
  - Use the MODE button to switch-off the beacon LED.
  - All port LED behavior is undefined until interfaces are fully initialized.
  - 1G with Cisco QSA Module (CVR-QSFP-SFP10G) is not supported on the uplink ports of the C9500-24Y4C and C9500-48Y4C models.
  - The following limitations apply to Cisco QSA Module (CVR-QSFP-SFP10G) when Cisco 1000Base-T Copper SFP (GLC-T) or Cisco 1G Fiber SFP Module for Multimode Fiber are plugged into the QSA module:
    - 1G Fiber modules over QSA do not support autonegotiation. Auto-negotiation should be disabled on the far-end devices.
    - Although visible in the CLI, the command [**no**] **speed nonegotiate** is not supported with 1G Fiber modules over QSA.
    - Only GLC-T over QSA supports auto-negotiation.
    - GLC-T supports only port speed of 1000 Mb/s over QSA. Port speeds of 10/100-Mb/s are not supported due to hardware limitation.
  - When you use Cisco QSFP-4SFP10G-CUxM Direct-Attach Copper Cables, autonegotiation is enabled by default. If the other end of the line does not support autonegotation, the link does not come up.
  - Autonegotiation is not supported on HundredGigabitEthernet1/0/49 to HundredGigabitEthernet1/0/52 uplink ports of the C9500-48Y4C models, and HundredGigabitEthernet1/0/25 to HundredGigabitEthernet1/0/28 uplink ports of the C9500-24Y4C models. Disable autonegotiation on the peer device if you are using QSFP-H40G-CUxx and QSFP-H40G-ACUxx cables.
  - For QSFP-H100G-CUxx cables, the C9500-48Y4C and C9500-24Y4C models support the cables only if both sides of the connection are either C9500-48Y4C or C9500-24Y4C.

- Interoperability limitations—When you use Cisco QSFP-4SFP10G-CUxM Direct-Attach Copper Cables, if one end of the 40G link is a Catalyst 9400 Series Switch and the other end is a Catalyst 9500 Series Switch, the link does not come up, or comes up on one side and stays down on the other. To avoid this interoperability issue between devices, apply the **speed nonegotiate** command on the Catalyst 9500 Series Switch interface. This command disables autonegotiation and brings the link up. To restore autonegotiation, use the **no speed nonegotiation** command.

- In-Service Software Upgrade (ISSU)
  - While performing ISSU from Cisco IOS XE Fuji 16.9.x to Cisco IOS XE Gibraltar 16.12.x, if **interface-id snmp-if-index**command is not configured with OSPFv3, packet loss can occur. Configure the **interface-id snmp-if-index** command either during the maintenance window or after isolating the device (by using maintenance mode feature) from the network before doing the ISSU.

- On Cisco Catalyst 9500 Series Switches (C9500-12Q, C9500-16X, C9500-24Q, C9500-40X), ISSU from Cisco IOS XE Fuji 16.9.x to Cisco IOS XE Gibraltar 16.10.x or to Cisco IOS XE Gibraltar 16.11.x is not supported.
- On Cisco Catalyst 9500 Series Switches (C9500-12Q, C9500-16X, C9500-24Q, C9500-40X), ISSU from Cisco IOS XE Fuji 16.9.x to Cisco IOS XE Gibraltar 16.12.x is not supported in the FIPs mode of operation.
- On Cisco Catalyst 9500 Series Switches - High Performance (C9500-24Y4C, C9500-32C, C9500-32QC, and C9500-48Y4C), ISSU with Cisco StackWise Virtual is supported only starting from Cisco IOS XE Gibraltar 16.12.1. Therefore, ISSU upgrades can be performed only starting from this release to a later release.
- While ISSU allows you to perform upgrades with zero downtime, we recommend you to do so during a maintenance window only.
- If a new feature introduced in a software release requires a change in configuration, the feature should not be enabled during ISSU.
- If a feature is not available in the downgraded version of a software image, the feature should be disabled before initiating ISSU.

- QoS restrictions
  - 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.

- 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
```

- VLAN Restriction—It is advisable to have well-defined segregation while defining data and voice domain during switch configuration and to maintain a data VLAN different from voice VLAN across the switch stack. If the same VLAN is configured for data and voice domains on an interface, the resulting high CPU utilization might affect the device.
- Wired Application Visibility and Control limitations:
  - NBAR2 (QoS and Protocol-discovery) configuration is allowed only on wired physical ports. It is not supported on virtual interfaces, for example, VLAN, port channel nor other logical interfaces.
  - NBAR2 based match criteria 'match protocol' is allowed only with marking or policing actions. NBAR2 match criteria will not be allowed in a policy that has queuing features configured.
  - 'Match Protocol': up to 256 concurrent different protocols in all policies.
  - NBAR2 and Legacy NetFlow cannot be configured together at the same time on the same interface. However, NBAR2 and wired AVC Flexible NetFlow can be configured together on the same interface.
  - Only IPv4 unicast (TCP/UDP) is supported.
  - AVC is not supported on management port (Gig 0/0)
  - NBAR2 attachment should be done only on physical access ports. Uplink can be attached as long as it is a single uplink and is not part of a port channel.
  - Performance—Each switch member is able to handle 500 connections per second (CPS) at less than 50% CPU utilization. Above this rate, AVC service is not guaranteed.
  - Scale—Able to handle up to 5000 bi-directional flows per 24 access ports and 10000 bi-directional flows per 48 access ports.
- YANG data modeling limitation—A maximum of 20 simultaneous NETCONF sessions are supported.
- Embedded Event Manager—Identity event detector is not supported on Embedded Event Manager.
- The File System Check (fsck) utility is not supported in install mode.
- 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.

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.

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 Gibraltar 16.12.x

There are no open caveats in this release.

Resolved Caveats in Cisco IOS XE Gibraltar 16.12.8

Identifier	Applicable Models	Description
CSCwa68343	All models	Cisco IOS XE Software for Catalyst Switches MPLS Denial of Service Vulnerability

Resolved Caveats in Cisco IOS XE Gibraltar 16.12.7

Identifier	Applicable Models	Description
CSCwa21130	Catalyst 9500 High Performance	16.12.4:Cat9kQSFP-H40G-CUxM are not recognized or listed as Unknown pluggable optics and link not up

Resolved Caveats in Cisco IOS XE Gibraltar 16.12.6

Identifier	Applicable Models	Description
CSCvv27849	All models	Cat 9K & 3K: Unexpected reload caused by the FED process.
CSCvx94722	All models	Radius protocol generate jumbo frames for dot1x packets
CSCvy25845	All models	SNMP: ifHCInOctets - snmpwalk on sub-interface octet counter does not increase

Resolved Caveats in Cisco IOS XE Gibraltar 16.12.5b

Identifier	Applicable Models	Description
CSCvx23125	Catalyst 9500 High Performance	SVL Link Instability May Result in IOMD Exhaustion
CSCvr73771	All models	Session not getting authenticated via MAB after shut/no shut of interface
CSCvv27849	All models	Cat 9K & Cat3K fed crash when running 16.12.5
CSCvw64798	All models	Cisco IOx for IOS XE Software Command Injection Vulnerability

Resolved Caveats in Cisco IOS XE Gibraltar 16.12.5

Identifier	Applicable Models	Description
CSCvr77861	Catalyst 9500 High Performance	Cat9300/C9500/C9500H switches may reload with last reload reason as LocalSoft or CpuCatastrophicErr
CSCvt60188	Catalyst 9500 High Performance	Authentication Config Removal leads to standby reload
CSCvu62273	All models	CLI should be auto-upgraded from "tacacs-server" cli to newer version while upgrading
CSCvv16874	All models	Catalyst Switch: SISF Crash due to a memory leak
CSCvw63161	All models	ZTP failing with error in creating downloaded_script.py
CSCvw74061	Catalyst 9500	Cat9300 & Cat9500 series switches may see unexpected reloads due to Localsoft or CpuCatastrophicErr

Resolved Caveats in Cisco IOS XE Gibraltar 16.12.4

Identifier	Description
CSCvk13860	C9K switch does not boot with IOS above 16.8.1a
CSCvp77133	systemd service flash-recovery.service always in the running mode
CSCvq17488	show module info for active switch is n/a after booting remaining switches
CSCvr41932	17.1.1 - Memory leak @ SAMsgThread.
CSCvr82708	Device crash when upgrading via ISSU
CSCvr86162	Output of crepSegmentComplete is incorrect for the switches with single Edge port
CSCvs14641	C9500H: SFPs no longer recognized after OIR
CSCvs22896	DHCPv6 RELAY-REPLY packet is being dropped
CSCvs71084	Cat9k - Not able to apply Et-analytics on an interface
CSCvs73383	"show mac address-table" does not show remote EIDs when vlan filter used
CSCvs74413	Modifying the child service policy causes the standby chassis/switch to reboot due to sync failure.
CSCvs75010	Traffic forwarding stops when Session Idle time out is configured 10 sec with active traffic running
CSCvs77781	Critical auth failing to apply DEFAULT_CRITICAL_DATA_TEMPLATE

Identifier	Description
CSCvs89792	INJECT_FEATURE_ESCAPE: Egress IP packet delivered via legacy inject path for NetBios packets
CSCvs91195	Crash Due to AutoSmart Port Macros
CSCvs91593	offer is dropped in data vlan with dhcp snooping using dot1x/mab
CSCvs97551	Unable to use VLAN range 4084-4095 for any business operations
CSCvt01187	Eigrp neighbor down up occurred frequently
CSCvt17460	SVL/DAD links will be err-disabled when there is link-flap due to faulty SFPs
CSCvt30243	connectivity issue after moving client from dot1x enable port to non dot1x port
CSCvt31437	DAD links go into err-disable due to portfast bpduguard global config when both members reload
CSCvt32195	Interfaces are not usable after switchport is enabled/disabled when one of the SVL switch is down
CSCvt34738	SVL // DHCP discover relayed in a different vlan
CSCvt35095	Connection for L3 interfaces and SVIs may go down when power cycled SVL active switch comes online.
CSCvt35866	1G GLC-T DAD link wont come up in 16.12.3, works fine 16.12.2 and 17.1.1
CSCvt39133	OID cswDistrStackPhyPortInfo triggers memory leak
CSCvt58704	Crash may be seen configuring ptp on Cat9500 series switches
CSCvt60712	Switch crashed after removing route-map
CSCvt64058	Loopback error is not detected on trunk interface
CSCvt72401	MACSEC protected link no longer passes traffic.
CSCvt72427	Cat3k/9k Switch running 16.12.3 is not processing superior BPDUs for non-default native vlan
CSCvt82323	Interface storm-control configuration causes policing of same-type traffic elsewhere on the device.
CSCvt83025	Memory utilization increasing under fman_fp_image due to WRC Stats Req
CSCvt85720	Cat9500 SVL remote portchannel port will link up before Bulk Sync finished
CSCvt99199	MACSEC issue in SDA deployment
CSCvu15007	Crash when invalid input interrupts a role-based access-list policy installation

Resolved Caveats in Cisco IOS XE Gibraltar 16.12.3a

Identifier	Applicable Models	Description
CSCvt41134	All models	Unexpected reload (or boot loop) caused by Smart Agent (SASRcvWQWrk2)
CSCvt72427	All models	Switch running 16.12.3 is not processing superior BPDUs for non-default native vlan
CSCvt17460	Catalyst 9500 High Performance	SVL/DAD links will be err-disabled when there is link-flap due to faulty SFPs

Resolved Caveats in Cisco IOS XE Gibraltar 16.12.3

Identifier	Applicable Models	Description
CSCvm55401	All models	DHCP snooping may drop dhcp option82 packets w/ ip dhcp snooping information option allow-untrusted
CSCvp73666	All models	DNA - LAN Automation doesn't configure link between Peer Device and PnP Agent due CDP limitation
CSCvq72472	All models	Private-vlan mapping XXX configuration under SVI is lost from run config after switch reload
CSCvr23358	All models	Switches are adding Device SGT to proxy generated IGMP leave messages while keeping End host src IP
CSCvr59959	All models	Cat3k/9k Flow-based SPAN(FSPAN) can only work in one direction when mutilple session configured
CSCvr88090	All models	Cat3k/9k crash on running show platform software fed switch 1 fss abstraction
CSCvr90477	All models	Cat3k/Cat9k incorrectly set more-fragment flag for double fragmentation
CSCvr91162	All models	Layer 2 flooding floods IGMP queries causing network outage
CSCvr92638	All models	OSPF External Type-1 Route Present in OSPF Database but not in RIB
CSCvr98281	All models	After valid ip conflict, SVI admin down responds to GARP
CSCvs01943	All models	"login authentication VTY_authen" is missing on "line vty 0 4" only
CSCvs14374	All models	Standby crashes on multiple port flaps
CSCvs14920	All models	Block overrun crash due to Corrupted redzone
CSCvs20038	All models	qos softmax setting doesn't take effect on Catalyst switch in Openflow mode

Identifier	Applicable Models	Description
CSCvs25412	All models	CTS Environmental Data download request triggered before PAC provisioned
CSCvs25428	All models	Netconf incorrectly activate IPv4 address-family for IPv6 BGP peer.
CSCvs36803	All models	When port security applied mac address not learned on hardware
CSCvs42476	All models	Crash during authentication failure of client
CSCvs45231	All models	Memory exhaustion in sessmgrd process due to EAPoL announcement
CSCvs50391	All models	FED crash when premature free of SG element
CSCvs50868	All models	Fed memory leak in 16.9.X related to netflow
CSCvs61571	All models	Cat3k/Cat9k- OBJ_DWNLD_TO_DP_FAILED after exceeding hardware capacity for adjacency table
CSCvs62003	All models	In COPP policy, ARP traffic should be classified under the "system-cpp-police-forus" class
CSCvs68255	All models	Traceback seen when IS-IS crosses LSP boundary and tries to add information in new LSP
CSCvs73580	All models	Memory leak in fed main event qos
CSCvr96863	Catalyst 9500	C9500 breakout interfaces on standby switch of stackwise virtual pair may remain down/down
CSCvs15521	Catalyst 9500	Incorrect interface up/down detection using QSFP-4X10G-LR-S breakout-cable
CSCvq75887	Catalyst 9500 High Performance	intermediate hop with SVI in PIM domain is not forwarding multicast traffic
CSCvr46622	Catalyst 9500 High Performance	Cat9k || scaled mVPN || tracebacks and errors seen in FED trace
CSCvr90442	Catalyst 9500 High Performance	Unknown status shown in "show platform software status control-processor"
CSCvr98368	Catalyst 9500 High Performance	CAT9K intermittently not responding to SNMP
CSCvs38457	Catalyst 9500 High Performance	c9500 stack-wise slot reloaded, newly linked up GLC-GE-100FX cannot passing traffic

Resolved Caveats in Cisco IOS XE Gibraltar 16.12.2

Identifier	Applicable Models	Description
CSCvm89086	All models	span destination interface not dropping ingress traffic
CSCvn04524	All models	IP Source Guard blocks traffic after host IP renewal
CSCvn31653	All models	Missing/incorrect FED entries for IGMP Snooping
CSCvn77683	All models	Switch crashed at mcprp_pak_add_l3_inject_hdr with dhcp snooping
CSCvm89086	All models	span destination interface not dropping ingress traffic
CSCvn04524	All models	IP Source Guard blocks traffic after host IP renewal
CSCvn31653	All models	Missing/incorrect FED entries for IGMP Snooping on
CSCvn77683	All models	Switch crashed at mcprp_pak_add_l3_inject_hdr with dhcp snooping
CSCvn83940	All models	TFTP copy failed with Port Security enabled
CSCvo15594	All models	Hardware MAC address programming issue for remote client
CSCvo17778	All models	Switch not updating checksum after DSCP change
CSCvo24073	All models	multiple CTS sessions stuck in HELD/SAP_NE
CSCvo32446	All models	High CPU Due To Looped Packet and/or Unicast DHCP ACK Dropped
CSCvo33983	All models	Mcast traffic loss seen looks due to missing fed entries during IGMP/MLD snooping.
CSCvo56629	All models	Interface in Admin shutdown showing incoming traffic and interface Status led in green.
CSCvo59504	All models	SVI becomes inaccesible upon reboot
CSCvo71264	All models	Gateway routes DHCP offer incorrectly after DHCP snooping
CSCvo75559	All models	First packet not forwarded when (S,G) needs to be built
CSCvo83305	All models	MAC Access List Blocks Unintended Traffic
CSCvp49518	All models	DHCP SNOOPING DATABASE IS NOT REFRESHED AFTER RELOAD
CSCvp69629	All models	Authentication sessions does not come up on configuring dot1x when there is active client traffic .
CSCvp72220	All models	crash at sisf_show_counters after entering show device-tracking counters command
CSCvm77197	Catalyst 9500	%IOSXE-2-PLATFORM: Switch 1 R0/0: kernel: EXT2-fs (sda1): error:

Identifier	Applicable Models	Description
CSCvn30230	Catalyst 9500	Catalyst 3k/9k: Slow memory leak in linux_iosd-imag
CSCvn78058	Catalyst 9500	C9500:port status LED goes AMBER when stack reload
CSCvo48808	Catalyst 9500	QSFP-40G-SR4 does not breakout in C9500-16X
CSCvq01185	Catalyst 9500	%SNMP-3-RESPONSE_DELAYED: and timeout when polling entSensorValueEntry on 16.9.3
CSCvo61106	Catalyst 9500 High Performance	System report not created for stack_mgr crashes
CSCvp74115	Catalyst 9500 High Performance	A host side PHY link goes down in 1-2 weeks time
CSCvp73588	Catalyst 9500 High Performance	IFS-3-FSDUP: Failed to add stby-bootflash, filesystem prefix exists
CSCvq32597	Catalyst 9500 High Performance	Port LED status not displayed correctly
CSCvq54265	Catalyst 9500 High Performance	Ip bootp server should be disabled by default as a device hardening best practice
CSCvq59740	Catalyst 9500 High Performance	Standby reboots when certain configurations changes are done via WEBUI
CSCvr02957	Catalyst 9500 High Performance	Re-add app-hosting move support - removed in v16.12.1
CSCvr37037	Catalyst 9500 High Performance	SVL:BaseMac addr changes to all Zero and there by causing L2 intf to have same mac on sw1/sw2
CSCvr42801	Catalyst 9500 High Performance	SF-Gryphon/Gryphon-Lite: Hardware initialization is not done for IR3570/IR35215 Volt Sensor
CSCvr45410	Catalyst 9500 High Performance	SVL//channel-misconfig error on port channel interfaces after a failover on the peer device

Identifier	Applicable Models	Description
CSCvr55472	Catalyst 9500 High Performance	Breakout multiple interfaces via SNMP walk
CSCvr70470	All models	sessmgrd crash with "clear dot1x mac" command
CSCvq55940	Catalyst 9500 High Performance	%BIT-4-OUTOFRANGE: bit 4095 is not in the expected range of 1 to 4093

Resolved Caveats in Cisco IOS XE Gibraltar 16.12.1c

Identifier	Applicable Models	Description
CSCvo02294	Catalyst 9500 High Performance	L3 configs are lost when upgraded to 16.11.1 or 16.12.1 from Pre-16.11.1 release

Resolved Caveats in Cisco IOS XE Gibraltar 16.12.1

Identifier	Applicable Models	Description
CSCvm89086	All models	cat 9300 | span destination interface not dropping ingress traffic
CSCvn04524	All models	IP Source Guard blocks traffic after host IP renewal
CSCvn31653	All models	Missing/incorrect FED entries for IGMP Snooping on Cat9300/Cat3850/Cat3650
CSCvn77683	All models	Switch crashed at mcprp_pak_add_l3_inject_hdr with dhcp snooping
CSCvm89086	All models	cat 9300 | span destination interface not dropping ingress traffic
CSCvn04524	All models	IP Source Guard blocks traffic after host IP renewal
CSCvn31653	All models	Missing/incorrect FED entries for IGMP Snooping on Cat9300/Cat3850/Cat3650
CSCvn77683	All models	Switch crashed at mcprp_pak_add_l3_inject_hdr with dhcp snooping
CSCvn83940	All models	Cat9k TFTP copy failed with Port Security enabled
CSCvo15594	All models	Hardware MAC address programming issue for remote client catalyst 9300
CSCvo17778	All models	Cat9k not updating checksum after DSCP change
CSCvo24073	All models	multiple CTS sessions stuck in HELD/SAP_NE

Identifier	Applicable Models	Description
CSCvo32446	All models	High CPU Due To Looped Packet and/or Unicast DHCP ACK Dropped
CSCvo33983	All models	Mcast traffic loss seen looks due to missing fed entries during IGMP/MLD snooping.
CSCvo56629	All models	Cat9500 - Interface in Admin shutdown showing incoming traffic and interface Status led in green.
CSCvo59504	All models	Cat3K | Cat9K - SVI becomes inaccesible upon reboot
CSCvo71264	All models	Cat3k / Cat9k Gateway routes DHCP offer incorrectly after DHCP snooping
CSCvo75559	All models	Cat9300 | First packet not forwarded when (S,G) needs to be built
CSCvo83305	All models	MAC Access List Blocks Unintended Traffic
CSCvp49518	All models	DHCP SNOOPING DATABASE IS NOT REFRESHED AFTER RELOAD
CSCvp69629	All models	Authentication sessions does not come up on configuring dot1x when there is active client traffic .
CSCvp72220	All models	crash at sisf_show_counters after entering show device-tracking counters command
CSCvm77197	Catalyst 9500	C9300/9500 : %IOSXE-2-PLATFORM: Switch 1 R0/0: kernel: EXT2-fs (sda1): error:
CSCvn30230	Catalyst 9500	Catalyst 3k/9k: Slow memory leak in linux_iosd-imag
CSCvn78058	Catalyst 9500	C9500:port status LED goes AMBER when stack reload
CSCvo48808	Catalyst 9500	QSFP-40G-SR4 does not breakout in C9500-16X
CSCvq01185	Catalyst 9500	%SNMP-3-RESPONSE_DELAYED: and timeout when polling entSensorValueEntry on 16.9.3
CSCvo61106	Catalyst 9500 High Performance	System report not created for stack_mgr crashes on Cat 9500
CSCvp74115	Catalyst 9500 High Performance	C9500-48Y4C-A host side PHY link goes down in 1-2 weeks time
CSCvp37771	Catalyst 9500	Mgig - Half-Pair Ethernet Cables do not auto-negotiate to 100 Full with Certain IP Phones
CSCvp62101	Catalyst 9500	~3sec Traffic Loss on Uplink Port Channel After Active SUP removal
CSCvp66193	Catalyst 9500	IOSd Crash within "DHCPD Receive" process

Identifier	Applicable Models	Description
CSCvp70112	Catalyst 9500	EnvMon trap not received after Power Supply and FAN OIR
CSCvp95156	Catalyst 9500	Memory leak in linux_iosd when polling mabClientIndexTest mib.
CSCvq22224	Catalyst 9500	// evpn/vxlan // dhcp relay not working over l3vni
CSCvq29115	Catalyst 9500	Failed to get Board ID shown if stack member boots up
CSCvq30460	Catalyst 9500	SYS-2-BADSHARE: Bad refcount in datagram_done - messages seen during system churn
CSCvq35631	Catalyst 9500	Switch crashed due to HTTP Core
CSCvq40137	Catalyst 9500	Mac address not being learnt when "auth port-control auto" command is present
CSCvq43450	Catalyst 9500	Sup uplinks with netflow configuration stopped forwarding traffic after switchover
CSCvq44397	Catalyst 9500	ospf down upon switchover with aggressive timers "hello-interval 1" and "dead-interval 4"
CSCvq50632	Catalyst 9500	SUP uplinks and/or slot 7 or slot 8 stop passing traffic or fail POST upon SUP failover
CSCvq66802	Catalyst 9500	igmp query with src ip 0.0.0.0 is not ignored
CSCvq89352	Catalyst 9500	missing system_report when crashed - revisit fix of CSCvq26295
CSCvq94738	Catalyst 9500	The COPP configuration back to the default After rebooting the device
CSCvq97365	Catalyst 9500	2 interfaces of client in different vrf connected to same vlan of server not able to get ip via dhcp
CSCvr03905	Catalyst 9500	Memory Leak on FED due to IPv6 Source Guard
CSCvr04551	Catalyst 9500	Multicast stream flickers on igmp join/leave
CSCvr20522	Catalyst 9500	BOOTREPLY dropped when DHCP snooping is enabled
CSCvr29921	Catalyst 9500	Inserting 1Gige SFP (GLC-SX-MMD or SFP GE-T) to SUP port causes another port to link flap.
CSCvr46931	Catalyst 9500	ports remain down/down object-manager (fed-ots-mo thread is stuck)
CSCvr51939	Catalyst 9500	Inactive Interfaces Incorrectly Holding Buffers, causing output drops on switch SUP active ports.
CSCvr71158	Catalyst 9500	Commands returning invalid PRC error message

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 9500 Series Switches is at this URL: https://www.cisco.com/c/en/us/support/switches/catalyst-9500-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://cfnng.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 results you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2019–2021 Cisco Systems, Inc. All rights reserved.