Release Notes for Cisco Catalyst 9400 Series Switches, Cisco IOS XE Gibraltar 16.10.x

First Published: 2018-11-15

Release Notes for Cisco Catalyst 9400 Series Switches, Cisco IOS XE Gibraltar 16.10.x

Introduction

Cisco Catalyst 9400 Series Switches are Cisco's leading modular enterprise switching access platform and have been purpose-built to address emerging trends of Security, IoT, Mobility, and Cloud.

They deliver complete convergence with the rest of the Cisco Catalyst 9000 Series Switches in terms of ASIC architecture with Unified Access Data Plane (UADP) 2.0 and UADP 3.0. The platform runs an Open Cisco IOS XE that supports model driven programmability, has the capacity to host containers, and run 3rd party applications and scripts natively within the switch (by virtue of x86 CPU architecture, local storage, and a higher memory footprint). This series forms the foundational building block for SD-Access, which is Cisco's lead enterprise architecture.

Cisco Catalyst 9400 Series Switches are enterprise optimized with a dual-serviceable fan tray design, side to side airflow, and are closet-friendly with a16-inch depth

Whats New in Cisco IOS XE Gibraltar 16.10.1

Hardware Features in Cisco IOS XE Gibraltar 16.10.1

Feature Name	Description and Documentation Link
Cisco 10GBASE-AOC SFP+ Cable	Supported cable product number—SFP-10G-AOC3M For information about the cable, see the Cisco 10GBASE SFP+ Modules Data Sheet. For information about device compatibility, see the Transceiver Module Group (TMG) Compatibility Matrix.
Cisco 40GBASE QSFP Modules	Supported transceiver module product number—QSFP-40G-CSR-S For information about the cable, see the 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 16.10.1

Feature Name	Description, Documentation Link and License Level Information
Border Gateway Protocol (BGP): • BGP-RT and VPN Distinguisher Attribute Rewrite Wildcard • BGP-VPN Distinguisher Attribute	These BGP features were introduced in this release: • BGP-RT and VPN Distinguisher Attribute Rewrite Wildcard —Introduces the ability to set a range of route target (RT) community attributes or virtual private network (VPN) distinguisher community attributes when mapping them. The VPN Distinguisher Attribute feature allows an administrator to map RTs to a VPN distinguisher that is carried using external Border Gateway Protocol (eBGP) and then mapped to RTs at an ingress Autonomous System Border Router (ASBR). See Routing → Configuring BGP-RT and VPN Distinguisher Attribute Rewrite Wildcard. • BGP-VPN Distinguisher Attribute—Enables a network administrator to keep source route targets (RTs) private from an Autonomous System Border Router (ASBR) in a destination autonomous system. An RT at an egress ASBR is mapped to a VPN distinguisher, the VPN distinguisher is carried through the eBGP, and then it is mapped to an RT at the ingress ASBR. See Routing → Configuring BGP-VPN Distinguisher Attribute. (Network Advantage)
Graceful Insertion and Removal (GIR) Support for BGP	GIR is now supported for the BGP protocol. See High Availability → Configuring Graceful Insertion and Removal . (Network Advantage)
Intermediate System to Intermediate System (IS-IS) Generic Cryptographic Authentication	IS-IS now supports Secure Hash Algorithm (SHA) authentication (SHA-1, SHA-256, SHA-384, and SHA-512), which is more secure than MD5 authentication or clear text authentication. See Routing → Configuring IS-IS Routing. (Network Advantage)
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. (Network Essentials and Network Advantage)

Feature Name	Description, Documentation Link and License Level Information
Media Access Control Security (MACsec): • MACsec connection across intermediate switches • 256-bit AES MACsec (IEEE 802.1AE) host link encryption) with MACsec Key Agreement (MKA) • MKA cipher announcement exchange • MACsec Port Channel Support • MACsec Support for Switch to Switch Connections	These MACsec features were introduced in this release: • MACsec connection across intermediate switches—MACsec connection between end devices in a WAN MACsec deployment with intermediate switches as Catalyst 9000 Series Switches is supported. 128-bit—(Network Essentials and Network Advantage) 256-bit—(Network Advantage) • 256-bit AES MACsec (IEEE 802.1AE) host link encryption) with MACsec Key Agreement (MKA)—Support for 256-bit AES MACsec (IEEE 802.1AE) encryption with MKA on the downlink ports is enabled. 256-bit—(Network Advantage) • MKA cipher announcement exchange—Support for cipher announcement is enabled. Cipher Announcement allows the supplicant and the authenticator to announce their respective MACsec Cipher Suite capabilities through EAPoL announcements. Two types of EAPoL announcements are supported – Secured announcements and unsecured announcements. 128-bit—(Network Essentials and Network Advantage) 256-bit—(Network Advantage) • MACsec Port Channel Support—Support for MACsec over port channels is enabled. 128-bit—(Network Essentials and Network Advantage) 256-bit—(Network Advantage) • MACsec Support for Switch to Switch Connections—Support for switch-to-switch connections on the supervisor ports is enabled. **Note** The feature is supported on C9400-SUP-1 and C9400-SUP-1XL. It is not supported on C9400-SUP-1XL-Y. 128-bit—(Network Essentials and Network Advantage) 256-bit—(Network Advantage) See Security → MACsec Encryption .

Feature Name	Description, Documentation Link and License Level Information
Multiprotocol Label Switching (MPLS): • Ethernet over MPLS (EoMPLS) • Virtual Private LAN Services (VPLS)	The following MPLS features were introduced in this release: • EoMPLS—One of the Any Transport over MPLS (AToM) transport types. EoMPLS provides a tunneling mechanism for Ethernet traffic through an MPLS-enabled Layer 3 core. It encapsulates Ethernet protocol data units (PDUs) inside MPLS packets and uses label stacking to forward them across the MPLS network. • VPLS—A class of VPN that supports the connection of multiple sites in a single bridged domain over a managed IP/MPLS network. VPLS uses the provider core to join multiple attachment circuits together, to simulate a virtual bridge that connects the multiple attachment circuits together. See Multiprotocol Label Switching . (Network Advantage)
Programmability • gNMI Wildcard Support • gNMI Namespace • Model Driven Telemetry - gRPC Dial-Out • YANG Data Models	These programmability features were introduced in the release: • gNMI Wildcard Support—Wildcard in gNMI XPaths are now allowed to be used to match all the elements of a node in the schema. GNMI utilizes wildcards for GET requests (now) and telemetry subscriptions (future) to collect all the data for a specified node. (Network Essentials and Network Advantage) • gNMI Namespace—gNMI protocol supports namesapces. Only valid RFC 7951-compliant prefixes are accepted or presented in either the JSON pointer or in the values of SET Request and GET Request. (Network Essentials and Network Advantage) • Model Driven Telemetry - gRPC Dial-Out—Expands existing Model Driven Telemetry capabilities with the addition of gRPC protocol support and Dial-Out (configured) telemetry subscriptions. (Network Essentials and Network Advantage) • 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/16101. 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 Configuration Guide, Cisco IOS XE Gibraltar 16.10.x.

Feature Name	Description, Documentation Link and License Level Information
Secure Shell File Transfer Protocol (SFTP)	Secure Shell (SSH) now includes support for SSH File Transfer Protocol (SFTP), a new standard file transfer protocol introduced in SSHv2. This feature provides a secure and authenticated method for copying device configuration or device image files. See Security → Configuring SSH File Transfer Protocol. (Network Essentials and Network Advantage)
Security Enhanced (SE) Linux Permissive Mode	Makes it possible for the practical implementation of "principle of least privilege" by enforcing Mandatory Access Control (MAC) on the IOS-XE platform. SELinux provides the capability to define policies to control the access from an application process to any resource object, thereby allowing for the clear definition and confinement of process behavior. In this introductory release for the feature, operation in a permissive mode is available - with the intent of confining specific components (process or application) of the IOS-XE platform. In the permissive mode, access violation events are detected and system logs are generated, but the event or operation itself is not blocked. The solution operates mainly in an access violation detection mode. No user configuration is required for the feature. See Interface and Hardware Commands . (Network Essentials and Network Advantage)

Serviceability	
See → Command Reference, Cisco IOS XE Gibraltar 16.10.x (Catalyst 9400 Switches) .	
debug commands	• The **debug ilpower** command output was enhanced to display the power unit (mW). • The **debug platform condition feature multicast controlplane** command was introduced. It enables radioactive tracing for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) snooping features. • The **debug platform condition mac** command was introduced. It enables radioactive tracing for MAC learning. • The **debug platform rep** command was introduced. It enables debugging of Resilient Ethernet Protocol (REP) functions. • The **debug platform software fed switch active punt packet-capture** command was introduced. It enables debugging of packets during high CPU utilization.

Serviceability	
set platform commands	• The **set platform software nif-mgr switch** command was introduced. It sets the packet cache count per Cisco StackWise Virtual port. • The **set platform software fed switch** command was introduced. It sets the packet cache count per Cisco StackWise Virtual port.

show ip bgp and **show ip bgp neighbor** commands	• **show ip bgp**
	  • The **bestpath-reason** keyword was introduced. This compares the best path with every other path and displays the reason why a path loses out to the best path.
	  • Command output was enhanced to display BGP path installation time stamp. This indicates the time at which the route's path was received from the neighbor.
	  • Command output was also enhanced to display the BGP Peak Prefix Watermark. These are peak watermarks and timestamps for the maximum number of route entries per neighbor.
	• **show ip bgp neighbor**
	  • Command output was enhanced to provide the time of soft inbound and outbound refresh.
	• For both **show ip bgp** and **show ip bgp neighbor** commands, the outputs were also enhanced to display the BGP Peak Prefix Watermark. These are peak watermarks and timestamps for the maximum number of route entries per neighbor.

show logging commands	The **show logging onboard rp uptime** command was introduced. It displays a history of all reset reasons for the supervisor modules in a system.

Serviceability	
show platform commands	• The **show platform hardware fed switch forward interface** command was enhanced to trace packets across a stack and also trace packets captured in a PCAP file. • The **show platform hardware fed switch forward last summary** command was enhanced to display the details about all the copies of the packets and the corresponding outgoing ports. • The **show platform software fed switch** command was introduced. It displays the per port SDP/LMP control packet exchange history between FED and Network Interface Manager (NIF Mgr) software processes. • The **show platform software nif-mgr switch** command was introduced. It displays the control packet exchange history between the Network Interface Manager software process (NIF Mgr) and the StackWise Virtual Link (SVL) interfaces. • The **show platform software fed switch punt cause** command was introduced. It displays information about why the packets received on an interface are punted to the Router Processor (RP). • The **show platform software fed switch punt cpuq** command was introduced. It displays information about punt traffic on CPU queues. • The **show platform software fed switch punt rates interfaces** command was introduced. It displays the overall statistics of punt rate for all the interfaces. • The **show platform software fed punt cpuq rates** command was introduced. It displays the rate at which packets are punted, including the drops in the punted path. • The **show platform software fed switch punt packet-capture display** command was introduced. It displays packet information captured during high CPU utilization. • The **show platform software process memory** command was modified and the virtual size column was deleted from the output. • The **show platform software thread list** and **show platform software process list** commands outputs were modified. The `size` columns in the outputs display the Resident Set Size (RSS) in KB.
show processes commands	The **show processes platform**, **show processes cpu platform**, and **show processes cpu platform history** commands outputs were modified. The `size` columns in the outputs display the Resident Set Size (RSS) in KB.

Serviceability	
show processes memory platform commands	• **show processes memory platform** command was enhanced, the **accounting** keyword was added. • The **show processes memory platform**, **show processes memory platform location**, and **show processes memory platform sorted** commands were modified and the `Total` column was deleted from the output.
show tech-support commands	• The **show tech-support** command was modified to display the history of all reset reasons for all modules or switches in a system. • The **show tech-support acl** command was introduced. It displays access control list (ACL)-related information. • The **show tech-support bgp** command was enhanced to trigger various BGP show commands and log the outputs in the show tech file. • The **show tech-support diagnostic** command was introduced. It displays diagnostic information for technical support. • The **show tech-support platform** command was introduced. It displays detailed information about a platform. • The **show tech-support platform igmp_snooping** command was introduced. It displays Internet Group Management Protocol (IGMP) snooping information about a group. • The **show tech-support poe** command was introduced. It displays outputs of all the PoE-related troubleshooting commands. • The **show tech-support port** command output was updated. • The **show tech-support qos control-plane** command was introduced. It displays QoS-related information for the control-plane. • The **show tech-support qos** command was introduced. It displays the Quality of Service (QoS)-related information. • The **show tech-support stack** command was introduced. It displays all switch stack-related information.

New on the Web UI	
Web UI	• Spanning Tree Protocol (STP) in Layer 2 configuration—Provides path redundancy to build a loop-free topology for Ethernet networks. Security mechanisms like bridge protocol data units (BPDU) Guard and BPDU Filtering provide further protection by ensuring a more stable network. • VLAN Trunk Protocol (VTP)—Reduces administration in a switched network. When you configure a new VLAN on one VTP server, the VLAN is distributed through all switches in the domain. This reduces the need to configure the same VLAN everywhere.

Important Notes

- Cisco StackWise Virtual - Supported and Unsupported Features, on page 9
- Unsupported Features, on page 9
- Complete List of Supported Features, on page 10
- Accessing Hidden Commands, on page 10

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, and High Availability 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, Remote Switched Port Analyzer, and Sofware-Defined Access are NOT supported

Unsupported Features

- Audio Video Bridging (including IEEE802.1AS, IEEE 802.1Qat, and IEEE 802.1Qav)
- Bluetooth
- Cisco TrustSec Network Device Admission Control (NDAC) on Uplinks
- Converged Access for Branch Deployments
- Gateway Load Balancing Protocol (GLBP)
- IPsec VPN
- MACsec Switch to Switch Connections on C9400-SUP-1XL-Y.
- Performance Monitoring (PerfMon)

- Virtual Routing and Forwarding (VRF)-Aware web authentication

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.

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. Such hidden commands are only meant to assist Cisco TAC in advanced troubleshooting and are therefore not documented. For more information about CLI help, see the *Using the Command-Line Interface → Understanding the Help System* chapter of the Comman Reference document.

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.

Supported Hardware

Cisco Catalyst 9400 Series Switches—Model Numbers

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

Switch Model (append with "=" for spares)	Description
C9404R	Cisco Catalyst 9400 Series 4 slot chassis • Redundant supervisor module capability • Two switching module slots • Hot-swappable, front and rear serviceable, non-redundant fan tray assembly • Four power supply module slots
C9407R	Cisco Catalyst 9400 Series 7 slot chassis • Redundant supervisor module capability • Five switching module slots • Hot-swappable, front and rear serviceable fan tray assembly • Eight power supply module slots
C9410R	Cisco Catalyst 9400 Series 10 slot chassis • Redundant supervisor module capability • Eight switching module slots • Hot-swappable, front and rear serviceable fan tray assembly • Eight power supply module slots

Supported Hardware on Cisco Catalyst 9400 Series Switches

Product ID (append with "=" for spares)	Description
Supervisor Modules	
C9400-SUP-1	Cisco Catalyst 9400 Series Supervisor 1 Module This supervisor module is supported on the C9404R, C9407R, and C9410R chassis.

Product ID (append with "=" for spares)	Description
C9400-SUP-1XL	Cisco Catalyst 9400 Series Supervisor 1XL Module This supervisor module is supported on the C9404R, C9407R, and C9410R chassis.
C9400-SUP-1XL-Y	Cisco Catalyst 9400 Series Supervisor 25XL Module This supervisor module is supported on the C9404R, C9407R, and C9410R chassis.
Line Cards	
C9400-LC-24S	24-port, 1 Gigabit Ethernet SFP module that supports 100/1000 BASET-T with Cu-SFP
C9400-LC-24XS	24-port Gigabit Ethernet module that supports 1 and 10 Gbps connectivity.
C9400-LC-48P	48-port, 1 Gigabit Ethernet POE/POE+ module supporting up to 30W per port.
C9400-LC-48S	48-port, 1 Gigabit Ethernet SFP module that supports 100/1000 BASET-T with Cu-SFP.
C9400-LC-48T	48-port, 10/100/1000 BASE-T Gigabit Ethernet module.
C9400-LC-48U	48-port UPOE 10/100/1000 (RJ-45) module supporting up to 60W per port.
C9400-LC-48UX	48-port, UPOE Multigigabit Ethernet Module with: • 24 ports (Ports 1 to 24) 1G UPOE 10/100/1000 (RJ-45) • 24 ports (Ports 25 to 48) MultiGigabit Ethernet 100/1000/2500/5000/10000 UPOE ports
M.2 SATA SSD Modules[1] **(for the Supervisor)**	
C9400-SSD-240GB	Cisco Catalyst 9400 Series 240GB M2 SATA memory
C9400-SSD-480GB	Cisco Catalyst 9400 Series 480GB M2 SATA memory
C9400-SSD-960GB	Cisco Catalyst 9400 Series 960GB M2 SATA memory
AC Power Supply Modules	
C9400-PWR-2100AC	Cisco Catalyst 9400 Series 2100W AC Power Supply
C9400-PWR-3200AC	Cisco Catalyst 9400 Series 3200W AC Power Supply
DC Power Supply Modules	
C9400-PWR-3200DC	Cisco Catalyst 9400 Series 3200W DC Power Supply

[1] M.2 Serial Advanced Technology Attachment (SATA) Solid State Drive (SSD) Module

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 9400 Series Switches, Cisco Identity Services Engine, Cisco Access Control Server, and Cisco Prime Infrastructure.

Catalyst 9400	Cisco Identity Services Engine	Cisco Access Control Server	Cisco Prime Infrastructure
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**.

Catalyst 9400	Cisco Identity Services Engine	Cisco Access Control Server	Cisco Prime Infrastructure
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**.
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**

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[2]	512 MB[3]	256	1280 x 800 or higher	Small

[2] We recommend 1 GHz
[3] 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)

ROMMON and CPLD Versions

The following table provides ROMMON and CPLD version information for the Cisco Catalyst 9400 Series Supervisor Modules. For ROMMON and CPLD version information of Cisco IOS XE 17.x.x releases, refer to the corresponding Cisco IOS XE 17.x.x release notes of the respective platform.

Release	ROMMON Version (C9400-SUP-1, C9400-SUP-1XL, C9400-SUP-1XL-Y)	CPLD Version (C9400-SUP-1, C9400-SUP-1XL, C9400-SUP-1XL-Y)
Gibraltar 16.10.1	16.6.2r	17101705
Fuji 16.9.x	16.6.2r[FC1]	17101705
Fuji 16.8.1a	16.6.2r	17101705
Everest 16.6.x	16.6.2r[FC1]	17101705

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

Release	Image Type	File Name
Cisco IOS XE Gibraltar 16.10.1	CAT9K_IOSXE	cat9k_iosxe.16.10.01.SPA.bin
	Licensed Data Payload Encryption (LDPE)	cat9k_iosxeldpe.16.10.01.SPA

Automatic Boot Loader Upgrade

Note If Cisco Catalyst 9400 Series Supervisor 1 Module power is disconnected and reconnected within a 5-second window, the boot SPI may get corrupted.

Caution

- Do not power cycle your switch during an upgrade.
- Do not disconnect power or remove the supervisor module during an upgrade.
- Do not perform an online insertion and replacement (OIR) of either supervisor (in a High Availability setup), if one of the supervisor modules in the chassis is in the process of a bootloader upgrade or when the switch is booting up.
- Do not perform OIR of a switching module (linecard) when the switch is booting up.

Complex Programmable Logic Device (CPLD) Upgrade

This refers to hardware-programmable firmware. The CPLD upgrade process is part of the automatic boot loader upgrade. The sequence of events is as follows:

Note There are no FPGA or CPLD upgrades in Cisco IOS XE Gibraltar 16.10.1.

1. The system copies `mcnewfpgaclose.hdr` and `mcnewfpgaclose.img` to the bootflash.
2. The supervisor module then automatically reloads to enable the new boot loader.
3. When the new boot loader boots up, the CPLD upgrade process starts automatically. The CPLD upgrade process takes approximately from 7 to 10 minutes. The supervisor will power cycle itself during the CPLD upgrade.

The following is sample output from a CPLD upgrade:

```
Initializing Hardware...
Initializing Hardware...
Initializing Hardware...

System Bootstrap, Version 16.6.2r, RELEASE SOFTWARE (P)
Compiled Thu 10/26/2017 8:30:34.63 by rel

Current image running:
Primary Rommon Image
Last reset cause: SoftwareResetTrig
C9400-SUP-1 platform with 16777216 Kbytes of main memory

Starting System FPGA Upgrade .....
Programming SPI Primary image is completed.
Authenticating SPI Primary image .....
IO FPGA image is authenticated successfully.

Programming Header .....
FPGA HDR file size: 12
Image page count: 1
Verifying programmed header .....
Verifying programmed header .....
Programmed header is verified successfully.

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

Power Cycle is needed to complete System firmware upgrade.
It takes ~7 mins to upgrade firmware after power cycle starts.

DO NOT DISRUPT AFTER POWER CYCLE UNTIL ROMMON PROMPT APPEARS.

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

Power Cycling the Supervisor card now !
Initializing Hardware...
Initializing Hardware...

System Bootstrap, Version 16.6.2r, RELEASE SOFTWARE (P)
Compiled Thu 10/26/2017 8:30:34.63 by rel
Current image running:
Primary Rommon Image
Last reset cause: PowerOn
C9400-SUP-1 platform with 16777216 Kbytes of main memory

rommon 1 >version -v
System Bootstrap, Version 16.6.2r, RELEASE SOFTWARE (P)
Compiled Thu 10/26/2017 8:30:34.63 by rel
```

```
Current image running:
Primary Rommon Image
Last reset cause: PowerOn
C9400-SUP-1 platform with 16777216 Kbytes of main memory
Fpga Version: 0x17101705
System Integrity Status: C334ABCE 6A40 6A48
```

Software Installation Commands

Summary of Software Installation Commands	
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.

Upgrading in Install Mode

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

Before you begin

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

When upgrading from ...	Permitted Supervisor Setup (Applies to the release you are upgrading from)	First upgrade to...	To upgrade to ...
Cisco IOS XE Everest 16.6.1[4]	Upgrade a single supervisor, and complete the boot loader and CPLD upgrade. After completing the first supervisor upgrade, remove and swap in the second supervisor. After both supervisors are upgraded, they can be inserted and booted in a high availability setup. **Note** Do not simultaneously upgrade dual supervisors from Cisco IOS XE Everest 16.6.1 to a later release. Doing so may cause hardware damage.	Cisco IOS XE Everest 16.6.3 Follow the upgrade steps as in the Release Notes for Cisco Catalyst 9400 Series Switches, Cisco IOS XE Everest 16.6.x → Upgrading the Switch Software → Upgrading in Install Mode	Cisco IOS XE Gibraltar 16.10.1
Cisco IOS XE Everest 16.6.2 and later releases	This procedure automatically copies the images to both active and standby supervisor modules. Both supervisor modules are simultaneously upgraded.	Not applicable	

[4] When upgrading from Cisco IOS XE Everest 16.6.1 to a later release, the upgrade may take a long time, and the system will reset three times due to rommon and complex programmable logic device (CPLD) upgrade. Stateful switchover is supported from Cisco IOS XE Everest 16.6.2

Caution

- Do not power cycle your switch during an upgrade.
- Do not disconnect power or remove the supervisor module during an upgrade.
- Do not perform an online insertion and replacement (OIR) of either supervisor (in a High Availability setup), if one of the supervisor modules in the chassis is in the process of a bootloader upgrade or when the switch is booting up.
- Do not perform OIR of a switching module (linecard) when the switch is booting up.

The sample output in this section displays upgrade from Cisco IOS XE Everest 16.6.3 to Cisco IOS XE Gibraltar 16.10.1 using **install** commands.

Procedure

Step 1 Clean Up

a) **install remove inactive**

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

```
Switch# install remove inactive
install_remove: START Wed Oct 31 14:14:40 PDT 2018
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.16.06.03.SPA.pkg
File is in use, will not delete.
cat9k-espbase.16.06.03.SPA.pkg
File is in use, will not delete.
cat9k-rpbase.16.06.03.SPA.pkg
File is in use, will not delete.
cat9k-rpboot.16.06.03.SPA.pkg
File is in use, will not delete.
cat9k-sipbase.16.06.03.SPA.pkg
File is in use, will not delete.
cat9k-sipspa.16.06.03.SPA.pkg
File is in use, will not delete.
cat9k-srdriver.16.06.03.SPA.pkg
File is in use, will not delete.
cat9k-webui.16.06.01.SPA.pkg
File is in use, will not delete.
packages.conf
File is in use, will not delete.
done.

The following files will be deleted:
[R0]:
/flash/cat9k-cc_srdriver.16.06.03.SPA.pkg
/flash/cat9k-espbase.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_1.bin
/flash/cat9k_1.conf
/flash/cat9k_2.1.conf
/flash/cat9k_2.bin
/flash/cat9k_2.conf
/flash/cat9k_iosxe.16.06.03.SPA.bin
/flash/packages.conf.00-

Do you want to remove the above files? [y/n]y
[R0]:
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
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_1.bin ... done.
Deleting file flash:cat9k_1.conf ... done.
Deleting file flash:cat9k_2.1.conf ... done.
Deleting file flash:cat9k_2.bin ... done.
Deleting file flash:cat9k_2.conf ... done.
```

```
Deleting file flash:cat9k_iosxe.16.06.03.SPA.bin ... done.
Deleting file flash:packages.conf.00- ... done.
SUCCESS: Files deleted.
--- Starting Post_Remove_Cleanup ---
Performing Post_Remove_Cleanup on Active/Standby
[R0] Post_Remove_Cleanup package(s) on R0
[R0] Finished Post_Remove_Cleanup on R0
Checking status of Post_Remove_Cleanup on [R0]
Post_Remove_Cleanup: Passed on [R0]
Finished Post_Remove_Cleanup

SUCCESS: install_remove Wed Oct 31 14:16:29 PDT 2018
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.16.10.01.SPA.bin flash:

Destination filename [cat9k_iosxe.16.10.01.SPA.bin]?
Accessing tftp://10.8.0.6//cat9k_iosxe.16.10.01.SPA.bin...
Loading /cat9k_iosxe.16.10.01.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 Oct 31 2018 10:18:11 -07:00 cat9k_iosxe.16.10.01.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 the boot variable is set to **flash:packages.conf**.

The output should display **BOOT variable** = **flash:packages.conf**.

```
Switch# show boot system
```

Step 4 Software install image to flash

a) **install add file activate commit**

Use this command to install the target image to flash. You can point to the source image on your TFTP server or in flash if you have it copied to flash.

```
Switch# install add file flash:cat9k_iosxe.16.10.01.SPA.bin activate commit

install_add_activate_commit: START Wed Oct 31 22:49:41 UTC 2018

*Oct 31 22:49:42.772: %IOSXE-5-PLATFORM: Switch 1 R0/0: Oct 31 22:49:42 install_engine.sh:

 %INSTALL-5-INSTALL_START_INFO: Started install one-shot
flash:cat9k_iosxe.16.10.01.SPA.bin
install_add_activate_commit: Adding PACKAGE

--- Starting initial file syncing ---
Info: Finished copying flash:cat9k_iosxe.16.10.01.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

/flash/cat9k-webui.16.10.01.SPA.pkg
/flash/cat9k-srdriver.16.10.01.SPA.pkg
/flash/cat9k-sipspa.16.10.01.SPA.pkg
/flash/cat9k-sipbase.16.10.01.SPA.pkg
/flash/cat9k-rpboot.16.10.01.SPA.pkg
/flash/cat9k-rpbase.16.10.01.SPA.pkg
/flash/cat9k-guestshell.16.10.01.SPA.pkg
/flash/cat9k-espbase.16.10.01.SPA.pkg
/flash/cat9k-cc_srdriver.16.10.01.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
[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!

Chassis 1 reloading, reason - Reload command
SUCCESS: install_add_activate_commit
```

```
/flash/cat9k-webui.16.10.01.SPA.pkg
/flash/cat9k-srdriver.16.10.01.SPA.pkg
/flash/cat9k-sipspa.16.10.01.SPA.pkg
/flash/cat9k-sipbase.16.10.01.SPA.pkg
/flash/cat9k-rpboot.16.10.01.SPA.pkg
/flash/cat9k-rpbase.16.10.01.SPA.pkg
/flash/cat9k-guestshell.16.10.01.SPA.pkg
/flash/cat9k-espbase.16.10.01.SPA.pkg
/flash/cat9k-cc_srdriver.16.10.01.SPA.pkg
Wed Oct 31 22:53:58 UTC 2018
Switch#
```

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

b) **dir flash:**

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

```
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  Oct 31 2018 11:49:33 -07:00  cat9k-cc_srdriver.16.10.01.SPA.pkg
491525 -rw- 78484428  Oct 31 2018 11:49:35 -07:00  cat9k-espbase.16.10.01.SPA.pkg
491526 -rw- 1598412   Oct 31 2018 11:49:35 -07:00  cat9k-guestshell.16.10.01.SPA.pkg
491527 -rw- 404153288 Oct 31 2018 11:49:47 -07:00  cat9k-rpbase.16.10.01.SPA.pkg
491533 -rw- 31657374  Oct 31 2018 11:50:09 -07:00  cat9k-rpboot.16.10.01.SPA.pkg
491528 -rw- 27681740  Oct 31 2018 11:49:48 -07:00  cat9k-sipbase.16.10.01.SPA.pkg
491529 -rw- 52224968  Oct 31 2018 11:49:49 -07:00  cat9k-sipspa.16.10.01.SPA.pkg
491530 -rw- 31130572  Oct 31 2018 11:49:50 -07:00  cat9k-srdriver.16.10.01.SPA.pkg
491531 -rw- 14783432  Oct 31 2018 11:49:51 -07:00  cat9k-webui.16.10.01.SPA.pkg
491532 -rw- 9160      Oct 31 2018 11:49:51 -07:00  cat9k-wlc.16.10.01.SPA.pkg

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

The following sample output displays the .conf files in the flash partition; note the three .conf files:

- packages.conf—the file that has been re-written with the newly installed .pkg files
- packages.conf.00—backup file of the previously installed image
- cat9k_iosxe.16.010.01.SPA.conf— a copy of packages.conf and not used by the system.

```
Switch# dir flash:*.conf

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

```
434197 -rw- 7406 Oct 31 2018 10:59:16 -07:00 packages.conf
434196 -rw- 7504 Oct 31 2018 10:59:16 -07:00 packages.conf.00-
516098 -rw- 7406 Oct 31 2018 10:58:08 -07:00 cat9k_iosxe.16.10.01.SPA.conf
11353194496 bytes total (8963174400 bytes free)
```

Step 5 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
```

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 16.10.1 image on the device:

```
Switch# show version
Cisco IOS XE Software, Version 16.10.01
Cisco IOS Software [Gibraltar], Catalyst L3 Switch Software (CAT9K_IOSXE), Version
16.10.1, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2018 by Cisco Systems, Inc.
Compiled Fri 09-Nov-18 19:43 by mcpre
```

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 ...	Permitted Supervisor Setup (Applies to the release you are downgrading from)	To ...
Cisco IOS XE Gibraltar 16.10.1	This procedure automatically copies the images to both active and standby supervisor modules. Both supervisor modules are simultaneously downgraded. **Note** Do not perform an Online Removal and Replacement (OIR) of either supervisor module during the process.	Cisco IOS XE Fuji 16.9.x or earlier releases.

The sample output in this section shows downgrade from Cisco IOS XE Gibraltar 16.10.1 to Cisco IOS XE Everest 16.6.2, using **install** commands.



Important New hardware modules (supervisors or line card modules) that are introduced in a release cannot be downgraded. The release in which a module is introduced is the minimum software version for that model. We recommend upgrading all existing hardware to the same release as the latest hardware.

Procedure

Step 1 Clean Up

a) **install remove inactive**

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

```
Switch# install remove inactive
install_remove: START Wed Oct 31 14:14:40 PDT 2018
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.16.10.01.SPA.pkg
File is in use, will not delete.
cat9k-espbase.16.10.01.SPA.pkg
File is in use, will not delete.
cat9k-guestshell.16.10.01.SPA.pkg
File is in use, will not delete.
cat9k-rpbase.16.10.01.SPA.pkg
File is in use, will not delete.
cat9k-rpboot.16.10.01.SPA.pkg
File is in use, will not delete.
cat9k-sipbase.16.10.01.SPA.pkg
File is in use, will not delete.
cat9k-sipspa.16.10.01.SPA.pkg
File is in use, will not delete.
cat9k-srdriver.16.10.01.SPA.pkg
File is in use, will not delete.
```

```
cat9k-webui.16.10.01.SPA.pkg
File is in use, will not delete.
packages.conf
File is in use, will not delete.
done.

The following files will be deleted:
[R0]:
/flash/cat9k-cc_srdriver.16.10.01.SPA.pkg
/flash/cat9k-espbase.16.10.01.SPA.pkg
/flash/cat9k-guestshell.16.10.01.SPA.pkg
/flash/cat9k-rpbase.16.10.01.SPA.pkg
/flash/cat9k-rpboot.16.10.01.SPA.pkg
/flash/cat9k-sipbase.16.10.01.SPA.pkg
/flash/cat9k-sipspa.16.10.01.SPA.pkg
/flash/cat9k-srdriver.16.10.01.SPA.pkg
/flash/cat9k-webui.pkg
/flash/cat9k_1.bin
/flash/cat9k_1.conf
/flash/cat9k_2.1.conf
/flash/cat9k_2.bin
/flash/cat9k_2.conf
/flash/cat9k_iosxe.16.09.01.SSA.bin
/flash/packages.conf.00-

Do you want to remove the above files? [y/n]y
[R0]:
Deleting file flash:cat9k-cc_srdriver.16.10.01.SPA.pkg ... done.
Deleting file flash:cat9k-espbase.16.10.01.SPA.pkg ... done.
Deleting file flash:cat9k-guestshell.16.10.01.SPA.pkg ... done.
Deleting file flash:cat9k-rpbase.16.10.01.SPA.pkg ... done.
Deleting file flash:cat9k-rpboot.16.10.01.SPA.pkg ... done.
Deleting file flash:cat9k-sipbase.16.10.01.SPA.pkg ... done.
Deleting file flash:cat9k-sipspa.16.10.01.SPA.pkg ... done.
Deleting file flash:cat9k-srdriver.16.10.01.SPA.pkg ... done.
Deleting file flash:cat9k-webui.16.10.01.SPA.pkg ... done.
Deleting file flash:cat9k_1.bin ... done.
Deleting file flash:cat9k_1.conf ... done.
Deleting file flash:cat9k_2.1.conf ... done.
Deleting file flash:cat9k_2.bin ... done.
Deleting file flash:cat9k_2.conf ... done.
Deleting file flash:cat9k_iosxe.16.10.01.bin ... done.
Deleting file flash:packages.conf.00- ... done.
SUCCESS: Files deleted.
--- Starting Post_Remove_Cleanup ---
Performing Post_Remove_Cleanup on Active/Standby
[R0] Post_Remove_Cleanup package(s) on R0
[R0] Finished Post_Remove_Cleanup on R0
Checking status of Post_Remove_Cleanup on [R0]
Post_Remove_Cleanup: Passed on [R0]
Finished Post_Remove_Cleanup

SUCCESS: install_remove Wed Oct 31 14:16:29 PDT 2018
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.16.06.02.SPA.bin flash:

Destination filename [cat9k_iosxe.16.06.02.SPA.bin]?
Accessing tftp://10.8.0.6//cat9k_iosxe.16.06.02.SPA.bin...
Loading /cat9k_iosxe.16.06.02.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 Wed Oct 31 2018 13:35:16 -07:00 cat9k_iosxe.16.06.02.SPA.bin
11353194496 bytes total (9055866880 bytes free)
```

Step 3 Downgrade software image

- **install add file activate commit**
- **install rollback to committed**

The following example displays the installation of the `cat9k_iosxe.16.06.02.SPA.bin` software image to flash, to downgrade the switch by using the **install add file activate commit** command. You can point to the source image on your tftp server or in flash if you have it copied to flash.

```
Switch# install add file flash:
Switch# install add file flash:cat9k_iosxe.16.06.02.SPA.bin activate commit

install_add_activate_commit: START Wed Oct 31 22:49:41 UTC 2018

*Oct 31 22:49:42.772: %IOSXE-5-PLATFORM: Switch 1 R0/0: Oct 31 22:49:42 install_engine.sh:
%INSTALL-5-INSTALL_START_INFO: Started install one-shot
flash:cat9k_iosxe.16.06.02.SPA.bininstall_add_activate_commit: Adding PACKAGE

--- Starting initial file syncing ---
Info: Finished copying flash:cat9k_iosxe.16.06.02.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

/flash/cat9k-webui.16.06.02.SPA.pkg
/flash/cat9k-srdriver.16.06.02.SPA.pkg
/flash/cat9k-sipspa.16.06.02.SPA.pkg
/flash/cat9k-sipbase.16.06.02.SPA.pkg
/flash/cat9k-rpboot.16.06.02.SPA.pkg
/flash/cat9k-rpbase.16.06.02.SPA.pkg
/flash/cat9k-espbase.16.06.02.SPA.pkg
/flash/cat9k-cc_srdriver.16.06.02.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
[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!

Chassis 1 reloading, reason - Reload command
SUCCESS: install_add_activate_commit
/flash/cat9k-webui.16.06.02.SPA.pkg
/flash/cat9k-srdriver.16.06.02.SPA.pkg
/flash/cat9k-sipspa.16.06.02.SPA.pkg
/flash/cat9k-sipbase.16.06.02.SPA.pkg
/flash/cat9k-rpboot.16.06.02.SPA.pkg
/flash/cat9k-rpbase.16.06.02.SPA.pkg
/flash/cat9k-guestshell.16.06.02.SPA.pkg
/flash/cat9k-espbase.16.06.02.SPA.pkg
/flash/cat9k-cc_srdriver.16.06.02.SPA.pkg
Fri Mar 16 22:53:58 UTC 2018
Switch#
```

The following example displays sample output when downgrading the switch by using the **install rollback to committed** command.

Important
You use the **install rollback to committed** command for downgrading, only if the version you want to downgrade to, is committed.

```
Switch# install rollback to committed

install_rollback: START Wed Oct 31 14:24:56 UTC 2018

This operation requires a reload of the system. Do you want to proceed? [y/n]
*Oct 31 14:24:57.555: %IOSXE-5-PLATFORM: R0/0: Oct 31 14:24:57 install_engine.sh:
%INSTALL-5-INSTALL_START_INFO: Started install rollbacky
--- Starting Rollback ---
Performing Rollback on Active/Standby

WARNING: Found 55 disjoint TDL objects.
[R0] Rollback package(s) on R0
--- Starting rollback impact ---
Changes that are part of this rollback
Current : rp 0 0 rp_boot cat9k-rpboot.16.10.01.SPA.pkg
Current : rp 1 0 rp_boot cat9k-rpboot.16.10.01.SPA.pkg
Replacement: rp 0 0 rp_boot cat9k-rpboot.16.06.02.SPA.pkg
Replacement: rp 1 0 rp_boot cat9k-rpboot.16.06.02.SPA.pkg
Current : cc 0 0 cc_srdriver cat9k-cc_srdriver.16.10.01.SPA.pkg
Current : cc 0 0 cc cat9k-sipbase.16.10.01.SPA.pkg
Current : cc 0 0 cc_spa cat9k-sipspa.16.10.01.SPA.pkg
Current : cc 1 0 cc_srdriver cat9k-cc_srdriver.16.10.01.SPA.pkg
Current : cc 1 0 cc cat9k-sipbase.16.10.01.SPA.pkg
```

```
Current : cc 1 0 cc_spa cat9k-sipspa.16.10.01.SPA.pkg
Current : cc 10 0 cc cat9k-sipbase.16.10.01.SPA.pkg
Current : cc 10 0 cc_spa cat9k-sipspa.16.10.01.SPA.pkg
Current : cc 10 0 cc_srdriver cat9k-cc_srdriver.16.10.01.SPA.pkg
Current : cc 2 0 cc_srdriver cat9k-cc_srdriver.16.10.01.SPA.pkg
Current : cc 2 0 cc cat9k-sipbase.16.10.01.SPA.pkg
Current : cc 2 0 cc_spa cat9k-sipspa.16.10.01.SPA.pkg
Current : cc 3 0 cc_srdriver cat9k-cc_srdriver.16.10.01.SPA.pkg
Current : cc 3 0 cc cat9k-sipbase.16.10.01.SPA.pkg
Current : cc 3 0 cc_spa cat9k-sipspa.16.10.01.SPA.pkg
Current : cc 4 0 cc_srdriver cat9k-cc_srdriver.16.10.01.SPA.pkg
Current : cc 4 0 cc cat9k-sipbase.16.10.01.SPA.pkg
Current : cc 4 0 cc_spa cat9k-sipspa.16.10.01.SPA.pkg
Current : cc 5 0 cc_srdriver cat9k-cc_srdriver.16.10.01.SPA.pkg
Current : cc 5 0 cc cat9k-sipbase.16.10.01.SPA.pkg
Current : cc 5 0 cc_spa cat9k-sipspa.16.10.01.SPA.pkg
Current : cc 6 0 cc_srdriver cat9k-cc_srdriver.16.10.01.SPA.pkg
Current : cc 6 0 cc cat9k-sipbase.16.10.01.SPA.pkg
Current : cc 6 0 cc_spa cat9k-sipspa.16.10.01.SPA.pkg
Current : cc 7 0 cc_srdriver cat9k-cc_srdriver.16.10.01.SPA.pkg
Current : cc 7 0 cc cat9k-sipbase.16.10.01.SPA.pkg
Current : cc 7 0 cc_spa cat9k-sipspa.16.10.01.SPA.pkg
Current : cc 8 0 cc_srdriver cat9k-cc_srdriver.16.10.01.SPA.pkg
Current : cc 8 0 cc cat9k-sipbase.16.10.01.SPA.pkg
Current : cc 8 0 cc_spa cat9k-sipspa.16.10.01.SPA.pkg
Current : cc 9 0 cc_srdriver cat9k-cc_srdriver.16.10.01.SPA.pkg
Current : cc 9 0 cc cat9k-sipbase.16.10.01.SPA.pkg
Current : cc 9 0 cc_spa cat9k-sipspa.16.10.01.SPA.pkg
Current : fp 0 0 fp cat9k-espbase.16.10.01.SPA.pkg
Current : fp 1 0 fp cat9k-espbase.16.10.01.SPA.pkg
Current : rp 0 0 guestshell cat9k-guestshell.16.10.01.SPA.pkg
Current : rp 0 0 rp_base cat9k-rpbase.16.10.01.SPA.pkg
Current : rp 0 0 rp_daemons cat9k-rpbase.16.10.01.SPA.pkg
Current : rp 0 0 rp_iosd cat9k-rpbase.16.10.01.SPA.pkg
Current : rp 0 0 rp_security cat9k-rpbase.16.10.01.SPA.pkg
Current : rp 0 0 rp_webui cat9k-webui.16.10.01.SPA.pkg
Current : rp 0 0 rp_wlc cat9k-wlc.16.10.01.SPA.pkg
Current : rp 0 0 srdriver cat9k-srdriver.16.10.01.SPA.pkg
Current : rp 1 0 guestshell cat9k-guestshell.16.10.01.SPA.pkg
Current : rp 1 0 rp_base cat9k-rpbase.16.10.01.SPA.pkg
Current : rp 1 0 rp_daemons cat9k-rpbase.16.10.01.SPA.pkg
Current : rp 1 0 rp_iosd cat9k-rpbase.16.10.01.SPA.pkg
Current : rp 1 0 rp_security cat9k-rpbase.16.10.01.SPA.pkg
Current : rp 1 0 rp_webui cat9k-webui.16.10.01.SPA.pkg
Current : rp 1 0 rp_wlc cat9k-wlc.16.10.01.SPA.pkg
Current : rp 1 0 srdriver cat9k-srdriver.16.10.01.SPA.pkg
Replacement: cc 0 0 cc_srdriver cat9k-cc_srdriver.16.06.02.SPA.pkg
Replacement: cc 0 0 cc cat9k-sipbase.16.06.02.SPA.pkg
Replacement: cc 0 0 cc_spa cat9k-sipspa.16.06.02.SPA.pkg
Replacement: cc 1 0 cc_srdriver cat9k-cc_srdriver.16.06.02.SPA.pkg
Replacement: cc 1 0 cc cat9k-sipbase.16.06.02.SPA.pkg
Replacement: cc 1 0 cc_spa cat9k-sipspa.16.06.02.SPA.pkg
Replacement: cc 10 0 cc cat9k-sipbase.16.06.02.SPA.pkg
Replacement: cc 10 0 cc_spa cat9k-sipspa.16.06.02.SPA.pkg
Replacement: cc 10 0 cc_srdriver cat9k-cc_srdriver.16.06.02.SPA.pkg
Replacement: cc 2 0 cc_srdriver cat9k-cc_srdriver.16.06.02.SPA.pkg
Replacement: cc 2 0 cc cat9k-sipbase.16.06.02.SPA.pkg
Replacement: cc 2 0 cc_spa cat9k-sipspa.16.06.02.SPA.pkg
Replacement: cc 3 0 cc_srdriver cat9k-cc_srdriver.16.06.02.SPA.pkg
Replacement: cc 3 0 cc cat9k-sipbase.16.06.02.SPA.pkg
Replacement: cc 3 0 cc_spa cat9k-sipspa.16.06.02.SPA.pkg
Replacement: cc 4 0 cc_srdriver cat9k-cc_srdriver.16.06.02.SPA.pkg
Replacement: cc 4 0 cc cat9k-sipbase.16.06.02.SPA.pkg
Replacement: cc 4 0 cc_spa cat9k-sipspa.16.06.02.SPA.pkg
```

```
Replacement: cc 5 0 cc_srdriver cat9k-cc_srdriver.16.06.02.SPA.pkg
Replacement: cc 5 0 cc cat9k-sipbase.16.06.02.SPA.pkg
Replacement: cc 5 0 cc_spa cat9k-sipspa.16.06.02.SPA.pkg
Replacement: cc 6 0 cc_srdriver cat9k-cc_srdriver.16.06.02.SPA.pkg
Replacement: cc 6 0 cc cat9k-sipbase.16.06.02.SPA.pkg
Replacement: cc 6 0 cc_spa cat9k-sipspa.16.06.02.SPA.pkg
Replacement: cc 7 0 cc_srdriver cat9k-cc_srdriver.16.06.02.SPA.pkg
Replacement: cc 7 0 cc cat9k-sipbase.16.06.02.SPA.pkg
Replacement: cc 7 0 cc_spa cat9k-sipspa.16.06.02.SPA.pkg
Replacement: cc 8 0 cc_srdriver cat9k-cc_srdriver.16.06.02.SPA.pkg
Replacement: cc 8 0 cc cat9k-sipbase.16.06.02.SPA.pkg
Replacement: cc 8 0 cc_spa cat9k-sipspa.16.06.02.SPA.pkg
Replacement: cc 9 0 cc_srdriver cat9k-cc_srdriver.16.06.02.SPA.pkg
Replacement: cc 9 0 cc cat9k-sipbase.16.06.02.SPA.pkg
Replacement: cc 9 0 cc_spa cat9k-sipspa.16.06.02.SPA.pkg
Replacement: fp 0 0 fp cat9k-espbase.16.06.02.SPA.pkg
Replacement: fp 1 0 fp cat9k-espbase.16.06.02.SPA.pkg
Replacement: rp 0 0 guestshell cat9k-guestshell.16.06.02.SPA.pkg
Replacement: rp 0 0 rp_base cat9k-rpbase.16.06.02.SPA.pkg
Replacement: rp 0 0 rp_daemons cat9k-rpbase.16.06.02.SPA.pkg
Replacement: rp 0 0 rp_iosd cat9k-rpbase.16.06.02.SPA.pkg
Replacement: rp 0 0 rp_security cat9k-rpbase.16.06.02.SPA.pkg
Replacement: rp 0 0 rp_webui cat9k-webui.16.06.02.SPA.pkg
Replacement: rp 0 0 srdriver cat9k-srdriver.16.06.02.SPA.pkg
Replacement: rp 1 0 guestshell cat9k-guestshell.16.06.02.SPA.pkg
Replacement: rp 1 0 rp_base cat9k-rpbase.16.06.02.SPA.pkg
Replacement: rp 1 0 rp_daemons cat9k-rpbase.16.06.02.SPA.pkg
Replacement: rp 1 0 rp_iosd cat9k-rpbase.16.06.02.SPA.pkg
Replacement: rp 1 0 rp_security cat9k-rpbase.16.06.02.SPA.pkg
Replacement: rp 1 0 rp_webui cat9k-webui.16.06.02.SPA.pkg
Replacement: rp 1 0 srdriver cat9k-srdriver.16.06.02.SPA.pkg
Finished rollback impact
[R0] Finished Rollback on R0
Checking status of Rollback on [R0]
Rollback: Passed on [R0]
Finished Rollback

Install will reload the system now!
SUCCESS: install_rollback Wed Oct 31 14:26:35 UTC 2018

Switch#
*Mar 16 14:26:35.880: %IOSXE-5-PLATFORM: R0/0: Mar 16 14:26:35 install_engine.sh:
%INSTALL-5-INSTALL_COMPLETED_INFO: Completed install rollback PACKAGE
*Mar 16 14:26:37.740: %IOSXE_OIR-6-REMCARD: Card (rp) removed from slot R1
*Mar 16 14:26:39.253: %IOSXE_OIR-6-INSCARD: Card (rp) inserted in slot R1Nov 2 14:26:5

Initializing Hardware...

System Bootstrap, Version 16.8.1r[FC1], RELEASE SOFTWARE (P)
Compiled Tue 10/31/2017 11:38:44.98 by rel

Current image running:
Primary Rommon Image

Last reset cause: SoftwareResetTrig
C9400-SUP-1 platform with 16777216 Kbytes of main memory

Preparing to autoboot. [Press Ctrl-C to interrupt] 0
attempting to boot from [bootflash:packages.conf]

Located file packages.conf
#
################################################################################################################################
```

```
Warning: ignoring ROMMON var "BOOT_PARAM"
Warning: ignoring ROMMON var "USER_BOOT_PARAM"

Restricted Rights Legend

Use, duplication, or disclosure by the Government is
subject to restrictions as set forth in subparagraph
(c) of the Commercial Computer Software - Restricted
Rights clause at FAR sec. 52.227-19 and subparagraph
(c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.

cisco Systems, Inc.
170 West Tasman Drive
San Jose, California 95134-1706



Cisco IOS Software [Everest], Catalyst L3 Switch Software (CAT9K_IOSXE), Version 16.6.2,
RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2017 by Cisco Systems, Inc.
Compiled Sat 22-Jul-17 05:51 by mcpre



Cisco IOS-XE software, Copyright (c) 2005-2017 by cisco Systems, Inc.
All rights reserved. Certain components of Cisco IOS-XE software are
licensed under the GNU General Public License ("GPL") Version 2.0. The
software code licensed under GPL Version 2.0 is free software that comes
with ABSOLUTELY NO WARRANTY. You can redistribute and/or modify such
GPL code under the terms of GPL Version 2.0. For more details, see the
documentation or "License Notice" file accompanying the IOS-XE software,
or the applicable URL provided on the flyer accompanying the IOS-XE
software.



FIPS: Flash Key Check : Begin
FIPS: Flash Key Check : End, Not Found, FIPS Mode Not Enabled

This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.

cisco C9410R (X86) processor (revision V00) with 868521K/6147K bytes of memory.
Processor board ID FXS2118Q1GM
312 Gigabit Ethernet interfaces
40 Ten Gigabit Ethernet interfaces
4 Forty Gigabit Ethernet interfaces
32768K bytes of non-volatile configuration memory.
```

```
15958516K bytes of physical memory.
11161600K bytes of Bootflash at bootflash:.
1638400K bytes of Crash Files at crashinfo:.
0K bytes of WebUI ODM Files at webui:.

%INIT: waited 0 seconds for NVRAM to be available

Press RETURN to get started!
```

Step 4 Reload

a) **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.

b) **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 16.6.2 image on the device:

```
Switch# show version
Cisco IOS XE Software, Version 16.06.02
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 Tue 10-Jul-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 9400 Series Switches 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 1: Permitted Combinations

	DNA Essentials	DNA Advantage
Network Essentials	Yes	No
Network Advantage	Yes[5]	Yes

[5] 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.

See: 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 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.

See: 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.

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.

  See: 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.

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.

See: Registering the Device in CSSM

Scaling Guidelines

For information about feature scaling guidelines, see these datasheets for Cisco Catalyst 9400 Series Switches:

https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9400-series-switches/nb-06-cat9400-ser-data-sheet-cte-en.html

https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9400-series-switches/nb-06-cat9600-series-line-data-sheet-cte-en.html

https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9400-series-switches/nb-06-cat9400-ser-sup-eng-data-sheet-cte-en.html

Limitations and Restrictions

- Cisco Catalyst 9400 Series 3200W DC Power Supply—The power supply module operates normally as long as DC input voltage is within the full input range (-40 to -75VDC). However, if the input voltage range is beyond the -51 to -57VDC range, Cisco IOS software displays the `Capacity` field as `n.a` (the **show power** command). This issue exists in the Cisco IOS XE Fuji 16.9.1, Cisco IOS XE Fuji 16.9.2, and Cisco IOS XE Gibraltar 16.10.1 releases; it is corrected in all the later releases of Cisco IOS XE Fuji 16.9.x train.
- Cisco StackWise Virtual—A special, additional, C9400-SUP-UPG-LIC= license is required to configure the feature on the Cisco Catalyst 9400 Series Supervisor 1 Module (C9400-SUP-1).
- Cisco TrustSec restrictions—Cisco TrustSec can be configured only on physical interfaces, not on logical interfaces.
- 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.
- 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 switched virtual interfaces (SVIs), port-channel, 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—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.
- 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 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)—ISSU from Cisco IOS XE Fuji 16.9.x to Cisco IOS XE Gibraltar 16.10.x is not supported. This applies to both a single and dual supervisor module setup.
- No service password recovery—With ROMMON versions R16.6.1r and R16.6.2r, the 'no service password-recovery' feature is not available.
- QoS restrictions
  - When configuring QoS queuing policy, the sum of the queuing buffer should not exceed 100%.
  - For QoS policies, only switched virtual interfaces (SVI) are supported for logical interfaces.
  - QoS policies are not supported for port-channel interfaces, tunnel interfaces, and other logical interfaces.
  - Stack Queuing and Scheduling (SQS) drops CPU bound packets exceeding 1.4 Gbps.

- Redundancy—The supervisor module (hardware) supports redundancy. Software redundancy is supported starting with Cisco IOS XE Everest 16.6.2. However, the associated route processor redundancy (RPR) feature is not supported.

  Before performing a switchover, use the **show redundancy**, **show platform**, and **show platform software iomd redundancy** commands to ensure that both the SSOs have formed and that the IOMD process is completed.

  In the following sample output for the **show redundancy**, note that both the SSOs have formed.

```
Switch# show redundancy
Redundant System Information :
------------------------------
Available system uptime = 3 hours, 30 minutes
Switchovers system experienced = 2
Standby failures = 0
Last switchover reason = active unit removed

Hardware Mode = Duplex
Configured Redundancy Mode = sso
Operating Redundancy Mode = sso
Maintenance Mode = Disabled
Communications = Up

Current Processor Information :
-------------------------------
Active Location = slot 3
Current Software state = ACTIVE
Uptime in current state = 2 hours, 57 minutes
Image Version = Cisco IOS Software [Fuji], Catalyst L3 Switch Software (CAT9K_IOSXE),
Version 16.8.1, RELEASE SOFTWARE (fc3)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2018 by Cisco Systems, Inc.
Compiled Tue 27-Mar-18 13:43 by mcpre
BOOT = bootflash:packages.conf;
CONFIG_FILE =
Configuration register = 0x1822

Peer Processor Information :
----------------------------
Standby Location = slot 4
Current Software state = STANDBY HOT
Uptime in current state = 2 hours, 47 minutes
Image Version = Cisco IOS Software [Fuji], Catalyst L3 Switch Software (CAT9K_IOSXE),
Version 16.8.1, RELEASE SOFTWARE (fc3)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2018 by Cisco Systems, Inc.
Compiled Tue 27-Mar-18 13:43 by mcpre
BOOT = bootflash:packages.conf;
CONFIG_FILE =
Configuration register = 0x1822
```

  In the following sample output for the **show platform** command, note that both SSOs have formed and the `HA_STATE` field is `ready`.

```
Switch# show platform
Configured Redundancy Mode = sso
Operating Redundancy Mode = sso
Local RF state = ACTIVE
Peer RF state = STANDBY HOT

slot  PSM STATE   SPA INTF   HA_STATE HA_ACTIVE
   1     ready   started     ready    00:01:16
```

```
   2     ready   started     ready    00:01:22
   3     ready   started     ready    00:01:27 ***active RP
   4     ready   started     ready    00:01:27
<output truncated>
```

In the following sample output for the **show platform software iomd redundancy** command, note that the `State` for all the linecards and supervisor modules is `ok`. This indicates that the IOMD processes are completed.

```
Switch# show platform software iomd redundancy
Chassis type: C9407R

Slot      Type                State                 Insert time (ago)
--------- ------------------- --------------------- -----------------
1         C9400-LC-24XS       ok                    3d09h
2         C9400-LC-48U        ok                    3d09h
R0        C9400-SUP-1         ok, active            3d09h
R1        C9400-SUP-1         ok, standby           3d09h
P1        C9400-PWR-3200AC    ok                    3d08h
P2        C9400-PWR-3200AC    ok                    3d08h
P17       C9407-FAN           ok                    3d08h
<output truncated>
```

- With bootloader version 16.6.2r, you cannot access the M.2 SATA SSD drive at the ROMMON prompt (`rommon>` **dir disk0**). The system displays an error message indicating that the corresponding file system protocol is not found on the device. The only way to access the drive when on bootloader version 16.6.2r, is through the Cisco IOS prompt, after boot up.
- 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.

- Uplink Symmetry—When a redundant supervisor module is inserted, we recommend that you have symmetric uplinks, to minimize packet loss during a switchover.

  Uplinks are said to be in symmetry when the same interface on both supervisor modules have the same type of transceiver module. For example, a TenGigabitEthernet interface with no transceiver installed operates at a default 10G mode; if the matching interface of the other supervisor has a 10G transceiver, then they are in symmetry. Symmetry provides the best SWO packet loss and user experience.

  Asymmetric uplinks have at least one or more pairs of interfaces in one supervisor not matching the transceiver speed of the other supervisor.

- 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.
- YANG data modeling limitation—A maximum of 20 simultaneous NETCONF sessions are supported.
- Secure Password Migration—Type 6 encrypted password is supported from Cisco IOS XE Gibraltar 16.10.1 and later releases. Autoconversion to password type 6 is supported from Cisco IOS XE Gibraltar 16.11.1 and later releases.

  If the startup configuration has a type 6 password and you downgrade to a version in which type 6 password is not supported, you can/may be locked out of the device.
- 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 16.10.x

Caveat ID Number	Description
CSCvh85225	Smart licensing(SL)Actions done soon after system bootup can cause SL to get stuck, requiring reload
CSCvk20217	ISSU / SSO convergence time for EoMPLS is high
CSCvm33622	WCCP redirection to proxy server breaks in certain scenarios.
CSCvm77667	C9400 Standby sup might be in "faulty" state after OIR, if sup port config was chngd L2 > L3 earlier
CSCvm82912	C9400/16.6.4- standby sup port shows green LED even when port is err-disabled due to POST fail
CSCvn00802	Standby member of stackwise-virtual crashes after removing allowed VLAN on trunk interfaces

Caveat ID Number	Description
CSCvn04524	IP Source Guard blocks traffic after host IP renewal

Resolved Caveats in Cisco IOS XE Gibraltar 16.10.1

Caveat ID Number	Description
CSCvh87270	StackWise Virtual not forwarding IGMP traffic over the standby switch.
CSCvj13139	Everest 16.6.2 // FMAN FP Fails to create objects for some prefixes
CSCvj15473	Linux IOSD crash with sh vtp counters cmd
CSCvj73828	Output drops counter mismatch after applied "qos queue-softmax-multiplier 1200"
CSCvk00432	Memory leak in alloc_repexp_entry caused by alloc_ril_index failure
CSCvk32563	Catalyst 9400 cmand memory leak
CSCvk33369	Stack-merge on Stby and CONN_ERR_CONN_TIMEOUT_ERR on Active with multiple SWO
CSCvk33620	in MPLS VPNv6 scenario, egress PE device does not generate ICMPv6 Too Big message
CSCvk33624	SFF8472-3-READ_ERROR message seen for SVL ports
CSCvk59895	COPP: The default and set rate are different for COPP queues
CSCvm09570	SPAN Filter Drops All Traffic
CSCvm09611	C9x00 crashed with multicast memory corruption.
CSCvm33622	WCCP redirection to proxy server breaks in certain scenarios.
CSCvm35904	16.6.3: Access Tunnel Create Interface code is considered to be update request in FMAN_FP
CSCvm36748	FED crash at expired "FED MAC AGING TIMER" or "unknown" timer without a stack trace.
CSCvm47139	Catalyst 3850/9300 Switches not providing PoE+ power for APs
CSCvm48081	WDAVC: FNF doesn't work in some stack scenarios.
CSCvm68064	Cat 9400: MAC address entries not cleared out after aging
CSCvm72517	ECR Installation fails and Pending-Acknowledgement, Pending-Issue counters go up
CSCvm75378	Cat9x000: IPv6 SPAN filter still applied in hardware when removing entire monitor session
CSCvm77162	FED logs overrun 20,000 times with same trace

Caveat ID Number	Description
CSCvm91107	Standby reloads and crashed @fnf_ios_config_dist_validate_sel_process_add

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 9400 Series Switches is at this URL: https://www.cisco.com/c/en/us/support/switches/catalyst-9400-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.

© 2018 Cisco Systems, Inc. All rights reserved.