



Release Notes for Cisco Catalyst 9600 Series Switches, Cisco IOS XE Gibraltar 16.11.x

First Published: 2019-04-15

Release Notes for Cisco Catalyst 9600 Series Switches, Cisco IOS XE Gibraltar 16.11.x

Introduction

Cisco Catalyst 9600 Series Switches are the next generation purpose-built 40 GigabitEthernet and 100 GigabitEthernet modular core and aggregation platform providing resiliency at scale with the industry's most comprehensive security while allowing your business to grow at the lowest total operational cost. They have been purpose-built to address emerging trends of Security, IoT, Mobility, and Cloud.

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

It also supports features that provide high availability, advanced routing and infrastructure services, security capabilities, and application visibility and control.

Important Notes

- [Unsupported Features, on page 1](#)
- [Complete List of Supported Features, on page 2](#)
- [Accessing Hidden Commands, on page 2](#)

Unsupported Features

- Breakout Cables
- Cisco Application Visibility and Control (AVC)
- Cisco StackWise Virtual
- Network-Based Application Recognition (NBAR) and Next Generation NBAR (NBAR2)

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

This section provides information about hidden commands in Cisco IOS XE and the security measures in place, when they are accessed. Hidden commands are 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 Command 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 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 9600 Series Switches—Model Numbers

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

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

Supported Hardware on Cisco Catalyst 9600 Series Switches

Product ID (append with "=" for spares)	Description
Supervisor Modules	
C9600-SUP-1	<p>Cisco Catalyst 9600 Series Supervisor 1 Module</p> <p>This supervisor module is supported on the C9606R chassis</p>
SATA¹ SSD² Modules (for the Supervisor)	
C9K-F2-SSD-240GB	Cisco Catalyst 9600 Series 240GB SSD Storage
C9K-F2-SSD-480GB	Cisco Catalyst 9600 Series 480GB SSD Storage
C9K-F2-SSD-960GB	Cisco Catalyst 9600 Series 960GB SSD Storage
40 or 100 GigabitEthernet Line Cards	
C9600-LC-24C	<p>Cisco Catalyst 9600 Series 24-Port 40GE/12-Port 100GE Line Card.</p> <p>It supports:</p> <ul style="list-style-type: none"> • 12 ports of 100 GigabitEthernet (GE) or 24 ports of 40GE • QSFP on all ports and QSFP28 on the 100 GE ports
25 GigabitEthernet Line Cards	
C9600-LC-48YL	<p>Cisco Catalyst 9600 Series 48-Port 25GE/10GE/1GE³ line card.</p> <p>It supports:</p> <ul style="list-style-type: none"> • 48 ports of 25 GE, or 10GE. • SFP28, SFP+ transceivers on all ports
AC Power Supply Modules	

Product ID (append with "=" for spares)	Description
C9600-PWR-2KWAC	Cisco Catalyst 9600 Series 2000W AC Power Supply Module ⁴
DC Power Supply Modules	
C9600-PWR-2KWDC	Cisco Catalyst 9600 Series 2000W DC Power Supply Module

¹ Serial Advanced Technology Attachment (SATA)

² Solid State Drive (SSD) Module

³ 1GE is currently not supported.

⁴ Power supply output capacity is 1050W at 110 VAC.

Optics Modules

Cisco Catalyst Series Switches support a wide range of optics and the list of supported optics is updated on a regular basis. Use the [Transceiver Module Group \(TMG\) Compatibility Matrix](#) tool, or consult the tables at this URL for the latest transceiver module compatibility information: https://www.cisco.com/en/US/products/hw/modules/ps5455/products_device_support_tables_list.html

Compatibility Matrix

The following table provides software compatibility information.

Catalyst 9600	Cisco Identity Services Engine	Cisco Access Control Server	Cisco Prime Infrastructure
Gibraltar 16.11.1	2.6 2.4 Patch 5	5.4 5.5	-

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 ⁵	512 MB ⁶	256	1280 x 800 or higher	Small

⁵ We recommend 1 GHz

⁶ 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)

Licensing

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

License Levels

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

Base Licenses

- Network Advantage

Add-On Licenses

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

- DNA Advantage

To find information about platform support and to know which license levels a feature is available with, use Cisco Feature Navigator. To access Cisco Feature Navigator, go to <https://www.cisco.com/go/cfn>. 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-Advantage) are ordered and fulfilled only with a permanent license type.
- Add-on licenses (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.
- 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.

Smart Licensing

Cisco Smart Licensing is a unified license management system that manages all the software licenses across Cisco products.

It enables you to purchase, deploy, manage, track and renew Cisco Software. It provides information about license ownership and consumption through a single user interface.

The solution is composed of Smart Accounts and Cisco Smart Software Manager. The former is an online account of your Cisco software assets and is required to use the latter. Cisco Smart Software Manager is where you can perform all your licensing management related tasks, such as, registering, de-registering, moving, and transferring licenses. Users can be added and given access and permissions to the smart account and specific virtual accounts.



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. Links to the configuration guide provide detailed information to help you complete each one of the smaller tasks.

Procedure

- Step 1** Begin by establishing a connection from your network to Cisco Smart Software Manager on cisco.com.
In the [software configuration guide](#) of the required release, see *System Management* → *Configuring Smart Licensing* → *Connecting to CSSM*
- Step 2** Create and activate your Smart Account, or login if you already have one.
To create and activate Smart Account, go to Cisco Software Central → [Create Smart Accounts](#). Only authorized users can activate the Smart Account.
- Step 3** Complete the Cisco Smart Software Manager set up.
- Accept the Smart Software Licensing Agreement.
 - Set up the required number of Virtual Accounts, users and access rights for the virtual account users.
- Virtual accounts help you organize licenses by business unit, product type, IT group, and so on.

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

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

With this,

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

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

If an out-of-the-box device has the software version factory-provisioned, all licenses on such a device remain in evaluation mode until registered in Cisco Smart Software Manager.

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

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 16.11.1	CAT9K_IOSXE	cat9k_iosxe.16.11.01.SPA.bin
	Licensed Data Payload Encryption (LDPE)	cat9k_iosxeldpe.16.11.01.SPA.bin

Scaling Guidelines

Limitations and Restrictions

- 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.
- Hardware Limitations — Optics:
 - Copper cables are not supported with 25GE, 40GE, and 100GE configurations
 - 1G (SFP) transceivers are not supported.
 - Installation restriction for C9600-LC-24C linecard with CVR-QSFP-SFP10G adapter —This adapter must not be installed on an even numbered port where the corresponding odd numbered port is configured as 40GE port. For example, if port 1 is configured as 40GE, CVR-QSFP-SFP10G must not be installed in port 2.
- Hardware Limitations — Power Supply Modules:
 - Input voltage for AC power supply modules—All AC-input power supply modules in the chassis must have the same AC-input voltage level.
 - Using power supply modules of different types—When mixing AC-input and DC-input power supplies, the AC-input voltage level must be 220 VAC.
- Memory leak—When a logging discriminator is configured and applied to a device, memory leak is seen under heavy syslog or debug output. The rate of the leak is dependent on the quantity of logs produced. In extreme cases, the device may fail. As a workaround, disable the logging discriminator on the device.
- 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.
- 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.
- YANG data modeling limitation—A maximum of 20 simultaneous NETCONF sessions are supported.

Caveats

Caveats describe unexpected behavior in Cisco IOS 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 16.11.x

Identifier	Description
CSCvm00478	"%FMFP-3-OBJ_DWNLD_TO_DP_FAILED: R0/0: fman_fp_image: intf TweFiveGigE5/0/1" error during bootup
CSCvm06279	C9600R convergence time is in milliseconds when SSO is done by manual SUP pull out
CSCvm44217	"show idprom int te0/1" should be supported for 10GE SFP mgmt port
CSCvm45875	HA/SVL: Setting MTU 9216 is rebooting the standby
CSCvm95962	SFP+ mgmt: Incorrect led status for stby sup when transceiver isnt inserted.
CSCvn03974	C9600R: interface cfgs resets to default upon mods shut-->save cfgs-->reload-->then no shut mods
CSCvn25403	The process iomd has been helddown (rc 134) on OIR of slot 2
CSCvn31685	After modifying security-acl SDM template Security acl functionality not working on Tunnel interface
CSCvn57413	Traffic drop during ipv6 multicast scale test
CSCvo47513	active supervisor crashed during oir of a linecard.

Resolved Caveats in Cisco IOS XE Gibraltar 16.11.1

Identifier	Description
CSCvk00432	Memory leak in alloc_repexp_entry caused by alloc_ril_index failure
CSCvm45417	Cat9K HA/ 16.9.x,16.10.x- Connectivity issue due to wrong dest MAC rewrite for routed packet
CSCvm94132	AAL-INFRA:L2 failed to get ID handle

Identifier	Description
CSCvo19717	crash in fib_path_list_walk_apply (cisco.comp/cfc_cefmppls/cef/src/fib_path_list_deps.c)

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

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

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

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

Obtaining Documentation and Submitting a Service Request

- To receive timely, relevant information from Cisco, sign up at [Cisco Profile Manager](#).
- To get the business impact you're looking for with the technologies that matter, visit [Cisco Services](#).
- To submit a service request, visit [Cisco Support](#).
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit [Cisco Marketplace](#).
- To obtain general networking, training, and certification titles, visit [Cisco Press](#).
- To find warranty information for a specific product or product family, access [Cisco Warranty Finder](#).

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

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

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

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

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

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

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

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

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

© 2019 Cisco Systems, Inc. All rights reserved.