# Release Notes for Cisco Catalyst 9300 Series Switches, Cisco IOS XE Gibraltar 16.10.x

**First Published:** 2018-11-15

## Release Notes for Cisco Catalyst 9300 Series Switches, Cisco IOS XE Gibraltar 16.10.x

## Introduction

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

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

## 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 SFP+ Modules<br>• Cisco SFP-10G-LR-X module<br>• Cisco SFP-10G-SR-X module | • Supported transceiver module product numbers—SFP-10G-LR-X, SFP-10G-SR-X,<br>• Compatible switch models— All models of the Cisco Catalyst 9300 Series Switches<br>• Compatible network modules—C9300-NM-8X<br>For information about the module, 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<br>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. |

| Feature Name | Description and Documentation Link |
|---|---|
| Support for Breakout Cables<br>• QSFP-4X10G-AC7M<br>• QSFP-4X10G-AC10M | • QSFP-4X10G-AC7M—Cisco 40GBASE-CR4 QSFP to 4 10GBASE-CU SFP+ direct-attach breakout cable.<br>• QSFP-4X10G-AC10M—Cisco 40GBASE-CR4 QSFP to 4 10GBASE-CU SFP+ direct-attach breakout cable.<br><br>For information about these breakout cables, see Cisco 40GBASE QSFP Modules Data Sheet. For information about device compatibility, see the Transceiver Module Group (TMG) Compatibility Matrix.<br>For related software configuration information, see Interface and Hardware Components → Configuring Interface Characteristics. |

## Software Features in Cisco IOS XE Gibraltar 16.10.1

| Feature Name | Description, Documentation Link and License Level Information |
|---|---|
| Border Gateway Protocol (BGP):<br>• BGP-RT and VPN Distinguisher Attribute Rewrite Wildcard<br>• BGP-VPN Distinguisher Attribute | These BGP features were introduced in this release:<br>• 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).<br>See Routing → Configuring BGP-RT and VPN Distinguisher Attribute Rewrite Wildcard.<br>• 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.<br>See Routing → Configuring BGP-VPN Distinguisher Attribute.<br>(Network Advantage) |
| Graceful Insertion and Removal (GIR) Support for BGP | GIR is now supported for the BGP protocol.<br>See Stack Manager and High Availability → Configuring Graceful Insertion and Removal<br>(Network Advantage) |

| Feature Name | Description, Documentation Link and License Level Information |
|---|---|
| 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.<br>See Routing → Configuring IS-IS Routing.<br>(Network Advantage) |
| Media Access Control Security (MACsec): MACsec connection across intermediate switches | MACsec connections between end devices in a WAN MACsec deployment with intermediate switches as Catalyst 9000 Series Switches is supported.<br>See Security → MACsec Encryption.<br>128-bit—(Network Essentials and Network Advantage)<br>256-bit—(Network Advantage) |
| Network Address Translation (NAT) | Enables private IP networks that uses unregistered IP address to connect to the internet. NAT operates on a device, usually connecting two networks together, and translates the private addresses in the internal network into global routable addresses, before packets are forwarded onto another network. NAT is supported on a stack set-up.<br>See IP → Configuring Network Address Translation .<br>(Network Advantage) |
| Password Authentication on USB 3.0 SSD | Enables you to configure security on a USB 3.0 SSD in order to protect the drive from unauthorized access and associated risks.<br>See Interface and Hardware Components → Configuring USB 3.0 SSD.<br>(Network Essentials and Network Advantage) |

| Feature Name | Description, Documentation Link and License Level Information |
|---|---|
| Programmability<br>• gNMI Wildcard Support<br>• gNMI Namespace<br>• Model Driven Telemetry - gRPC Dial-Out<br>• YANG Data Models | These programmability features were introduced in the release:<br>• 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.<br>(Network Essentials and Network Advantage)<br>• 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.<br>(Network Essentials and Network Advantage)<br>• 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.<br>(Network Essentials and Network Advantage)<br>• 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.<br>See → Programmability Configuration Guide, Cisco IOS XE Gibraltar 16.10.x. |
| 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.<br>See Security → Configuring SSH File Transfer Protocol.<br>(Network Essentials and Network Advantage) |

| Feature Name | Description, Documentation Link and License Level Information |
|---|---|
| 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.<br><br>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.<br><br>No user configuration is required for the feature.<br><br>See Interface and Hardware Commands .<br><br>(Network Essentials and Network Advantage) |

| Serviceability | |
|---|---|
| See → Command Reference, Cisco IOS XE Gibraltar 16.10.x (Catalyst 9300 Switches) . | |
| **debug** commands | • The **debug ilpower** command output was enhanced to display the power unit (mW).<br><br>• 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.<br><br>• The **debug platform condition mac** command was introduced. It enables radioactive tracing for MAC learning.<br><br>• The **debug platform rep** command was introduced. It enables debugging of Resilient Ethernet Protocol (REP) functions.<br><br>• The **debug platform software fed switch active punt packet-capture** command was introduced. It enables debugging of packets during high CPU utilization. |

| **Serviceability** | |
|---|---|
| **show ip bgp** and **show ip bgp neighbor** commands | • **show ip bgp**<br>  • 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.<br>  • 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.<br>  • 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.<br>• **show ip bgp neighbor**<br>  • Command output was enhanced to provide the time of soft inbound and outbound refresh.<br>• 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 switch uptime** command ws introduced. It displays a history of all reset reasons for all modules or switches 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.<br>• 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.<br>• 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.<br>• 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.<br>• 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).<br>• The **show platform software fed switch punt cpuq** command was introduced. It displays information about punt traffic on CPU queues.<br>• The **show platform software fed switch punt rates interfaces** command was introduced. It displays the overall statistics of punt rate for all the interfaces.<br>• 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.<br>• The **show platform software fed switch punt packet-capture display** command was introduced. It displays packet information captured during high CPU utilization.<br>• The **show platform integrity** command output was enhanced to display version information for individual packages in the software bundle.<br>• The **show platform software process memory** command was modified and the virtual size column was deleted from the output.<br>• 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. |

| **Serviceability** | |
|---|---|
| **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. |
| **show processes memory platform** commands | • **show processes memory platform** command was enhanced, the **accounting** keyword was added.<br>• 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 romvar** command | The **show romvar** command was introduced. It displays all the ROMMON environment variables. |
| **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.<br>• The **show tech-support acl** command was introduced. It displays access control list (ACL)-related information.<br>• The **show tech-support bgp** command was enhanced to trigger various BGP show commands and log the outputs in the show tech file.<br>• The **show tech-support diagnostic** command was introduced. It displays diagnostic information for technical support.<br>• The **show tech-support platform** command was introduced. It displays detailed information about a platform.<br>• The **show tech-support platform igmp_snooping** command was introduced. It displays Internet Group Management Protocol (IGMP) snooping information about a group.<br>• The **show tech-support poe** command was introduced. It displays outputs of all the PoE-related troubleshooting commands.<br>• The **show tech-support port** command output was updated.<br>• The **show tech-support qos control-plane** command was introduced. It displays QoS-related information for the control-plane.<br>• The **show tech-support qos** command was introduced. It displays the Quality of Service (QoS)-related information.<br>• The **show tech-support stack** command was introduced. It displays all switch stack-related information. |

| Serviceability | |
|---|---|
| **show version** command | Command output was enhanced to display the latest reload reason for all the members switches and the standby switch in the stack as well. The output now displays reload reasons for the active, standby, and member switches in a stack. |

| 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.<br>• 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


- Unsupported Features, on page 9
- Complete List of Supported Features, on page 9
- Accessing Hidden Commands, on page 10


### Unsupported Features

- Bluetooth
- Cisco TrustSec Network Device Admission Control (NDAC) on Uplinks
- Converged Access for Branch Deployments
- Gateway Load Balancing Protocol (GLBP)
- IPsec VPN
- 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 9300 Series Switches—Model Numbers

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

*Table 1: Cisco Catalyst 9300 Series Switches*

| Switch Model | Default License Level | Description |
|---|---|---|
| C9300-24P-A | Network Advantage | Stackable 24 10/100/1000 PoE+ ports; PoE budget of 437W; 715 WAC power supply; supports StackWise-480 and StackPower |
| C9300-24P-E | Network Essentials | |
| C9300-24T-A | Network Advantage | Stackable 24 10/100/1000 Ethernet ports; 350 WAC power supply; supports StackWise-480 and StackPower |
| C9300-24T-E | Network Essentials | |
| C9300-24U-A | Network Advantage | Stackable 24 10/100/1000 UPoE ports; PoE budget of 830W; 1100 WAC power supply; supports StackWise-480 and StackPower |
| C9300-24U-E | Network Essentials | |
| C9300-24UX-A | Network Advantage | Stackable 24 Multigigabit Ethernet 100/1000/2500/5000/10000 UPoE ports; PoE budget of 490 W with 1100 WAC power supply; supports StackWise-480 and StackPower |
| C9300-24UX-E | Network Essentials | |
| C9300-48T-A | Network Advantage | Stackable 48 10/100/1000 Ethernet ports; 350 WAC power supply; supports StackWise-480 and StackPower |
| C9300-48T-E | Network Essentials | |
| C9300-48P-A | Network Advantage | Stackable 48 10/100/1000 PoE+ ports; PoE budget of 437W; 715 WAC power supply; supports StackWise-480 and StackPower |
| C9300-48P-E | Network Essentials | |
| C9300-48T-A | Network Advantage | Stackable 48 10/100/1000 Ethernet ports; 350 WAC power supply; supports StackWise-480 and StackPower |
| C9300-48T-E | Network Essentials | |
| C9300-48U-A | Network Advantage | Stackable 48 10/100/1000 UPoE ports; PoE budget of 822 W; 1100 WAC power supply; supports StackWise-480 and StackPower |
| C9300-48U-E | Network Essentials | |

| Switch Model | Default License Level | Description |
|---|---|---|
| C9300-48UN-A | Network Advantage | Stackable 48 Multigigabit Ethernet (100 Mbps or 1/2.5/5 Gbps) UPoE ports; PoE budget of 610 W with 1100 WAC power supply; supports StackWise-480 and StackPower |
| C9300-48UN-E | Network Essentials | |
| C9300-48UXM-A | Network Advantage | Stackable 48 (36 2.5G Multigigabit Ethernet and 12 10G Multigigabit Ethernet Universal Power Over Ethernet (UPOE) ports) |
| C9300-48UXM-E | Network Essentials | |

## Network Modules

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

| Network Module | Description |
|---|---|
| C3850-NM-4-1G [1] | Four 1 Gigabit Ethernet SFP module slots |
| C3850-NM-2-10G [1] | Two 10 Gigabit Ethernet SFP module slots |
| C3850-NM-4-10G [1] | Four 10 Gigabit Ethernet SFP module slots |
| C3850-NM-8-10G [1] | Eight 10 Gigabit Ethernet SFP module slots |
| C3850-NM-2-40G [1] | Two 40 Gigabit Ethernet SFP module slots |
| C9300-NM-4G [2] | Four 1 Gigabit Ethernet SFP module slots |
| C9300-NM-4M [2] | Four MultiGigabit Ethernet slots |
| C9300-NM-8X [2] | Eight 10 Gigabit Ethernet SFP+ module slots |
| C9300-NM-2Q [2] | Two 40 Gigabit Ethernet QSFP+ module slots |
| C9300-NM-2Y [2] | Two 25 Gigabit Ethernet SFP28 module slots |

**Note**

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

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

***Table 2: Network Modules Supported on Catalyst 9300X-HXN Series Switches***

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

## 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 9300 Series Switches, Cisco Identity Services Engine, Cisco Access Control Server, and Cisco Prime Infrastructure.

| Catalyst 9300 | Cisco Identity Services Engine | Cisco Access Control Server | Cisco Prime Infrastructure |
|---|---|---|---|
| Gibraltar 16.10.1 | 2.3 Patch 1<br>2.4 Patch 1 | 5.4<br>5.5 | PI 3.4 + PI 3.4 latest maintenance release + PI 3.4 latest device pack<br>See Cisco Prime Infrastructure 3.4→ **Downloads**. |

| Catalyst 9300 | Cisco Identity Services Engine | Cisco Access Control Server | Cisco Prime Infrastructure |
|---|---|---|---|
| Fuji 16.9.8 | 2.5<br>2.1 | 5.4<br>5.5 | PI 3.9 + PI 3.9 latest maintenance release + PI 3.9 latest device pack<br>See Cisco Prime Infrastructure 3.9 → **Downloads**. |
| Fuji 16.9.7 | 2.5<br>2.1 | 5.4<br>5.5 | PI 3.9 + PI 3.9 latest maintenance release + PI 3.9 latest device pack<br>See Cisco Prime Infrastructure 3.9 → **Downloads**. |
| Fuji 16.9.6 | 2.3 Patch 1<br>2.4 Patch 1 | 5.4<br>5.5 | PI 3.4 + PI 3.4 latest maintenance release + PI 3.4 latest device pack<br>See Cisco Prime Infrastructure 3.4→ **Downloads**. |
| Fuji 16.9.5 | 2.3 Patch 1<br>2.4 Patch 1 | 5.4<br>5.5 | PI 3.4 + PI 3.4 latest maintenance release + PI 3.4 latest device pack<br>See Cisco Prime Infrastructure 3.4→ **Downloads**. |
| Fuji 16.9.4 | 2.3 Patch 1<br>2.4 Patch 1 | 5.4<br>5.5 | PI 3.4 + PI 3.4 latest maintenance release + PI 3.4 latest device pack<br>See Cisco Prime Infrastructure 3.4→ **Downloads**. |
| Fuji 16.9.3 | 2.3 Patch 1<br>2.4 Patch 1 | 5.4<br>5.5 | PI 3.4 + PI 3.4 latest maintenance release + PI 3.4 latest device pack<br>See Cisco Prime Infrastructure 3.4→ **Downloads**. |
| Fuji 16.9.2 | 2.3 Patch 1<br>2.4 Patch 1 | 5.4<br>5.5 | PI 3.4 + PI 3.4 latest maintenance release + PI 3.4 latest device pack<br>See Cisco Prime Infrastructure 3.4→ **Downloads**. |
| Fuji 16.9.1 | 2.3 Patch 1<br>2.4 Patch 1 | 5.4<br>5.5 | PI 3.4 + PI 3.4 latest device pack<br>See Cisco Prime Infrastructure 3.4→ **Downloads**. |
| Fuji 16.8.1a | 2.3 Patch 1<br>2.4 | 5.4<br>5.5 | PI 3.3 + PI 3.3 latest maintenance release + PI 3.3 latest device pack<br>See Cisco Prime Infrastructure 3.3→ **Downloads**. |

| Catalyst 9300 | Cisco Identity Services Engine | Cisco Access Control Server | Cisco Prime Infrastructure |
|---|---|---|---|
| Everest 16.6.4a | 2.2<br>2.3 | 5.4<br>5.5 | PI 3.1.6 + Device Pack 13<br>See Cisco Prime Infrastructure 3.1 → **Downloads**. |
| Everest 16.6.4 | 2.2<br>2.3 | 5.4<br>5.5 | PI 3.1.6 + Device Pack 13<br>See Cisco Prime Infrastructure 3.1 → **Downloads**. |
| Everest 16.6.3 | 2.2<br>2.3 | 5.4<br>5.5 | PI 3.1.6 + Device Pack 13<br>See Cisco Prime Infrastructure 3.1 → **Downloads** |
| Everest 16.6.2 | 2.2<br>2.3 | 5.4<br>5.5 | PI 3.1.6 + Device Pack 13<br>See Cisco Prime Infrastructure 3.1 → **Downloads** |
| Everest 16.6.1 | 2.2 | 5.4<br>5.5 | PI 3.1.6 + Device Pack 13<br>See Cisco Prime Infrastructure 3.1 → **Downloads** |
| Everest 16.5.1a | 2.1 Patch 3 | 5.4<br>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

| 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

When you upgrade from the existing release on your switch to a later or newer release for the first time, the boot loader may be automatically upgraded, based on the hardware version of the switch. If the boot loader is automatically upgraded, it will take effect on the next reload. If you go back to the older release after this, the boot loader is not downgraded. The updated boot loader supports all previous releases.

For subsequent Cisco IOS XE Everest 16.x.x, or Cisco IOS XE Fuji 16.x.x releases, if there is a new bootloader 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.



**Caution** Do not power cycle your switch during the upgrade.

| Scenario | Automatic Boot Loader Response |
|---|---|
| If you boot Cisco IOS XE Gibraltar 16.10.1 first time | The boot loader may be upgraded to version 16.10.1r[FC1]. For example:<br>`ROM: IOS-XE ROMMON`<br>`BOOTLDR: System Bootstrap, Version 16.10.1r[FC1], RELEASE SOFTWARE (P)`<br>If the automatic boot loader upgrade occurs, while booting, you will see the following on the console:<br>`!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!`<br>`%IOSXEBOOT-4-BOOTLOADER_UPGRADE: (rp/0): ### Thu Jul 5 18:03:28 Universal 2018 PLEASE DO NOT POWER CYCLE`<br>`### BOOT LOADER UPGRADING`<br>`waiting for upgrades to complete...` |

## Automatic Microcode Upgrade

During a Cisco IOS image upgrade or downgrade on a PoE or UPoE switch, the microcode is updated to reflect applicable feature enhancements and bug fixes. Do not restart the switch during the upgrade or downgrade process.

It takes approximately an additional 4 minutes to complete the microcode upgrade in addition to the normal reload time; however, data traffic continues to be forwarded during the upgrade. The microcode update occurs only during an image upgrade or downgrade on PoE or UPoE switches. It does not occur during switch reloads or on non-PoE switches.

The following console messages are displayed during microcode upgrade.

```
MM [1] MCU version 111 sw ver 105
MM [2] MCU version 111 sw ver 105

Front-end Microcode IMG MGR: found 4 microcode images for 1 device.
Image for front-end 0: /tmp/microcode_update/front_end/fe_type_6_0 mismatch: 0
Image for front-end 0: /tmp/microcode_update/front_end/fe_type_6_1 mismatch: 1
Image for front-end 0: /tmp/microcode_update/front_end/fe_type_6_2 mismatch: 1
Image for front-end 0: /tmp/microcode_update/front_end/fe_type_6_3 mismatch: 0

Front-end Microcode IMG MGR: Preparing to program device microcode...
Front-end Microcode IMG MGR: Preparing to program device[0], index=0 ...594412 bytes....
Skipped[0].
Front-end Microcode IMG MGR: Preparing to program device[0], index=1 ...393734 bytes.
Front-end Microcode IMG MGR: Programming device 0...rwRrrrrrrw..
0%.....................................................................
10%.....................................................................
20%.....................................................................
30%.....................................................................
```

```
40%.....................................................................
50%.....................................................................
60%.....................................................................
70%.....................................................................
80%.....................................................................
90%.....................................................................100%
Front-end Microcode IMG MGR: Preparing to program device[0], index=2 ...25186 bytes.
Front-end Microcode IMG MGR: Programming device
0...rrrrrrw..0%....10%....20%......30%...40%......50%....60%......70%...80%......90%....100%wRr!
Front-end Microcode IMG MGR: Microcode programming complete for device 0.
Front-end Microcode IMG MGR: Preparing to program device[0], index=3 ...86370 bytes....
Skipped[3].
Front-end Microcode IMG MGR: Microcode programming complete in 290 seconds
```

## Software Installation Commands

| **Summary of Software Installation Commands**<br>**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:<br>**install add file** *filename* [**activate commit**]<br>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** | |
|---|---|
| Device# **request platform software package ?** | |
| **clean** | Cleans unnecessary package files from media |
| **copy** | Copies package to media |
| **describe** | Describes package content |

| Summary of request platform software Commands | |
|---|---|
| **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 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 ... | 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 16.10.1 |
| Cisco IOS XE Everest 16.6.2 and later | Either **install** commands or **request platform software** commands | |

The sample output in this section displays upgrade from

- Cisco IOS XE Everest 16.5.1a to Cisco IOS XE Gibraltar 16.10.1 using **request platform software** commands.
- Cisco IOS XE Everest 16.6.3 to Cisco IOS XE Gibraltar 16.10.1 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 16.10.1. Use the **switch all** option to clean up all the switches in your stack

**Note**
Ignore the hexdump: messages in the CLI when you enter the command; they have no functional impact and will be removed in a later release. You will see this only on member switches and not on the active or standby. In the sample output below, hexdump messages are seen on switch 3, which is a member switch.

```
Switch# request platform software package clean switch all
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.
done.

Running command on switch 2
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.

Running command on switch 3
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 ...
hexdump: NVRAM: No such file or directory
hexdump: all input file arguments failed
head: cannot open 'NVRAM' for reading: No such file or directory
NVRAM: No such file or directory
hexdump: NVRAM: No such file or directory
hexdump: stdin: Bad file descriptor
tail: cannot open 'NVRAM' for reading: No such file or directory
hexdump: NVRAM: No such file or directory
hexdump: all input file arguments failed
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.SPA.pkg
/flash/cat9k-espbase.SPA.pkg
/flash/cat9k-guestshell.SPA.pkg
/flash/cat9k-rpbase.SPA.pkg
/flash/cat9k-rpboot.SPA.pkg
/flash/cat9k-sipbase.SPA.pkg
/flash/cat9k-sipspa.SPA.pkg
/flash/cat9k-srdriver.SPA.pkg
/flash/cat9k-webui.SPA.pkg
/flash/cat9k_iosxe.16.05.01a.SPA.conf
/flash/packages.conf.00-
[2]:
/flash/cat9k-cc_srdriver.SPA.pkg
/flash/cat9k-espbase.SPA.pkg
/flash/cat9k-guestshell.SPA.pkg
/flash/cat9k-rpbase.SPA.pkg
/flash/cat9k-rpboot.SPA.pkg
/flash/cat9k-sipbase.SPA.pkg
/flash/cat9k-sipspa.SPA.pkg
/flash/cat9k-srdriver.SPA.pkg
/flash/cat9k-webui.SPA.pkg
/flash/cat9k_iosxe.16.05.01a.SPA.conf
/flash/packages.conf.00-
[3]:
/flash/cat9k-cc_srdriver.SPA.pkg
```

```
/flash/cat9k-espbase.SPA.pkg
/flash/cat9k-guestshell.SPA.pkg
/flash/cat9k-rpbase.SPA.pkg
/flash/cat9k-rpboot.SPA.pkg
/flash/cat9k-sipbase.SPA.pkg
/flash/cat9k-sipspa.SPA.pkg
/flash/cat9k-srdriver.SPA.pkg
/flash/cat9k-webui.SPA.pkg
/flash/cat9k_iosxe.16.05.01a.SPA.conf
/flash/packages.conf.00-

Do you want to proceed? [y/n]y
[1]:
Deleting file flash:cat9k-cc_srdriver.SPA.pkg ... done.
Deleting file flash:cat9k-espbase.SPA.pkg ... done.
Deleting file flash:cat9k-guestshell.SPA.pkg ... done.
Deleting file flash:cat9k-rpbase.SPA.pkg ... done.
Deleting file flash:cat9k-rpboot.SPA.pkg ... done.
Deleting file flash:cat9k-sipbase.SPA.pkg ... done.
Deleting file flash:cat9k-sipspa.SPA.pkg ... done.
Deleting file flash:cat9k-srdriver.SPA.pkg ... done.
Deleting file flash:cat9k-webui.SPA.pkg ... done.
Deleting file flash:cat9k_iosxe.16.05.01a.SPA.conf ... done.
Deleting file flash:packages.conf.00- ... done.
SUCCESS: Files deleted.
[2]:
Deleting file flash:cat9k-cc_srdriver.SPA.pkg ... done.
Deleting file flash:cat9k-espbase.SPA.pkg ... done.
Deleting file flash:cat9k-guestshell.SPA.pkg ... done.
Deleting file flash:cat9k-rpbase.SPA.pkg ... done.
Deleting file flash:cat9k-rpboot.SPA.pkg ... done.
Deleting file flash:cat9k-sipbase.SPA.pkg ... done.
Deleting file flash:cat9k-sipspa.SPA.pkg ... done.
Deleting file flash:cat9k-srdriver.SPA.pkg ... done.
Deleting file flash:cat9k-webui.SPA.pkg ... done.
Deleting file flash:cat9k_iosxe.16.05.01a.SPA.conf ... done.
Deleting file flash:packages.conf.00- ... done.
SUCCESS: Files deleted.
[3]:
Deleting file flash:cat9k-cc_srdriver.SPA.pkg ... done.
Deleting file flash:cat9k-espbase.SPA.pkg ... done.
Deleting file flash:cat9k-guestshell.SPA.pkg ... done.
Deleting file flash:cat9k-rpbase.SPA.pkg ... done.
Deleting file flash:cat9k-rpboot.SPA.pkg ... done.
Deleting file flash:cat9k-sipbase.SPA.pkg ... done.
Deleting file flash:cat9k-sipspa.SPA.pkg ... done.
Deleting file flash:cat9k-srdriver.SPA.pkg ... done.
Deleting file flash:cat9k-webui.SPA.pkg ... done.
Deleting file flash:cat9k_iosxe.16.05.01a.SPA.conf ... done.
Deleting file flash:packages.conf.00- ... done.
SUCCESS: Files deleted
```

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 16.10.1:

```
Switch# install remove inactive
install_remove: START Wed Oct 31 19:51:48 UTC 2018
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 Wed Oct 31 19:52:25 UTC 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

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

You can point to the source image on your TFTP server or in flash if you have it copied to flash. We recommend copying the image to a TFTP server or the flash drive of the active switch. If you point to an image on the flash or USB drive of a member switch (instead of the active), you must specify the exact flash or USB drive - otherwise installation fails. For example, if the image is on the flash drive of member switch 3 (flash-3):

`Switch# request platform software package install switch all file flash-3:cat9k_iosxe.16.10.01.SPA.bin auto-copy`.

The following sample output displays installation of the Cisco IOS XE Gibraltar 16.10.1 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 16.10.1.

```
Switch# request platform software package install switch all file
flash:cat9k_iosxe.16.10.01.SPA.bin auto-copy

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

Expanding image file: flash:cat9k_iosxe.16.10.01.SPA.bin
[1]: Copying flash:cat9k_iosxe.16.10.01.SPA.bin from switch 1 to switch 2 3
[2 3]: Finished copying to switch 2 3
[1 2 3]: Expanding file
[1 2 3]: Finished expanding all-in-one software package in switch 1 2 3
SUCCESS: Finished expanding all-in-one software package.
[1 2 3]: 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.16.10.01.SPA.pkg
Added cat9k-espbase.16.10.01.SPA.pkg
Added cat9k-guestshell.16.10.01.SPA.pkg
Added cat9k-rpbase.16.10.01.SPA.pkg
Added cat9k-rpboot.16.10.01.SPA.pkg
Added cat9k-sipbase.16.10.01.SPA.pkg
Added cat9k-sipspa.16.10.01.SPA.pkg
Added cat9k-srdriver.16.10.01.SPA.pkg
Added cat9k-webui.16.10.01.SPA.pkg
Added cat9k-wlc.16.10.01.SPA.pkg
Finished list of software package changes
SUCCESS: Software provisioned. New software will load on reboot.
[1]: Finished install successful on switch 1
[2]: install package(s) on switch 2
--- 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.16.10.01.SPA.pkg
Added cat9k-espbase.16.10.01.SPA.pkg
Added cat9k-guestshell.16.10.01.SPA.pkg
Added cat9k-rpbase.16.10.01.SPA.pkg
Added cat9k-rpboot.16.10.01.SPA.pkg
Added cat9k-sipbase.16.10.01.SPA.pkg
Added cat9k-sipspa.16.10.01.SPA.pkg
Added cat9k-srdriver.16.10.01.SPA.pkg
Added cat9k-webui.16.10.01.SPA.pkg
Added cat9k-wlc.16.10.01.SPA.pkg
Finished list of software package changes
SUCCESS: Software provisioned. New software will load on reboot.
[2]: Finished install successful on switch 2
[3]: install package(s) on switch 3
--- 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.16.10.01.SPA.pkg
Added cat9k-espbase.16.10.01.SPA.pkg
Added cat9k-guestshell.16.10.01.SPA.pkg
```

```
Added cat9k-rpbase.16.10.01.SPA.pkg
Added cat9k-rpboot.16.10.01.SPA.pkg
Added cat9k-sipbase.16.10.01.SPA.pkg
Added cat9k-sipspa.16.10.01.SPA.pkg
Added cat9k-srdriver.16.10.01.SPA.pkg
Added cat9k-webui.16.10.01.SPA.pkg
Added cat9k-wlc.16.10.01.SPA.pkg
Finished list of software package changes
SUCCESS: Software provisioned. New software will load on reboot.
[3]: Finished install successful on switch 3
Checking status of install on [1 2 3]
[1 2 3]: Finished install in switch 1 2 3
SUCCESS: Finished install: Success on [1 2 3]
```

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

The following sample output displays installation of the Cisco IOS XE Gibraltar 16.10.1 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 16.10.1:

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

install_add_activate_commit: START Wed Oct 31 19:54:51 UTC 2018

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]y
Building configuration...

[OK]Modified configuration has been saved

*Oct 31 19:54:55.633: %IOSXE-5-PLATFORM: Switch 1 R0/0: Oct 31 19:54:55 install_engine.sh:

%INSTALL-5-INSTALL_START_INFO: Started install one-shot
flash:cat9k_iosxe.16.10.01.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.16.10.01.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
Following packages shall be activated:
/flash/cat9k-wlc.16.10.01.SPA.pkg
/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

*Oct 31 19:57:41.145: %IOSXE-5-PLATFORM: Switch 1 R0/0: Oct 31 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 Tue Oct 31 19:57:48 UTC 2018
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 16.10.1:

```
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  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 (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 16.10.1 upgrade scenario:

```
Switch# dir flash:*.pkg

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.16.10.01.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 6** 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 **dir flash:*.pkg** 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 through **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 16.10.1 | Either **install** commands or **request platform software** commands | 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 16.6.1, 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. If you add a new switch model to an existing stack, we recommend upgrading all existing switches to the latest release.

### 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 Cisco IOS XE Gibraltar 16.10.1 files using the **install remove inactive** command:

```
Switch# install remove inactive

install_remove: START Wed Oct 31 19:51:48 UTC 2018
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.16.10.01.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.16.10.01.SPA.pkg
/flash/cat9k-wlc.16.10.01.SPA.pkg
/flash/packages.conf

Do you want to remove the above files? [y/n]y
[switch 1]:
Deleting file flash:cat9k-cc_srdriver.16.10.01.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-wlc.16.10.01.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 Wed Oct 31 19:52:25 UTC 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.16.06.01.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 Oct 31 2018 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 Wed Oct 31 19:54:51 UTC 2018

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

*Oct 31 19:54:55.633: %IOSXE-5-PLATFORM: Switch 1 R0/0: Oct 31 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

*Oct 31 19:57:41.145: %IOSXE-5-PLATFORM: Switch 1 R0/0: Oct 31 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 Wed Oct 31 19:57:48 UTC 2018
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 will not automatically downgrade. It will remain 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 9300 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 3: 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.

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 the Cisco Catalyst 9300 Series Switches datasheet at:

http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/datasheet-c78-738977.html

# Limitations and Restrictions

- 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.

- 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.

- 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.

- Stacking:
  - A switch stack supports up to eight stack members.
  - Mixed stacking is not supported. Cisco Catalyst 9300 Series Switches cannot be stacked with Cisco Catalyst 3850 Series Switches.
  - Auto upgrade for a new member switch is supported only in the install 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 2000 connections per second (CPS) at less than 50% CPU utilization. Above this rate, AVC service is not guaranteed.
- Scale—Able to handle up to 20000 bi-directional flows per 24 access ports and per 48 access ports.

- YANG data modeling limitation—A maximum of 20 simultaneous NETCONF sessions are supported.
- 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 |
| CSCvi48988 | SNMP timeout when querying entSensorValueEntry |

| Caveat ID Number | Description |
|---|---|
| CSCvi56567 | When 9300 switch boots up, link up of its downlink has delayed if switch has network module |
| CSCvk62006 | SF: ERSPAN fragments the packet and truncated remaining portion is not captured |
| CSCvm08557 | After reloading gPTP/AVB ports stuck @ disabled (not dot1as capable) |
| CSCvm33622 | WCCP redirection to proxy server breaks in certain scenarios. |
| CSCvm65080 | usbflash1 entries are displayed multiple times in sh inventory o/p after multiple SSO |
| CSCvm69029 | Yang Get-config shows all the pwd configured on switch instead it should show only last updated pwd |
| CSCvn04524 | IP Source Guard blocks traffic after host IP renewal |
| CSCvn21168 | Configure for usb on the switch are gone after renumber the switch |

## Resolved Caveats in Cisco IOS XE Gibraltar 16.10.1

| Caveat ID Number | Description |
|---|---|
| CSCvi81569 | FNF is not exporting after reload when ETA + FNF enabled on interface |
| 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 |
| CSCvk02591 | When 10000 speed is configured on C9300-NM-4M uplink port , sh int status displays as 100 |
| CSCvk08304 | Slowness for x11perf with MGig port on 9300 |
| CSCvk33620 | in MPLS VPNv6 scenario, egress PE device does not generate ICMPv6 Too Big message |
| 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 |
| CSCvm47139 | Catalyst 3850/9300 Switches not providing PoE+ power for APs |

| Caveat ID Number | Description |
|---|---|
| CSCvm48081 | WDAVC: FNF doesn't work in some stack scenarios. |
| CSCvm51584 | Copper 25G SFPs not defaulting to autoneg |
| CSCvm65734 | IPv6 netflow not working on 9300 |
| 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 |
| CSCvm79234 | Show version cli shows invalid USB-SSD disk size on a CAT9k switch |
| 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 9300 Series Switches is at this URL: https://www.cisco.com/c/en/us/support/switches/catalyst-9300-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.