Release Notes for Cisco Catalyst 9300 Series Switches, Cisco IOS XE Fuji 16.8.x

First Published: 2018-04-06

Release Notes for Cisco Catalyst 9300 Series Switches, Cisco IOS XE Fuji 16.8.x

Introduction

Cisco Catalyst 9300 Series Switches are Cisco's lead stackable access platform for the next-generation enterprise and has 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). The series forms the foundational building block for SD-Access, which is Cisco's lead enterprise architecture.

Note Explore the Content Hub, the all new portal that offers an enhanced product documentation experience.

- Use faceted search to locate content that is most relevant to you.
- Create customized PDFs for ready reference.
- Benefit from context-based recommendations.

Get started with the Content Hub at content.cisco.com to craft a personalized documentation experience.

Do provide feedback about your experience with the Content Hub.

Whats New in Cisco IOS XE Fuji 16.8.1a

Hardware Features in Cisco IOS XE Fuji 16.8.1a

Feature Name	Description and Documentation Link
Cisco Catalyst 9300 Series Switches —Multigigabit 48-port switch (C9300-48UN)	This model is stackable, with 48 Multigigabit Ethernet (100 Mbps or 1/2.5/5 Gbps) UPoE ports, a PoE budget of 610W, with a 1100W AC power supply module. It supports StackWise-480 and StackPower. For information about the hardware, see the Cisco Catalyst 9300 Series Switches Hardware Installation Guide.
Cisco Catalyst 9300 Series Switches—25G Uplink Network Module (C9300-NM-2Y)	This module has two 25-GigabitEthernet SFP28 module slots. With the network module plugged in, the Cisco Catalyst 9300 Series Switches can support interface speeds of up to 25Gigabit. The 25-GigabitEthernet SFP28 ports also support SFP and SFP+ modules for 1-GigabitEthernet and 10-GigabitEthernet interfaces. To configure a 25-Gigabit Ethernet interface, starting in the global configuration mode, enter **interface TwentyFiveGigE** *interface-number* or **interface twe** *interface-number*. For information about the hardware, see the Cisco Catalyst 9300 Series Switches Hardware Installation Guide.
Cisco Catalyst 9300 Series Switches—MultiGigabit Ethernet Uplink Network Module (C9300-NM-4M)	This module has four 10G MultiGigabit Ethernet ports that support interface speeds of 100M/1G/2.5G/5G/10G); it can be installed in all models of Cisco Catalyst 9300 Series Switches. For information about the hardware, see the Cisco Catalyst 9300 Series Switches Hardware Installation Guide.
Cisco 25-Gigabit Ethernet Transceiver Module—SFP-H25G-CU	Supported transceiver module product numbers—SFP-H25G-CU1M, SFP-H25G-CU2M, SFP-H25G-CU3M, SFP-H25G-CU5M For information about the module, see the Cisco 25GBASE SFP28 Modules Data Sheet. For information about compatibility with a device, see the Cisco 25-Gigabit Ethernet Transceiver Modules Compatibility Matrix.

Feature Name	Description and Documentation Link
Cisco 40-Gigabit Ethernet, QSFP+ Transceiver—QSFP-H40G-AOC	Supported transceiver module product numbers—QSFP-H40G-AOC1M, QSFP-H40G-AOC2M, QSFP-H40G-AOC3M, QSFP-H40G-AOC5M, QSFP-H40G-AOC7M, QSFP-H40G-AOC10M, QSFP-H40G-AOC15M, QSFP-H40G-AOC20M, QSFP-H40G-AOC25M, QSFP-H40G-AOC30M. For information about the module, see the Cisco 40GBASE QSFP Modules Data Sheet. For information about compatibility, see the Cisco 40-Gigabit Ethernet Transceiver Modules Compatibility Matrix.
Cisco 40GBASE-LR4 QSFP module	Supported transceiver module product number—QSFP-40G-LR4-S. The module supports 40GBASE Ethernet rate only. For information about both modules, see Cisco 40GBASE QSFP Modules Data Sheet. For information about device compatibility, see the Cisco 40-Gigabit Ethernet Transceiver Modules Compatibility Matrix.
Cisco 4x10GBASE-LR QSFP module	• Supported transceiver module product number—QSFP-4X10G-LR-S • Compatible switch models—All models of the Cisco Catalyst 9300 Series Switches • Compatible network modules—C9300-NM-2Q For information about the module, see Cisco 40GBASE QSFP Modules Data Sheet. For information about device compatibility, see the Cisco 40-Gigabit Ethernet Transceiver Modules Compatibility Matrix.
Cisco 40GBASE-SR4 QSFP module	Supported transceiver module product number—QSFP-40G-SR4-S For information about the module, see Cisco 40GBASE QSFP Modules Data Sheet. For information about device compatibility, see the Cisco 40-Gigabit Ethernet Transceiver Modules Compatibility Matrix.
Cisco 40GBASE-SR4 QSFP module (4x10G breakout mode)	• Supported transceiver module product number—QSFP-40G-SR4 • Compatible switch models—All models of the Cisco Catalyst 9300 Series Switches • Compatible network modules—C9300-NM-2Q For information about the module, see Cisco 40GBASE QSFP Modules Data Sheet. For information about device compatibility, see the Cisco 40-Gigabit Ethernet Transceiver Modules Compatibility Matrix.

Software Features in Cisco IOS XE Fuji 16.8.1a

Feature Name	Description and License Level Information
Audio Video Bridging (AVB): IEEE 802.1BA	Refers to standard IEEE 802.1 BA - AVB. This feature defines a mech whereby endpoints and the network function as a whole, to enable high-quality streaming of professional audio and video (AV) over a Ethernet infrastructure. Instead of one-to-one, the network transport e many-to-many seamless plug-n-play connections for multiple AV enc including talkers and listeners. AVB is composed of the following: • Generalized Precision Time Protocol (gPTP)—IEEE 802.1AS Provides a mechanism to synchronize clocks of the bridges an point devices in an AVB network. • Quality of Service (QoS)—IEEE 802.1Qav. Guarantees bandv and minimum bounded latency for the time-sensitive audio and streams. • Multiple Stream Reservation Protocol (MSRP)—IEEE 802.1Q Provides a mechanism for end stations to reserve network reso that will guarantee the transmission and reception of data strea across a network with the requested bandwidth. • Multiple VLAN Registration Protocol (MVRP)—Provides a mechanism for dynamic maintenance of the contents of Dynar VLAN Registration Entries for each VLAN ID, and for propag the information they contain to other Bridges. **Note** AVB is supported only on the first 16 downlink ports and on all the u ports of the C9300-48UXM and C9300-48UN switch models. For t complete list of SKUs that support AVB, refer to the configuration of the required release. (Network Advantage)
AVC: NBAR2 attribute support for QoS	Wired Application Visibility and Control (Wired AVC) Attribute-ba QoS (EasyQoS)—Support for defining QoS classes and policies ba Network-Based Application Recognition (NBAR) attributes instead specific protocols, is available, with a few limitations. Only business-relevance and traffic-class are the supported NBAR attribu (DNA Advantage)

Feature Name	Description and License Level Information
Boot Integrity Visibility	Allows Cisco's platform identity and software integrity informa visible and actionable. Platform identity provides the platform's manufacturing installed identity, and software integrity exposes integrity measurements that can be used to assess whether the pl booted trusted code. (Network Essentials and Network Advantage)
DHCPv6: Client Link-Layer Address Option (RFC 6939)	Defines an optional mechanism and the related DHCPv6 option first-hop DHCPv6 relay agents (relay agents that are connected t link as the client) to provide the client's link-layer address in the messages being sent towards the server. (Network Essentials and Network Advantage)
DHCPv6: Support for Option 52 and DNS Search List (DNSSL) Option	Wireless access points use the The Dynamic Host Configuratio version 6 (DHCPv6) option 52 (RFC 5417) to supply the IPv6 ma interface addresses of the primary, secondary, and tertiary wirel controllers. The DNSSL option is a list of DNS suffix domain names used b hosts when they perform DNS query searches for short, unqualifi names. The DNSSL option contains one or more domain names (Network Essentials and Network Advantage)
Support for validation of DHCP Option 125	DHCP option 125 is used by DHCP clients and servers to ident vendor-specific information. Support for validation of DHCP option 125 is enabled if the sw configured as a DHCP relay agent or if the DHCP snooping featur on. Note that the switch drops those packets that do not conform to the format (HEX format) of option 125.
Hitless ACL Updates (IPv4 and IPv6)	Provides the capability to apply existing features to incoming tra updating new features in the TCAM. The feature prevents TCA reprogramming everytime there is a change in an IPv4 or IPv6 A given interface. (Network Advantage)

Feature Name	Description and License Level Information
IEEE 1588v2, Precision Time Protocol (PTP) support	PTP is defined in IEEE 1588 as Precision Clock Synchronization fo Networked Measurements and Control Systems, and was developed synchronize the clocks in packet-based networks that include distri device clocks of varying precision and stability. A PTP profile is the allowed PTP features applicable to a device. Only the default profil available in Cisco IOS XE Fuji 16.8.1a. (Network Advantage)
IGMP packet forwarding in IEEE 802.1Q Tunneling	This enhancement enables Internet Group Management Protocol (I packet forwarding in IEEE 802.1Q tunnels (Network Essentials and Network Advantage)
IP-aware Ingress Netflow on VRF Interfaces	Enables the collection of virtual routing and forwarding (VRF) IDs incoming packets on a device by applying an input flow monitor ha flow record that collects the VRF ID as a key or a non-key field. IP- VRF ingress Netflow is supported only on the ingress traffic with I IPv6 and Multicast Virtual Private Network version 4 (MVPNv4) a Customer Edge Router (CE) facing interface. (Network Advantage)
IPv6 support for IEEE 802.1Q Tunneling	Enables IPv6 support for the existing 802.1Q tunneling feature. 802.1Q tunneling, also known as Q-in-Q, enables service providers a single VLAN to support customers who have multiple VLANs, w preserving customer VLAN IDs and keeping traffic in different cus VLANs segregated. A port configured to support 802.1Q tunneling is a tunnel port. When you configure tunneling, you assign a tunnel po VLAN ID that is dedicated to tunneling. (Network Essentials and Network Advantage)
IPv6 support for Cisco TrustSec Security Group Tag (SGT) inline tagging	Enables IPv6 support for Cisco TrustSec SGT inline tagging. The SGT is a single label (identity tag) indicating the privileges of source within the network. It is propagated between network hops, allows any intermediary devices (switches or routers) to enforce po based on the identity tag. Cisco TrustSec capable devices can send receive packets with an SGT embedded in the MAC layer (Layer 2 (Network Advantage)

Feature Name	Description and License Level Information
IPv6 support for SGACL Policy Enforcement	Enables IPv6 support for Cisco TrustSec Security Group Acces List (SGACL) Policy Enforcement. An SGACL associates a Security Group Tag (SGT) with a polic policy is enforced upon SGT-tagged traffic egressing the Cisco domain. (Network Advantage)
Media Access Control Security (MACsec): MACsec host link encryption	Support for 128-bit AES MACsec (IEEE 802.1AE) encryption wit Key Agreement (MKA) on downlink ports is enabled. 128-bit—(Network Essentials and Network Advantage)
MACsec: Must-Secure Support for SW-SW MACsec (128-bit and 256-bit encryption)	Support for the must-secure feature is enabled for MKA uplink must-secure, all the packets in data traffic are encrypted and un packets are dropped. • 128-bit—(Network Essentials and Network Advantage) • 256-bit—(Network Advantage)
MACsec enhancements—MACsec Variable length CKN and Optional support for ICV	• MACsec Variable length CKN—Connectivity association (CKN) is enhanced to support variable length key-string fo encryption of MKA-PSK sessions. The range for CKN key varies from 1 to 32 hex-digits. • Optional support for ICV—A switch configured with MACs either MACsec or non-MACsec frames, depending on the associated with the MKA peer. MACsec frames are encryp protected with an integrity check value (ICV). Starting wit release, the ICV indicator in the MACsec Key Agreement Data Unit (MKPDU) is made optional. 128-bit—(Network Essentials and Network Advantage)
OCSP multiple response handling	Enables support to handle multiple Online Certificate Status Pro (OCSP) single responses on an OCSP client. (Network Advantage)

Feature Name	Description and License Level Information
Programmability	• gNMI Operations—Model-driven configuration and retrieval operational data using the gNMI capabilities, GET and SET R • Guest Shell Logging and Tracing Support—Provides logging s for guest applications that run separately from the host system report tracing data to the host file system. The tracing data is sa an IOX tracelog and the logging data is saved in the IOS syslo the host machine. • IPXE IPv6 support—iPXE IPv6 network boot is supported. • Model Based AAA—Implements the NETCONF Access Con Model (NACM). NACM is a form of role-based access control (R specified in RFC 6536. • NETCONF Global Session Lock and Kill Session—Provides a lock and the ability to kill non-responsive sessions in NETCO During a session conflict or client misuse of the global lock, NETCONF sessions can be monitored via the **show netconf-y sessions** command, and non-responsive sessions can be cleared the clear configuration lock command. • NETCONF and RESTCONF Debug commands—Commands debugging were added. • NETCONF and RESTCONF IPv6 Support—Data model inter (DMIs) support the use of IPv6 protocol. DMI IPv6 support h client applications to communicate with services that use IPv6 addresses. External facing interfaces will provide dual-stack su both IPv4 and IPv6. • RESTCONF—Provides an RFC 8040 compliant HTTP-based pr that provides a programmatic interface for accessing data defi YANG, using the datastore concepts defined in NETCONF. • YANG Data Models—For the list of Cisco IOS XE YANG mo available with this release, navigate to https://github.com/YangModels/yang/tree/master/vendor/cisco/xe Revision statements embedded in the YANG files indicate if th been a model revision. The *README.md* file in the same gith location highlights changes that have been made in the release • Operational Data Parser Polling—Starting with Cisco IOS XE 16.8.1a, the Operational Data Parser Polling feature is deprecat operational data models provide direct operational data model a hence this feature is no longer required. (Network Essentials and Network Advantage)

Feature Name	Description and License Level Information
Secure Storage of Encryption Keys and Passwords	Secures critical configuration, keys, and passwords by encrypti An instance-unique encryption key is stored in the hardware tru to prevent it from being compromised. This feature is enabled on that come with a hardware trust anchor, by default and is not sup platforms that do not have a hardware trust anchor. (Network Essentials and Network Advantage)
Simplified Factory Reset	Removes all customer specific data that has been added to the de the time of its shipping. Data erased includes configurations, lo bootvariables, corefiles, and credentials. (Network Essentials and Network Advantage)
Transmission Control Protocol (TCP) Maximum Segment Size (MSS) Adjustment	Enables configuration of the maximum segment size for transie that traverse the device during a TCP session. (Network Essentials and Network Advantage)
Virtual Ethernet Port Aggregator (VEPA)	Also referred to as reflective relay, the feature moves switching server, back to the physical network, and makes all virtual mach visible to the external network switch. This frees up server reso support virtual machines. VEPA provides several benefits to Virtu Bridge (VEB), which is a physical end station capability that sup bridging between multiple virtual end stations. (Network Essentials and Network Advantage)
VRF-Aware SGACL Logging	Enables logging of a Virtual Routing and Forwarding (VRF) na Security Group Access Control List (SGACL) logs, making the aware. (DNA Advantage)

New on the Web UI	
These features are introduced on the Web UI in this release	• Python Sandbox—A new sandbox is introduced that to allow APIs available to execute IOS commands (both Configurati NETCONF requests. You can try sample Python scripts to device responds to them and get a better understanding of h on the device. You can safely run your Python scripts in the them to the network device. • Expose the password life time details from AAA to Web U mechanism for defining rules, constraints and restrictions passwords.

Important Notes

Unsupported Features

- Bluetooth
- Cisco Plug-in for OpenFlow 1.3
- Cisco TrustSec Network Device Admission Control (NDAC) on Uplinks
- Converged Access for Branch Deployments
- Gateway Load Balancing Protocol (GLBP)
- IPsec VPN
- IPsec with FIPS
- Network-Powered Lighting (including COAP Proxy Server, 2-event Classification, Perpetual POE, Fast PoE)
- 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. For information about CLI help, see Understanding the Help System. Such hidden commands are only meant to assist Cisco TAC in advanced troubleshooting and are therefore not documented.

Starting with Cisco IOS XE Fuji 16.8.1a, hidden commands are available under:

- Category 1—Hidden commands in privileged or User EXEC mode. Begin by entering the **service internal** command to access these commands.
- Category 2—Hidden commands in one of the configuration modes (global, interface and so on). These commands do not require the **service internal** command.

Further, the following applies to hidden commands under Category 1 and 2:

- The commands have CLI help. Entering enter a question mark (?) at the system prompt displays the list of available commands.

  Note: For Category 1, enter the service internal command before you enter the question mark; you do not have to do this for Category 2.

- The system generates a %PARSER-5-HIDDEN syslog message when the command is used. For example:

```
*Feb 14 10:44:37.917: %PARSER-5-HIDDEN: Warning!!! 'show processes memory old-header '
 is a hidden command.
Use of this command is not recommended/supported and will be removed in future.
```

Apart from category 1 and 2, there remain internal commands displayed on the CLI, for which the system does NOT generate the %PARSER-5-HIDDEN syslog message.



Important We recommend that you use any hidden command only under TAC supervision.

If you find that you are using a hidden command, open a TAC case for help with finding another way of collecting the same information as the hidden command (for a hidden EXEC mode command), or to configure the same functionality (for a hidden configuration mode command) using non-hidden commands.

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	

Switch Model	Default License Level	Description
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	
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

Network Module	Description
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
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**

Catalyst 9300	Cisco Identity Services Engine	Cisco Access Control Server	Cisco Prime Infrastructure
Everest 16.6.1	2.2	5.4 5.5	PI 3.1.6 + Device Pack 13 See Cisco Prime Infrastructure 3.1 → **Downloads**
Everest 16.5.1a	2.1 Patch 3	5.4 5.5	-

Web UI System Requirements

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

Minimum Hardware Requirements

Processor Speed	DRAM	Number of Colors	Resolution	Font Size
233 MHz minimum[1]	512 MB[2]	256	1024 x 768	Small

1 We recommend 1 GHz
2 We recommend 1 GB DRAM

Software Requirements

Operating Systems

- Windows 10 or later
- Mac OS X 10.11 or later

Browsers

- Google Chrome—Version 38 or later (On Windows and Mac)
- Microsoft Edge
- Mozilla Firefox—Version 42 or later (On Windows and Mac)
- Safari—Version 9 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 Fuji 16.8.1a	CAT9K_IOSXE	cat9k_iosxe.16.08.01a.SPA.bin
	Licensed Data Payload Encryption (LDPE)	cat9k_iosxeldpe.16.08.01a.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 Fuji 16.8.1a first time	The boot loader may be upgraded to version 16.8.1r. For example:
	`ROM: IOS-XE ROMMON`
	`BOOTLDR: System Bootstrap, Version 16.8.1r [FC4], RELEASE SO`
	If the automatic boot loader upgrade occurs, while booting Cisco IOS X
	`%IOSXEBOOT-4-BOOTLOADER_UPGRADE: (rp/0): ### Tue Mar 13 17:5`
	`%IOSXEBOOT-4-BOOTLOADER_UPGRADE: (rp/0): boot loader upgrade`

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 **Supported starting from Cisco IOS XE Everest 16.6.2 and later releases**	
To install and activate the specified file, and to commit changes to be persistent across reloads: **install add file** *filename* [**activate commit**] To separately install, activate, commit, cancel, or remove the installation file: **install ?**	
add file tftp: *filename*	Copies the install file package from a remote location to the device and performs a compatibility check for the platform and image versions.

Summary of Software Installation Commands Supported starting from Cisco IOS XE Everest 16.6.2 and later releases	
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
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 Fuji 16.8.1a
Cisco IOS XE Everest 16.6.2 or Cisco IOS XE Everest 16.6.3	Either **install** commands or **request platform software** commands	

The sample output shows upgrade from

- Cisco IOS XE Everest 16.5.1a to Cisco IOS XE Fuji 16.8.1a using **request platform software** commands.
- Cisco IOS XE Everest 16.6.3 to Cisco IOS XE Fuji 16.8.1a 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 Fuji 16.8.1a. 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 Fuji 16.8.1a:

```
Switch# install remove inactive
install_remove: START Mon Oct 30 19:51:48 UTC 2017
Cleaning up unnecessary package files
Scanning boot directory for packages ... done.
Preparing packages list to delete ...
done.

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

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

```
Deleting file flash:packages.conf ... done.
SUCCESS: Files deleted.
--- Starting Post_Remove_Cleanup ---
Performing Post_Remove_Cleanup on all members
[1] Post_Remove_Cleanup package(s) on switch 1
[1] Finished Post_Remove_Cleanup on switch 1
Checking status of Post_Remove_Cleanup on [1]
Post_Remove_Cleanup: Passed on [1]
Finished Post_Remove_Cleanup

SUCCESS: install_remove Mon Oct 30 19:52:25 UTC 2017
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.16.08.01a.SPA.bin flash:
Destination filename [cat9k_iosxe.16.08.01a.SPA.bin]?
Accessing tftp://10.8.0.6//cat9k_iosxe.16.08.01a.SPA.bin...
Loading /cat9k_iosxe.16.08.01a.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 Mar 16 2018 10:18:11 -07:00 cat9k_iosxe.16.08.01a.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.16.08.01a.SPA.bin auto-copy.
```

The following sample output displays installation of the Cisco IOS XE Fuji 16.8.1a 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 Fuji 16.8.1a.

```
Switch# request platform software package install switch all file
flash:cat9k_iosxe.16.08.01a.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.16.08.01a.SPA.bin
[1]: Copying flash:cat9k_iosxe.16.08.01a.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.16.08.01a.SPA.pkg
Added cat9k-espbase.16.08.01a.SPA.pkg
Added cat9k-guestshell.16.08.01a.SPA.pkg
Added cat9k-rpbase.16.08.01a.SPA.pkg
Added cat9k-rpboot.16.08.01a.SPA.pkg
Added cat9k-sipbase.16.08.01a.SPA.pkg
Added cat9k-sipspa.16.08.01a.SPA.pkg
Added cat9k-srdriver.16.08.01a.SPA.pkg
Added cat9k-webui.16.08.01a.SPA.pkg
Added cat9k-wlc.16.08.01a.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.16.08.01a.SPA.pkg
Added cat9k-espbase.16.08.01a.SPA.pkg
Added cat9k-guestshell.16.08.01a.SPA.pkg
Added cat9k-rpbase.16.08.01a.SPA.pkg
Added cat9k-rpboot.16.08.01a.SPA.pkg
Added cat9k-sipbase.16.08.01a.SPA.pkg
Added cat9k-sipspa.16.08.01a.SPA.pkg
Added cat9k-srdriver.16.08.01a.SPA.pkg
Added cat9k-webui.16.08.01a.SPA.pkg
Added cat9k-wlc.16.08.01a.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.16.08.01a.SPA.pkg
Added cat9k-espbase.16.08.01a.SPA.pkg
Added cat9k-guestshell.16.08.01a.SPA.pkg
Added cat9k-rpbase.16.08.01a.SPA.pkg
Added cat9k-rpboot.16.08.01a.SPA.pkg
Added cat9k-sipbase.16.08.01a.SPA.pkg
Added cat9k-sipspa.16.08.01a.SPA.pkg
Added cat9k-srdriver.16.08.01a.SPA.pkg
Added cat9k-webui.16.08.01a.SPA.pkg
Added cat9k-wlc.16.08.01a.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 Fuji 16.8.1a 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 Fuji 16.8.1a:

```
Switch# install add file flash:cat9k_iosxe.16.08.01a.SPA.bin activate commit

install_add_activate_commit: START Fri Mar 16 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

*Mar 16 19:54:55.633: %IOSXE-5-PLATFORM: Switch 1 R0/0: Mar 16 19:54:55 install_engine.sh:

%INSTALL-5-INSTALL_START_INFO: Started install one-shot
flash:cat9k_iosxe.16.08.01a.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.16.08.01a.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.16.08.01a.SPA.pkg
/flash/cat9k-webui.16.08.01a.SPA.pkg
/flash/cat9k-srdriver.16.08.01a.SPA.pkg
/flash/cat9k-sipspa.16.08.01a.SPA.pkg
/flash/cat9k-sipbase.16.08.01a.SPA.pkg
/flash/cat9k-rpboot.16.08.01a.SPA.pkg
/flash/cat9k-rpbase.16.08.01a.SPA.pkg
/flash/cat9k-guestshell.16.08.01a.SPA.pkg
/flash/cat9k-espbase.16.08.01a.SPA.pkg
/flash/cat9k-cc_srdriver.16.08.01a.SPA.pkg

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

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

*Mar 16 19:57:41.145: %IOSXE-5-PLATFORM: Switch 1 R0/0: Mar 16 19:57:41 rollback_timer.sh:

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

```
Finished Commit

Install will reload the system now!
SUCCESS: install_add_activate_commit Mon Oct 30 19:57:48 UTC 2017
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 Fuji 16.8.1a:

```
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  Mar 16 2018 11:49:33 -07:00  cat9k-cc_srdriver.16.08.01a.SPA.pkg
491525 -rw- 78484428  Mar 16 2018 11:49:35 -07:00  cat9k-espbase.16.08.01a.SPA.pkg
491526 -rw- 1598412   Mar 16 2018 11:49:35 -07:00  cat9k-guestshell.16.08.01a.SPA.pkg
491527 -rw- 404153288 Mar 16 2018 11:49:47 -07:00  cat9k-rpbase.16.08.01a.SPA.pkg
491533 -rw- 31657374  Mar 16 2018 11:50:09 -07:00  cat9k-rpboot.16.08.01a.SPA.pkg
491528 -rw- 27681740  Mar 16 2018 11:49:48 -07:00  cat9k-sipbase.16.08.01a.SPA.pkg
491529 -rw- 52224968  Mar 16 2018 11:49:49 -07:00  cat9k-sipspa.16.08.01a.SPA.pkg
491530 -rw- 31130572  Mar 16 2018 11:49:50 -07:00  cat9k-srdriver.16.08.01a.SPA.pkg
491531 -rw- 14783432  Mar 16 2018 11:49:51 -07:00  cat9k-webui.16.08.01a.SPA.pkg
491532 -rw- 9160      Mar 16 2018 11:49:51 -07:00  cat9k-wlc.16.08.01a.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 Fuji 16.8.1a upgrade scenario:

```
Switch# dir flash:

Directory of flash:/

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

```
475148 -rw- 13248     Jul 26 2017 09:52:56 -07:00 cat9k-wlc.16.06.03.SPA.pkg

491524 -rw- 25711568  Mar 16 2018 11:49:33 -07:00  cat9k-cc_srdriver.16.08.01a.SPA.pkg
491525 -rw- 78484428  Mar 16 2018 11:49:35 -07:00  cat9k-espbase.16.08.01a.SPA.pkg
491526 -rw- 1598412   Mar 16 2018 11:49:35 -07:00  cat9k-guestshell.16.08.01a.SPA.pkg
491527 -rw- 404153288 Mar 16 2018 11:49:47 -07:00  cat9k-rpbase.16.08.01a.SPA.pkg
491533 -rw- 31657374  Mar 16 2018 11:50:09 -07:00  cat9k-rpboot.16.08.01a.SPA.pkg
491528 -rw- 27681740  Mar 16 2018 11:49:48 -07:00  cat9k-sipbase.16.08.01a.SPA.pkg
491529 -rw- 52224968  Mar 16 2018 11:49:49 -07:00  cat9k-sipspa.16.08.01a.SPA.pkg
491530 -rw- 31130572  Mar 16 2018 11:49:50 -07:00  cat9k-srdriver.16.08.01a.SPA.pkg
491531 -rw- 14783432  Mar 16 2018 11:49:51 -07:00  cat9k-webui.16.08.01a.SPA.pkg
491532 -rw- 9160      Mar 16 2018 11:49:51 -07:00  cat9k-wlc.16.08.01a.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.16.08.01a.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 Mar 16 2018 10:59:16 -07:00 packages.conf
434196 -rw- 7504 Mar 16 2018 10:59:16 -07:00 packages.conf.00-
516098 -rw- 7406 Mar 16 2018 10:58:08 -07:00 cat9k_iosxe.16.08.01a.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 Cisco IOS XE Fuji 16.8.1a image on the device:

```
Switch# show version
Cisco IOS XE Software, Version 16.08.01a
Cisco IOS Software [Fuji], Catalyst L3 Switch Software (CAT9K_IOSXE), Version 16.8.1a,
RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2018 by Cisco Systems, Inc.
Compiled Tue 03-Apr-18 18:49 by mcpre
<output truncated>
```

Downgrading in Install Mode

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

Before you begin

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

When downgrading from ...	Use these commands...	To downgrade to...
Cisco IOS XE Fuji 16.8.1a	Either **install** commands or **request platform software** commands	Cisco IOS XE Everest 16.5.1a or any Cisco IOS XE Everest 16.x.x release.

The sample output in this section shows downgrade from Cisco IOS XE Fuji 16.8.1a to Cisco IOS XE Everest 16.6.1, by using the **install** commands.

Important New switch models that are introduced in this release cannot be downgraded, so if you add a new switch to an existing stack, we recommend upgrading all existing switches to Cisco IOS XE Fuji 16.8.1a. For the list of models introduced in this release, see Hardware Features in Cisco IOS XE Fuji 16.8.1a, on page 2.

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 Fuji 16.8.1a files using the **install remove inactive** command:

```
Switch# install remove inactive

install_remove: START Fri Mar 16 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.16.08.01a.SPA.pkg
/flash/cat9k-espbase.16.08.01a.SPA.pkg
/flash/cat9k-guestshell.16.08.01a.SPA.pkg
/flash/cat9k-rpbase.16.08.01a.SPA.pkg
/flash/cat9k-rpboot.16.08.01a.SPA.pkg
/flash/cat9k-sipbase.16.08.01a.SPA.pkg
/flash/cat9k-sipspa.16.08.01a.SPA.pkg
/flash/cat9k-srdriver.16.08.01a.SPA.pkg
/flash/cat9k-webui.16.08.01a.SPA.pkg
/flash/cat9k-wlc.16.08.01a.SPA.pkg
/flash/packages.conf

Do you want to remove the above files? [y/n]y
[switch 1]:
Deleting file flash:cat9k-cc_srdriver.16.08.01a.SPA.pkg ... done.
Deleting file flash:cat9k-espbase.16.08.01a.SPA.pkg ... done.
Deleting file flash:cat9k-guestshell.16.08.01a.SPA.pkg ... done.
Deleting file flash:cat9k-rpbase.16.08.01a.SPA.pkg ... done.
Deleting file flash:cat9k-rpboot.16.08.01a.SPA.pkg ... done.
Deleting file flash:cat9k-sipbase.16.08.01a.SPA.pkg ... done.
Deleting file flash:cat9k-sipspa.16.08.01a.SPA.pkg ... done.
Deleting file flash:cat9k-srdriver.16.08.01a.SPA.pkg ... done.
Deleting file flash:cat9k-webui.16.08.01a.SPA.pkg ... done.
Deleting file flash:cat9k-wlc.16.08.01a.SPA.pkg ... done.
Deleting file flash:packages.conf ... done.
SUCCESS: Files deleted.
--- Starting Post_Remove_Cleanup ---
Performing Post_Remove_Cleanup on all members
[1] Post_Remove_Cleanup package(s) on switch 1
[1] Finished Post_Remove_Cleanup on switch 1
Checking status of Post_Remove_Cleanup on [1]
Post_Remove_Cleanup: Passed on [1]
Finished Post_Remove_Cleanup

SUCCESS: install_remove Mon Mar 16 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 Mar 16 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 Mon Oct 30 19:54:51 UTC 2017

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 30 19:54:55.633: %IOSXE-5-PLATFORM: Switch 1 R0/0: Oct 30 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

*Mar 16 19:57:41.145: %IOSXE-5-PLATFORM: Switch 1 R0/0: Mar 16 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 Fri Mar 16 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.

Using Smart Accounts

We recommend that you assign a Smart Account when you order devices or licenses. Smart Accounts enable you to manage all of your software licenses for switches, routers, firewalls, access-points or tools from one centralized website.

- Create Smart Accounts by going to https://software.cisco.com → **Administration** → **Request Smart Account**.
- Manage your licenses by going to https://software.cisco.com → **Administration** → **Manage Smart Account**.

Note This is especially relevant to the term licenses that you order, because information about the expiry of term licenses is available only through your Smart Account.

For more information about Smart Accounts and Smart Software Licensing in general, go to the Cisco Smart Software Manager (Cisco SSM) website on cisco.com: http://www.cisco.com/c/en/us/buy/smart-accounts/software-licensing.html

The possible deployment modes are:

- The right-to-use (RTU) licensing mode—Supported on Cisco Catalyst 9000 Series Switches. See The RTU Licensing Mode.
- The Smart Licensing mode—Currently not supported on Cisco Catalyst 9000 Series Switches. It is on the roadmap for future releases.

The RTU Licensing Mode

This is the currently supported licensing mode for Cisco Catalyst 9000 Series Switches.

Right-to-use (RTU) licensing allows you to order and activate a specific license type for a given license level, and then to manage license usage on your switch.

Note The RTU licensing structure has been modified to match the packaging model that will be used with Smart Licensing mode in the future. Unified licensing structures across the RTU and Smart Licensing modes, along with usage reports, will simplify migration and reduce the implementation time required for Smart Licensing.

The **license right-to-use** command (privilege EXEC mode) provides options to activate or deactivate any license supported on the platform.

Options for Base Licenses

```
license right-to-use[activate|deactivate][network-essentials|
network-advantage][all|evaluation|subscription{all|slot <1-8>}][acceptEULA]
```

Options for Add-On Licenses

```
license right-to-use[activate|deactivate]addon[dna-essentials|
dna-advantage][all|evaluation|subscription{all|slot <1-8>}][acceptEULA]
```

Usage Guidelines for the RTU Licensing Mode

- Base licenses (Network Essentials and Network-Advantage) may be ordered only with a permanent license type.
- Add-on licenses (DNA Essentials and DNA Advantage) may be ordered only with a term license type.
- You can set up Cisco SSM to receive daily e-mail alerts, to be notified of expiring add-on licenses that you want to renew.
- You must order an add-on license in order to purchase a switch. On term expiry, you can either renew the add-on license 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] For this combination, the DNA-Essentials license must be ordered separately using Cisco SSM.

- The following features are currently available only at the Network Advantage license level. However, the correct minimum license level for these features is Network Essentials and the CFN reflects this correct license level. You will be able to configure these features with a Network Essentials license level after the correction is made in an upcoming release:
  - IPv6 Multicast
  - IPv6 ACL Support for HTTP Servers
- Evaluation licenses cannot be ordered. They can be activated temporarily, without purchase. Warning system messages about the evaluation license expiry are generated 10 and 5 days before the 90-day window. Warning system messages are generated every day after the 90-day period. An expired evaluation license cannot be reactivated after reload.

For detailed configuration information about using the RTU Licensing Mode, see the *System Management Configuration Guide → Configuring Right-To-Use Licenses* chapter for your release.

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.
- Hardware limitations:
  - When you use Cisco 40GBASE-CR4 QSFP 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.



Note There is no option to turn autonegotiation off on the ports which connect to Cisco 40GBASE-CR4 QSFP cable.

- Interoperability limitations:
  - If one end of the link has a device running Cisco IOS XE Everest 16.6.1 or Cisco IOS XE Everest 16.6.2 or Cisco IOS XE Everest 16.6.3 and the other end is running Cisco IOS XE Fuji 16.8.1a, the link does not come up. To avoid this interoperability issue between releases, it is recommended to use the same image across all the Catalyst 9000 Series Switches in the network.
- 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.
- 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.
- 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 Fuji 16.8.x

Caveat ID Number	Description
CSCvg31906	[L3-PTP] TC mode sync/follow up packets are not forward b/w peers for inter vlan communication
CSCvg53159	%SNMP-3-RESPONSE_DELAYED: processing GetNext of cafSessionEntry.2 seen on catalyst switch
CSCvh30574	[SCALE] AVB QoS Crash "Packet Buffer Complex Stalled" with avb/no avb and overnight traffic
CSCvh49334	Cat9300 stops forwarding multicast - L3M Failed to allocate REP RI
CSCvh52491	AVB : FED_QOS_ERRMSG-3-QUEUE_BUFFER_HW_ERROR on shutting down neigh port connected to msrp listener
CSCvh63530	MPLS traffic drops with ECMP loadbalance towards core. All cat9ks
CSCvh80093	RSTP convergence is taking longer time in certain scenario
CSCvh87131	TRACEBACK: OID cefcModuleEntry crashes the box
CSCvi26179	Cat9k crash while accessing OBFL
CSCvg90106	[PTP] moving from one TC mode other mode, PTP packets is not forward by TC
CSCvg95580	interface speed config went lost after same FRU OIR with "write mem"
CSCvh72186	Cat9k ROMMON: HTTP booting does not allow specified port number
CSCvh63530	MPLS traffic drops with ECMP loadbalance towards core. All cat9ks
CSCvh80159	C9400: %BOOT-3-SYSD_STARTFAIL: R0/0: Failed to launch boot task binos_script.service (exit-code)
CSCvh84345	IOS CLI "show platform software fed switch active punt cause summary" may display negative counts

Caveat ID Number	Description
CSCvi01682	DOM data not available on SFP with Cazadero adapter when port is shut down
CSCvi21517	Username is not applying as configured in CAT 9K
CSCvi33020	QSFP-40G-SR4 (4X10G mode) in err_disable state on C9300 (2x40G uplink)
CSCvi48995	On mGig SKU - Link down with forced speed100/full duplex on both ends
CSCvi56567	When 9300 switch boots up, link up of its downlink has delayed if switch has network module
CSCvi75488	Ping from client fails with enforcement enabled on known mappings
CSCvi39202	DHCP fails when DHCP snooping trust is enabled on uplink etherchannel

Resolved Caveats in Cisco IOS XE Fuji 16.8.1a

Caveat ID Number	Description
CSCvf67030	Gi0/0 is operationally down after upgrade from 16.5.1a to 16.6.1
CSCvf75880	File size gets doubled after copy is done from FTP/USB to flash memory.
CSCvg33382	C9300 : % failed to initialize nvram
CSCvg63006	No traffic seen for SFP-10G-SR/QSA
CSCvg71134	Cat9300: Cannot transmit more then 400 Bytes on mGig ports going to Intel NIC
CSCvh04282	Cat9300 non-default system MTU config value is not respected after reload
CSCvh11925	9300 : 40G SFP displays improper DOM output with uplink FRU
CSCvh18282	Interface up is slow on Stanby(Member) after Stand(Mem) reload or redundancy force-switchover on ACT
CSCvh31431	Memory leak in linux_iosd-image on 16.6 releases
CSCvh52059	SFP-GE-T 100M full link is half duplex after reinserting SFP
CSCvh52882	Memory Leak the fed process due nbar config
CSCvh73433	Checkpoint inconsistency for FRU ports on Standby, when a member with FRU gets added during bulksync
CSCvi19809	Memory leak on C9300 due TMS process
CSCvi69699	9400 - 9300: 40G copper QSFP interoperability broken (link down)
CSCvf77673	Memory leak in OC-Platform

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

© 2018 Cisco Systems, Inc. All rights reserved.