Release Notes for Cisco Catalyst 9800 Series Wireless Controller, Cisco IOS XE Gibraltar Release 16.10.x

First Published: 2018-11-20

Release Notes for Cisco Catalyst 9800 Series Wireless Controller, Cisco IOS XE Gibraltar 16.10.x

Introduction to Cisco Catalyst 9800 Series Wireless Controllers

The Cisco Catalyst 9800 Series Wireless Controllers comprise next-generation wireless controllers (referred to as *controller* in this document) built for intent-based networking. The controllers use Cisco IOS XE software and integrate the radio frequency (RF) capabilities from Cisco Aironet with the intent-based networking capabilities of Cisco IOS XE to create a best-in-class wireless experience for your organization.

The controllers are enterprise ready to power your business-critical operations and transform end-customer experiences:

- The controllers come with high availability and seamless software updates that are enabled by hot and cold patching. This keeps your clients and services up and running always, both during planned and unplanned events.
- The controllers come with built-in security, including secure boot, run-time defenses, image signing, integrity verification, and hardware authenticity.
- The controllers can be deployed anywhere to enable wireless connectivity, for example, on an on-premise device, on cloud (public or private), or embedded on a Cisco Catalyst switch (for SDA deployments) or a Cisco Catalyst access point (AP).
- The controllers can be managed using Cisco Catalyst Center, programmability interfaces, for example, NETCONF and YANG,or web-based GUI or CLI.
- The controllers are built on a modular operating system. Open and programmable APIs enable the automation of your day zero to day *n* network operations. Model-driven streaming telemetry provides deep insights into your network and client health.

The controllers are available in multiple form factors to cater to your deployment options:

- Catalyst 9800 Series Wireless Controller Appliance
- Catalyst 9800 Series Wireless Controller for Cloud
- Catalyst 9800 Embedded Wireless Controller for a Cisco Switch

Note All the Cisco IOS XE programmability-related topics on the controllers are supported by DevNet, either through community-based support or through DevNet developer support. For more information, go to https://developer.cisco.com.

Note For information about the recommended Cisco IOS XE releases for Cisco Catalyst 9800 Series Wireless Controllers, see the documentation at:

https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/214749-tac-recommended-ios-xe-builds-for-wirele.html

What's New in Cisco IOS XE Gibraltar 16.10.1

The following table lists the supported virtual and hardware platforms:

Supported Virtual and Hardware Platforms

Table 1: Supported Virtual and Hardware Platforms

Platform	Description	Feature
Cisco Catalyst 9800-80 Wireless Controller	Modular wireless controller with up to 100-GE uplinks and seamless software updates. Controller occupies 2-rack unit space and supports multiple module uplinks. See Table for the list of supported modules.	Cisco IOS XE Gibraltar 16.10.1
Cisco Catalyst 9800-40 Wireless Controller	A fixed wireless controller with seamless software updates for mid-size to large enterprises. Controller occupies 1-rack unit space and provides four 1-GE or 10-GE uplink ports.	Cisco IOS XE Gibraltar 16.10.1
Cisco Catalyst 9800 Wireless Controller for Cloud	A virtual form factor of the Catalyst 9800 Wireless Controller that can be deployed in a private cloud (supports ESXi, KVM, and NFVIS on ENCS hypervisors) or in the public cloud as Infrastructure as a Service (IaaS).	Cisco IOS XE Gibraltar 16.10.1
Cisco Catalyst 9800 Embedded Wireless Controller for Switch	Catalyst 9800 Wireless Controller software for the Cisco Catalyst 9300 switch brings the wired and wireless infrastructure together with consistent policy and management. This deployment model supports only SD Access, which is a highly secure solution for small campuses and distributed branches. The embedded controller supports access points (APs) only in Fabric mode.	Cisco IOS XE Gibraltar 16.10.1

The following table lists the host environments supported for private and public cloud.

Table 2: Supported Host Environments for Public and Private Cloud

Host Environment	Software Version
VMware ESXi	• VMware ESXi vSphere 6.0 • VMware ESXi vCenter 6.0
KVM	• Linux KVM based on Red Hat Enterprise Linux 7.1 and 7.2 • Ubuntu 14.04.5 LTS, Ubuntu 16.04.5 LTS
AWS	AWS EC2 platform
NFVIS	ENCS 3.8.1 and 3.9.1

YANG Data Models

For the complete list of Cisco IOS XE YANG models available with this release, go to https://github.com/YangModels/yang/tree/master/vendor/cisco/xe/16101. Revision statements embedded in the YANG files indicate if there has been a model revision. The README.md file in the same GitHub location highlights the changes that have been made in this release.

Important Notes

- By default, the controller uses a TFTP block size value of 512, which is the lowest possible value. This default setting is used to ensure interoperability with legacy TFTP servers. However, you can manually change the block size value to 8192 K using the **ip tftp blocksize** command in global configuration mode to speed up the transfer process.
- We recommend that you configure the **password encryption aes** and the **key config-key password-encrypt** *key* commands to encrypt your password.
- The features and functions that work on IPv4 networks with IPv4 addresses also works on IPv6 networks with IPv6 addresses. For a list of unsupported features, see the Unsupported Features section of the *Native IPv6* feature.
- If you encounter ERR_SSL_VERSION_OR_CIPHER_MISMATCH error from the GUI after a reboot or system crash, we recommend that you regenerate the trustpoint certificate.

  The procedure to generate a new self signed trustpoint is as follows:

```
configure terminal
no crypto pki trustpoint <trustpoint_name>
no ip http server
no ip http secure-server
ip http server
ip http secure-server
ip http authentication <local/aaa>
! use local or aaa as applicable.
```

- SNMPv3 user configuration is not reflected in the running configuration. Only SNMPv3 group configuration is visible.
- The Cisco Catalyst 9800 Series Wireless Controller has a service port, which is referred to as *GigabitEthernet 0* port. You cannot use this port for RADIUS, SNMP, DNAC Telemetry, and other communications.

  The service port only supports the following IP protocols:

  - HTTP
  - HTTPS
  - SSH
  - Licensing for Smart Licensing feature to communicate with CSSM

- To migrate public IP address from 16.12.x to 17.x. ensure that you configure the **service internal** command. Failing to do so will not carry forward the IP address.

Supported Hardware

The following table lists the supported Cisco Catalyst 9800 Series Wireless Controller hardware models and the default license levels they are delivered with.

The Base PIDs are the model numbers of the controller.

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

Table 3: Supported PIDs and Ports

Controller Model	Description
C9800-40-K9	4 1/10-Gigabit Ethernet SFP or SFP+ ports and two power supply slots
C9800-80-K9	8 1/10-Gigabit Ethernet SFP/SFP+ ports and two power supply slots The following QSFP+ ports are also supported: • EPA-18X1GE • EPA-10X10GE • EPA-1X40GE • EPA-2X40GE • EPA-1X100GE
C9800-CL-K9	Catalyst Wireless Controller as an infrastructure for Cloud.
Cisco Catalyst 9800 Embedded Wireless Controller for Switch	Catalyst Wireless Controller function on Switch

Optics Modules

Cisco Catalyst 9800 Series Wireless Controller support a wide range of optics. The list of supported optics is updated on a regular basis. See 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.

Table 4: Compatibility Matrix

Cisco Catalyst 9800 Series Wireless Controller	Cisco Identity Services Engine	Cisco Prime Infrastructure	Cisco AireOS-IRCM Interoperability	Cisco CMX
Cisco IOS XE Gibraltar 16.10.1, Cisco IOS XE Gibraltar 16.10.1e	2.2 2.3 2.4	3.5	8.8.111.0	10.5.1

Web UI System Requirements

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

Table 5: Hardware Requirements

Processor Speed	DRAM	Number of Colors	Resolution	Font Size
233 MHz minimum[1]	512 MB[2]	256	1280 x 800 or higher	Small

1 We recommend 1 GHz
2 We recommend 1 GB DRAM

Software Requirements

Operating Systems:

- Windows 7 or later
- Mac OS X 10.11 or later

Browsers:

- Google Chrome—Version 59 or later (on Windows and Mac)
- Microsoft Edge (on Windows)
- Mozilla Firefox—Version 54 or later (on Windows and Mac)
- Safari—Version 10 or later (on Mac)

Supported APs

The following Cisco APs are supported in this release.

Indoor Access Points

- Cisco Aironet 1700 Series Access Points
- Cisco Aironet 1800 Series Access Points
- Cisco Aironet 2700 Series Access Points
- Cisco Aironet 2800 Series Access Points
- Cisco Aironet 3700 Series Access Points
- Cisco Aironet 3800 Series Access Points
- Cisco Aironet 4800 Series Access Points

Outdoor Access Points

- Cisco Aironet 1542 Access Points
- Cisco Aironet 1560 Series Access Points
- Cisco Aironet 1570 Series Access Points
- Cisco Catalyst 9124AXI Access Points - supported from 17.3.4
- Cisco Catalyst 9124AXD Access Points - supported from 17.3.4
- Cisco Catalyst 9124AXE Access Points - supported from 17.3.5a

Integrated Access Points

- Integrated Access Point on Cisco 1100 ISR

Network Sensor

- Cisco Aironet 1800s Active Sensor

For information about Cisco Wireless software releases that support specific Cisco AP modules, see the "Software Release Support for Specific Access Point Modules" section in the *Cisco Wireless Solutions Software Compatibility Matrix* document.

Upgrading the Controller Software

This section describes the various aspects of upgrading the controller software.

Finding the Software Version

The package files for the Cisco IOS XE software are stored in the system board flash device (flash:).

Use the **show version** privileged EXEC command to see the software version that is running on your controller.

Note Although the **show version** output always shows the software image running on the controller, the model name shown at the end of the output is the factory configuration, and does not change if you upgrade the software license.

Use the **show install summary** privileged EXEC command to see the information about the active package.

Use the **dir** *filesystem:* privileged EXEC command to see the directory names of other software images that you have stored in flash memory.

Software Images

- **Release**—Cisco IOS XE Gibraltar 16.10.1
- **Image**—Universal
- **File Name**—C9800-universalk9_wlc.16.10.01.SPA.bin

Software Installation Commands

Cisco IOS XE Gibraltar 16.10.1	
To install and activate a specified file, and to commit changes to be persistent across reloads, run the following command: **device# install add file** *filename* **[activate |commit]** To separately install, activate, commit, end, or remove the installation file, run the following command: **device# install ?** **Note** We recommend that you use the GUI for installation.	
add file tftp: *filename*	Copies the install file package from a remote location to a device, and performs a compatibility check for the platform and image versions.
activateauto-abort-timer]	Activates the file and reloads the device. The **auto-abort-timer** keyword automatically rolls back image activation.
commit	Makes changes that are 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.

Licensing

This section provides information about the licensing packages for the features that are available in the Cisco Catalyst 9800 Series Wireless Controller.

The software features that are available on the controller fall under these license categories:

- AIR DNA Essentials (AIR-DNA-E)
- AIR DNA Advantage (AIR-DNA-A) (Includes the features that are available with the Cisco DNA Essentials license and more.)

Note The controller starts with *AIR-DNA-A* as the default. Any change in the license level requires a reboot.

Note After adding new license in the Cisco Smart Software Manager (CSSM) for customer virtual account, run the **license smart renew auth** command on the controller to get the license status changed from Out OF Compliance to Authorized.

Base Licenses

Base licenses are perpetual licenses and can be used even after the expiry of *Air-DNA-A* and *AIR-DNA-E*. Base licenses include:

- AIR Network Essentials (AIR-NE)
- AIR Network Advantage (AIR-NA) (Includes the features that are available in the Network Essentials license.)

License Term

The licenses are available for a three, five, or seven-year periods.

For a more detailed overview on Cisco Licensing, go to cisco.com/go/licensingguide.

Guidelines and Restrictions

Software

- Do not use more than 31 characters for AP names. If the AP name is 32 characters or more, it may lead to a controller crash.
- Do not deploy OVA files directly to VMware ESXi 6.5. We recommend that you use an OVF tool to deploy the OVA files.

- AP connection over network address translation (NAT) and port address translation (PAT) is not supported in the following specific scenarios (all the following conditions need to be met):
  - Data-DTLS channel is ON
  - Packets sent from the controller are bigger than minimum Path MTU packets (576B in case of IPv4) with network PMTU >= 1485.
  - PAT configured on the router or firewall and the network PMTU is less than or equal to 1485.
  - AP connection over NAT/PAT is supported in all other scenarios.

Note This restriction is not applicable from Cisco IOS XE Gibraltar 16.12.2s onwards.

- Mobility NAT is not supported.
- Firefox Version 63.x is not supported.
- The Cisco Wave 1 APs may download the image twice while moving from Cisco AireOS Release 8.3 to Cisco IOS XE Gibraltar 16.10.1. This increases the AP downtime during migration.
- Ensure that you remove the controller from Cisco Prime before disabling or enabling Netconf-YANG. Otherwise, the system may reload unexpectedly.
- Unidirectional Link Detection (UDLD) protocol is not supported.
- Voice over WLAN (VoWLAN) using SIP is not supported for FlexConnect local switching deployments.
- The Cisco Catalyst 9800 Series Wireless Controllers (C9800-CL, C9800-L, C9800-40, and C9800-80) support a maximum of 14,000 leases with internal DHCP scope.
- When you configure the Cisco Catalyst 9800 Series Wireless controllers with Cisco Aironet 3700 Series Access Points, through IPv6, and then connect IPv6 capable clients, the IP addresses of all the IPv6 clients are not updated on the controller.

Hardware

Integrated Access Point on Cisco 1100 ISR is not supported.

Interoperability with Clients

This section describes the interoperability of the controller software with client devices.

The following table lists the configurations used for testing client devices.

Table 6: Test Configuration for Interoperability

Hardware or Software Parameter	Hardware or Software Type
Release	Cisco IOS XE Gibraltar 16.10.1
Cisco Wireless Controller	See Supported Hardware, on page 4.

Hardware or Software Parameter	Hardware or Software Type
Access Points	
Radio	• 802.11ac • 802.11a • 802.11g • 802.11n
Security	Open, PSK (WPA2-AES), 802.1X (WPA2-AES) (EAP-FAST, EAP-TLS)
RADIUS	See Supported Hardware, on page 4.
Types of tests	Connectivity, traffic (ICMP), and roaming between two APs

The following table lists the client types on which the tests were conducted. Client types included laptops, hand-held devices, phones, and printers.

Issues

Issues describe unexpected behavior in Cisco IOS releases in a product. Issues that are listed as Open in a prior release are carried forward to the next release as either Open or Resolved.

Note All incremental releases contain fixes from the current release.

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 an issue, click the corresponding identifier.

Open Caveats

Caveat ID	Description
CSCvm54565	All configs are not available in the new Active after a switchover.
CSCvh19066	Increase the TFTP default block size to reduce image download time.
CSCvk79428	The **show tech wireless** command is showing PSK information in clear text.
CSCvm44504	The client delete reason is shown as "WLAN Down", which is not the correct reason.
CSCvm46485	The **ipv6 radius source-interface vlan** command cannot be unconfigured.

Caveat ID	Description
CSCvm53357	The **ap country** command input (in lower case) is not working properly.
CSCvm60234	Configuring IPv6 non-local group mobility multicast also configures IPv4 non-local m
CSCvm63721	The RF profile assigned power label and channel width is failing.
CSCvm64394	Issuing the **show tech-support wireless** command from web UI results in controller re
CSCvm64484	The standby chassis is not showing redundancy IP address.
CSCvm68841	Pre-shared key (PSK) configuration is not giving an option to enter the PSK.
CSCvm75961	Observing wncd traceback in new active controller after Stateful Switchover (SSO).
CSCvm81999	The fully qualified domain name (FQDN) is not getting applied in datapath when being Identity Services Engine, post MAC Authentication Bypass (MAB).
CSCvm88919	Scanners (MC3190 and MC32N0) are not connecting to the controller after the image u
CSCvm89715	Custom webauth bundle with higher file size than the supported file size is failing to lo
CSCvm91187	Cisco Catalyst 9800-40 Wireless Controller in HA-active mode reloaded without core f was not in standby mode during upgrade.
CSCvm91561	Clients are getting deleted due to 802.11r pre-authentication failure.
CSCvm91900	Clients are getting deleted with "Invalid MDIE" error code.
CSCvm96029	Tracebacks are flooding the controller.
CSCvm98232	APs are getting reset while adding or removing description.
CSCvn04716	Running the **show logging profile wireless internal filter mac** command pauses contr
CSCvn05542	High Availability (HA) switchover retains the old active chassis uplink status irrespecti the current active link.
CSCvn06041	Cisco Aironet 2800 subordinate APs are unable to download an image from the primar
CSCvn06657	Multi-instance load balance is not working for APs joined over CAPWAPv6 tunnel.
CSCvn09552	While upgrading, subordinate APs are not fetching image from the controller.
CSCvn10305	The **clear wireless statistics fabric memory** command reports error and generates core controller.
CSCvn11667	Client is excluded due to VLAN failure, when VLAN name is propagated from the VLA (VTP) server.
CSCvn14380	The Controller GUI check boxes are not displayed in Firefox.
CSCvn19847	Client is stuck in Layer 2 authentication on the Guest controller as roam fails on the Inter- Mobility (IRCM) when **ipv4 dhcp required** command is enabled.

Caveat ID	Description
CSCvn20342	After SSO, CAPWAP IPv6 access point disjoins and joins back when wireless managemer VLAN are the same.
CSCvn22336	If the login URL for Local Web Authentication (LWA) external webauth contains a questio character, the URL is not accepted by the UI.
CSCvn23596	The output of the **show ap auto-rf dot11 24ghz** command is not displaying any data.
CSCvn26218	FlexConnect mode AP is not learning client MAC address, URL, IP address for the config URL filter.
CSCvn27287	The EXEC prompt timestamp configuration on the VTY line causes functionality issues or

Troubleshooting

For the most up-to-date, detailed troubleshooting information, see Troubleshooting TechNotes.

Related Documentation

- Information about Cisco IOS XE
- Cisco Validated Design documents
- MIB Locator to locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets

Cisco Wireless Controller

For more information about the Cisco wireless controller, lightweight APs, and mesh APs, see these documents:

- Cisco Wireless Solutions Software Compatibility Matrix
- Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide
- Cisco Catalyst 9800 Series Wireless Controller Command Reference
- Cisco Catalyst 9800 Series Configuration Best Practices
- In-Service Software Upgrade Matrix
- Upgrading Field Programmable Hardware Devices for Cisco Catalyst 9800 Series Wireless Controllers

The installation guide for your controller is available at:

- Hardware Installation Guides

All Cisco Wireless Controller software-related documentation

Cisco Wireless Access Points Detailed Channels and Maximum Power Settings

For detailed channels and maximum power settings for Cisco Wireless indoor and outdoor APs, and country support per release, see:

Detailed Channels and Maximum Power Settings Document for Supported Access Points

Feature Matrix for Cisco Wireless Access Points

Feature Matrix for Cisco Wireless Access Points

Cisco Catalyst 9800 Series Wireless Controller Data Sheets

- *Cisco Catalyst 9800-CL Wireless Controller for Cloud Data Sheet*
- *Cisco Catalyst 9800-80 Wireless Controller Data Sheet*
- *Cisco Catalyst 9800-40 Wireless Controller Data Sheet*
- *Cisco Catalyst 9800-L Wireless Controller Data Sheet*

Cisco Embedded Wireless Controller on Catalyst Access Points

For more information about the Cisco Embedded Wireless Controller on Catalyst Access Points, see:

https://www.cisco.com/c/en/us/support/wireless/embedded-wireless-controller-catalyst-access-points/tsd-products-support-series-home.html

Wireless Product Comparison

- Compare specifications of Cisco wireless APs and controllers
- Wireless LAN Compliance Lookup
- Cisco AireOS to Cisco Catalyst 9800 Wireless Controller Feature Comparison Matrix

Cisco Access Points–Statement of Volatility

The STATEMENT OF VOLATILITY is an engineering document that provides information about the device, the location of its memory components, and the methods for clearing device memory. Refer to the data security policies and practices of your organization and take the necessary steps required to protect your devices or network environment.

The Cisco Aironet and Catalyst AP Statement of Volatility (SoV) documents are available on the Cisco Trust Portal.

You can search by the AP model to view the SoV document.

Cisco Prime Infrastructure

Cisco Prime Infrastructure Documentation

Cisco Connected Mobile Experiences

Cisco Connected Mobile Experiences Documentation

Cisco Catalyst Center

Cisco Catalyst Center Documentation

Communications, Services, and Additional Information

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

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

© 2018 Cisco Systems, Inc. All rights reserved.