Release Notes for Cisco Catalyst 9800 Series Wireless Controller, Cisco IOS XE Gibraltar 16.11.1b

First Published: 2019-05-31

Release Notes for Cisco Catalyst 9800 Series Wireless Controller, Cisco IOS XE Gibraltar 16.11.1b

Introduction to Cisco Catalyst 9800 Series Wireless Controllers

Note The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

Cisco Catalyst 9800 Series comprises next-generation wireless controllers (controller) built for intent-based networking. The Catalyst 9800 Series Wireless Controllers are Cisco IOS XE-based 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 Catalyst 9800 wireless controllers are enterprise-ready to power your business-critical operations and transform end-customer experiences:

- The controllers come with high availability (HA) and seamless software updates that are enabled by hot and cold patching. This keeps your clients and services on 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 or Catalyst access point (AP).
- The controllers can be managed using Cisco Digital Network Architecture (DNA) Center, Programmability interfaces, for example, NETCONF and YANG, web-based GUI, or CLI.
- The controllers are built on a modular operating system. Open and programmable APIs enable the automation of your Day 0 to Day*n* network operations. Model-driven streaming telemetry provides deep insights into your network and client health.

The Catalyst 9800 Series Wireless 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

Note All of the Cisco IOS-XE programmability-related topics on the Cisco Catalyst 9800 Wireless Controller are supported by DevNet, either through community-based support or through DevNet developer support. For more information, go to https://developer.cisco.com.

What's New in Cisco IOS XE Gibraltar 16.11.1b

This section provides a brief introduction to the new features and enhancements that are introduced in this release.

Software Features

Automatic Spawning of Virtual Instance for Private and Public Cloud: The .RUN Installer package, which is a self-installing package, to install Cisco Catalyst 9800 Wireless Controller for ESXI, KVM, and Cisco Enterprise Network Compute System. (ENCS) environments. For more information, see the Cisco Catalyst 9800-CL Cloud Wireless Controller Installation Guide.

A public cloud supports 3000 Cisco APs and 32000 clients for flex local switching. A private cloud supports 6000 Cisco APs and 64000 clients for central switching, with a limitation of 1.5 Gbps. For more information, see the Cisco Catalyst C9800-CL Wireless Controller Virtual Deployment Guide and Deployment guide for Cisco Catalyst 9800 Wireless Controller for Cloud (C9800-CL) on Amazon Web Services (AWS).

Passive Client in SDA: Passive clients are wireless devices, such as printers and devices that are configured using a static IP address. Such clients, when associated to an access point (AP), do not transmit any IP information. That is why, the controller does not know the IP address unless they use the DHCP. For more information, see Configuring Passive Client on Software Defined Access [SDA-Wireless].

Mobility Group Member Statistics – Guest: From this release onwards, you can view the request and response packets for control and data separately. For more information, see Verifying Mobility.

Data Plane Conditional Debugging: This feature introduces MAC address as a filter for conditional debug configuration. For more information, see Conditional Debug, Radioactive Tracing, and Packet Tracing.

DHCP on AP with NAT (IPv4 only): This feature enables the internal DHCP server on a root AP in a mesh topology. For more information, see Configuring DHCP and NAT Functionality on Root Access Point.

Multicast-Based Service Discovery (mDNS Gateway): The controller acts as a Bonjour Gateway, listens for Bonjour services, caches the Bonjour advertisements (AirPlay, AirPrint, and so on) from the source or host. For more information, see Multicast Domain Name System.

Bi-directional Rate Limiting with AAA Override: The Rate Limiting feature, when clubbed with AAA override, supports a specific set of policies that is based on the time of day and day of the week. For more information, see Configuring Bi-Directional Rate Limiting Support with AAA Override.

RA Tracing for NMSP and CMX Interaction: This feature collects and provides all Cisco Connected Mobile Experiences-related (CMX-related) events. For more information, see Radioactive Tracing for NMSP.

BLE Management: The BLE Management feature supports the tasks of sending beacons or listening to beacons from small battery-powered devices. For more information, see BLE Beacons in CiscoWave 2 Access Points.

Support for AP Device PAK Updates: This feature introduces a new AP model in your wireless network using the SMU infrastructure without the need to upgrade to the new controller version. This solution is termed as AP Device Package (APDP). For more information, see New AP Model - AP Device Package (APDP).

Flex Client V6 Support with Webauth Pre and Post ACL: This feature supports IPv6 web authentication with a custom ACL and Fully Qualified Domain Name (FQDN) ACL. For more information, see Flex Client IPv6 Support with WebAuth Pre and Post ACL.

Creating a Lobby Ambassador Account and Guest User Accounts: This feature is introduced to support guest user accounts on the controller; these accounts have limited access to the network. A user with special privileges, who creates and manages the guest user accounts, and is called lobby admin, is introduced. For more information, see Creating a Lobby Ambassador Account and Guest User Accounts.

Wireless Support on Fabric Edge and Border and CP on Different Node: This is an enhancement to the Software-Defined Access Wireless deployment topologies. For more information, see Software-Defined Access Wireless.

PAT Support on CAPWAP: CAPWAP PAT is supported on the APs connected with the Cisco Catalyst 9800 Series Wireless Controller platforms from this release onwards. The following AP modes are supported: Local, Flex, SD-Wireless, Mesh, and ME. The CAPWAP PAT Support feature is not supported along with AP LAG feature.

Reboot APs by Groups: You can reboot APs by group using the **ap reset site-tag** *site-tag-name*command. For more information, see Command Reference.

Policy Classification Engine: This feature allows you to apply policies that are based on rules such as time of day, EAP profile, and so on. For more information, see Native Profiling.

Action Profile for UNKNOWN devices with Local Profiling: This feature allows you to classify a device based on new classification rules. For more information, see Native Profiling.

EoGRE: Ethernet over GRE (EoGRE) is an aggregation solution for grouping Wi-Fi traffic from hotspots. This solution enables customer premises equipment (CPE) devices to bridge the Ethernet traffic coming from an end-host, and encapsulate the traffic in Ethernet packets over an IP GRE tunnel. For more information, see Ethernet over GRE.

Note Configuring EoGRE using GUI is not supported in this release.

Mesh CAC: The Call Admission Control (CAC) enables a mesh AP to maintain controlled quality of service (QoS) on the controller to manage the voice and video quality on the mesh network. For more information, see Mesh CAC.

Per Site or Per AP Model AP SMU Upgrade: Using this feature, you can roll out the critical AP bug fixes to a subset of APs on a site or group of sites, using SMU in a staggered manner. For more information, see Software Maintenance Upgrade.

Guest Shell: A virtualized Linux-based environment that is designed to run custom Linux applications, including Python scripts for the automated control and management of Cisco devices. Using the Guest Shell, you can also install, update, and operate third-party Linux applications. This feature is applicable only to Cisco Catalyst 9800-40 and 9800-80 Series Wireless Controllers. For more information, see Guest Shell.

RESTCONF Configuration Management Protocol (RESTCONF): The HTTP-based RESTCONF protocol provides a programmatic interface that is based on standard mechanisms for accessing configuration data, state data, data-model-specific RPC operations, and events, which are defined in the YANG model. For more information, see RESTCONF Protocol.

NETCONF and RESTCONF Service Level Access Control Lists: Enables you to configure an IPv4 or IPv6 access control list (ACL) for NETCONF and RESTCONF sessions. Clients that do not conform to the configured ACLs are not allowed to access the NETCONF or RESTCONF subsystems. When service-level ACLs are configured, NETCONF and RESTCONF connection requests are filtered based on the source IP address. For more information, see NETCONF/RESTCONF Service-Level ACLs.

YANG Data Models

For the complete list of Cisco IOS XE YANG models available with this release, navigate to https://github.com/YangModels/yang/tree/master/vendor/cisco/xe/16111. Revision statements that are 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.

Hardware Features

Cisco Catalyst 9115AX APs: The Cisco Catalyst 9115AX access points are the next generation of enterprise access points that are ideal for the high-density high-definition applications. For more information, see the product page of Cisco Catalyst 9100 Access Point.

Cisco Catalyst 9117AX APs: The Cisco Catalyst 9117AX access points are the next generation Wi-Fi 802.11ax access points that are ideal for the high-density high-definition applications. For more information, see the product page of Cisco Catalyst 9100 Access Point.

Cisco Catalyst 9120AX APs: The Cisco Catalyst 9120AX access points are the next generation Wi-Fi 802.11ax access points that are ideal for the high-density high-definition applications. For more information, see the product page of Cisco Catalyst 9100 Access Point.

Note The Cisco Catalyst 9115AX, 9117AX, and 9120AX APs support only IEEE 802.11ac features.

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

When you search for the list of features by platform, select:

- 9800-40—To view all the features supported on the Cisco Catalyst 9800-40 Wireless Controller models.
- 9800-80—To view all the features supported on the Cisco Catalyst 9800-80 Wireless Controller models.
- 9800-CL—To view all the features supported on the Cisco Catalyst 9800 Wireless Controller for Cloud models.

Important Notes

- The Cisco Catalyst 9800-L Wireless Controller may fail to respond to BREAK signals received on its console port during boot time preventing the user from getting to the ROMMON. This problem is observed on the controllers manufactured till November 2019, with the default config-register setting of 0x2102. This problem can be avoided if you set the config-register to 0x2002. This problem is fixed in the 16.12(3r) ROMMON for Cisco Catalyst 9800-L Wireless Controller. For steps on how to upgrade the ROMMON, see the *Upgrading ROMMON for Cisco Catalyst 9800-L Wireless Controllers* section of Upgrading Field Programmable Hardware Devices for Cisco Catalyst 9800 Series Wireless Controllers.
- 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

Supported Hardware

The following table lists the supported virtual and hardware platforms:

Supported Virtual and Hardware Platforms

Table 1: Supported Virtual and Hardware Platforms

Platform	Description
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 Supported PIDs and Ports for the list of supported modules.
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 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).

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 and 6.7 • VMware ESXi vCenter 6.0, 6.5, and 6.7
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

The following table lists the supported Cisco Catalyst 9800 Series Wireless Controller hardware models and the default license levels they are delivered with. For information about the available license levels, see the Licensing section.

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 or 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.

Optics Modules

Cisco Catalyst 9800 Series Wireless Controller supports a wide range of optics. The list of supported optics is updated on a regular basis. See the tables at the following location for the latest transceiver module compatibility information:

https://www.cisco.com/en/US/products/hw/modules/ps5455/products_device_support_tables_list.html

Web UI System Requirements

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

Table 4: 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 Cisco Access Point Platforms

The following Cisco AP platforms 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
- Cisco Catalyst 9115AX Access Points
- Cisco Catalyst 9117AX Access Points
- Cisco Catalyst 9120AX-i Access Points - Internal Antenna SKUs only

Outdoor Access Points

- Cisco Aironet 1542 Access Points
- Cisco Aironet 1560 Series Access Points
- Cisco Aironet 1570 Series Access Points
- Cisco Industrial Wireless 3700 Series Access Points

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.

Compatibility Matrix

The following table provides software compatibility information.

Table 5: Compatibility Information

Cisco Catalyst 9800 Series Wireless Controller Software	Cisco Identity Services Engine	Cisco CMX	Cisco Prime Infrastructure	Cisco AireOS-IRCM Interoperability
Gibraltar 16.11.1b	2.6 2.4 2.3	10.6 10.5.1	3.7 3.6	8.9.100.0 8.8.120.0 8.8.111.0

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 on 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 this 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.

You can also 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 16.11.1b
- **Image**—Universal
- **File Name**—C9800-universalk9_wlc.16.11.01b.SPA.bin

Software Installation Commands

Cisco IOS XE Gibraltar 16.11.x	
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.
activate [**auto-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

- Internet Group Management Protocol (IGMP)v3 is not supported on Cisco Aironet Wave 2 APs.
- 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 16.11.1b. 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.

- Features such as AP sniffer, HALO, Multicast, and Client IPv6 are not supported on the Layer 3 deployment (wireless management interface on the Gigabit Ethernet interface 0/1 having Layer 3 IP address, or a loopback interface using Layer 3 IP address).
- 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.

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 16.11.1b
Cisco Wireless Controller	See Supported Hardware, on page 6.
Access Points	
Radio	• 802.11ax • 802.11ac • 802.11a • 802.11g • 802.11n (2.4 GHz or 5 GHz)
Security	Open, PSK (WPA2-AES), 802.1X (WPA2-AES) (EAP-FAST, EAP-TLS) 802.11ax
RADIUS	
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.

Table 7: Client Types

Client Type and Name	Driver or Software Version
Laptop Model	
Acer Aspire 15 Windows 8 Home	Qc Atheros Qca9377 11.0.0.492 and later
Acer Aspire E15 Windows 8	Qc Atheros Qca9377 15.1.1.1 and later
Acer Aspire E 15 Windows 8.1	QC Atheros Qca9377 11.0.0.492 and later
Acer Aspire E15 Windows 8.1 Pro	Qc Atheros Qca9377 11.0.0.492 and later
Apple MAC mini Windows 7 Professional	Broadcom 802.11ac 6.30.224.217 and later
Dell 80TJ	Broadcom 802.11n Network Adapter
Dell Inspiron 15 7569 Windows 10 Home	Ntel Ac 3165 18.32.0.5 and later
Dell Latitude 6430 Windows 8.1 Pro	Intel 6205w8 15.16.0.2 and later
Dell Latitude E5400 Windows 7 Professional	Intel Wifi Link 5300 AGN 12.4.1.4 and later
Dell Latitude E5430 Windows 7	Intel Centrino N 6205 15.17.0.1 and later
Dell Latitude E5450 Windows 7 Professional	Intel 7260 18.33.6.2 and later
Dell Latitude E5530	TU2-ET100 (Version v5.0R) and later
Dell Latitude E5540 Windows 7	Intel Dualband Ac7260 1.566.0.0 and later
Dell Latitude E6430 Windows 10 Enterprise	Intel Wifi Link 5300 AGN 14.2.1.4 and later
Dell Latitude E6430 Windows 10 Enterprise	Linksys AE2500 N 5.100.68.46 and later
Dell Latitude E6430 Windows 7 Professional	Intel 6250 15.11.0.7 and later
Dell Latitude E6430 Windows 7 Professional	Intel 3160 6.30.223.215 and later
Dell Latitude E7450 Windows 7 Professional	Broadcom 1560 15.1.1.1 and later
Dell Latitude Windows 8.1 Pro	Intel Ac7260 18.33.3.2 and later
Fujitsu Lifebook E556 Windows 10 Pro	Intel 8260 11.0.0.492 and later
Lenovo Ideapad T420	TU3-ETG (Version v1.0R) and later
Lenovo T420 Windows 10 Pro	Intel Ac8260 19.1.0.4 and later
Lenovo T420 Windows 7 Enterprise	Intel Centrino Ultimate-N6300 AGN 13.5.0.6 and later
Lenovo T420 Windows 7 Enterprise	Linksys AE6000 5.0.7.0 and later
Lenovo Yoga 460 Windows 10 Pro	Intel Ac8260 19.1.0.4 and later
Macbook Air Mac OS Sierra 10.12.3	Broadcom Bcm43xx 1.0 6.30.225.29.1 and later
Macbook Air Macos Sierra 10.12.6	Broadcom Bcm43xx 1.0 7.21.171.68.1a4 and later
Macbook Air OS X Yosemite (10.10.5)	Broadcom Bcm43xx 1.0 7.15.166.24.3 and later
Macbook Mac OS Mojave 10.8.5	Broadcom Bcm43xx 1.0 5.106.98.100.17 and later

Client Type and Name	Driver or Software Version
Macbook Mac OS Sierra 10.12 Beta	Broadcom Bcm43xx 1.0 7.21.149.34.1a7 and later
Macbook Pro Mac OS Sierra 10.12.4	Broadcom Bcm43xx 1.0 7.21.171.68.1a4 and later
Macbook Pro OS X 10.8.5	Broadcom Bcm43xx 1.0 5.106.98.100.17 and later
Macbook Pro Retina Mac OS Sierra 10.12.3	Broadcom Bcm43xx 1.0 7.15.166.24.3 and later
Tablet Model	
Apple iPad	iOS 12.0.1 and later
Apple iPad mini	iOS 12.0 and later
Apple iPad mini 2	iOS 10.3.1 and later
Apple iPad Air	iOS 10.1.1 and later
Apple iPad Air 2	iOS 10.2.1 and later
Mobile Phone Model	
Apple iPhone 5	iOS 10.3.1 and later
Apple iPhone 5S	iOS 11.4.1 and later
Apple iPhone 6	iOS 12.0.1 and later
Apple iPhone 6 Plus	iOS 12.0.1 and later
Apple iPhone 7	iOS 12.0.1 and later
Apple iPhone 7 Plus	iOS 12.0.1 and later
Apple iPhone 8	iOS 12.0.1 and later
Apple iPhone SE	iOS 10.3.1 and later
Apple iPhone X	iOS 12.2 and later
Apple iPhone XR	iOS 12.2 and later
Cisco 8821	SIP8821.11-0-3SR4-3 6.50.0.3 (r) and later
Google Nexus 5	Android 6.0.1 and later
MI A1	Android 8.1.0 and later
Microsoft Lumia	Windows 8 and later
Moto G 3rd Gen	Andriod 6.0.1 and later
Moto G 4	Andriod 7.0.1 and later
Moto G4 Plus	Andriod 7.0.1 and later
Moto X 2nd Gen	Android 5.0 and later
Nokia 6.1 Plus	Android 9.0.1 and later
Nokia Lumia 730	Windows 8 and later
One Plus 3	Android 6.0.1 and later

Client Type and Name	Driver or Software Version
One Plus 5	Android 8.1.0 and later
One Plus 5T	Android 8.1.0 and later
One Plus 6	Android 8.1.0 and later
One Plus One	Android 4.3 and later
Redmi Note 3	Android 6.0.1 and later
Samsung Galaxy S4	Android 4.2.2 and later
Samsung Galaxy S6	Android 7.0 and later
Samsung Galaxy S7	Android 8.0.0 and later
Samsung Galaxy S8	Android 7.0 and later
Samsung Galaxy S Duos 2	Android 6.0.1 and later
Samsung Tab Pro	Android 4.4.2 and later
Samsung Galaxy S10	Android 9.0 and later

Caveats

Caveats describe unexpected behavior in Cisco IOS releases. Caveats 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 will cover 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 a caveat, click the corresponding identifier.

Open Caveats

Caveat ID	Description
CSCvk79428	The **show tech wireless** command is showing PSK information in clear text.
CSCvk79805	The outputs of the **auto-rf dot11** commands (such as **show ap name** *name* **auto-rf dot11 dual-band** and **show ap auto-rf dot11 dual-band**) are not displaying any interference device details.

Caveat ID	Description
CSCvm69349	Link test is failing for mesh access points (APs).
CSCvn06657	Multi-instance load balance is not working for APs joined over CAPWAPv6 tunnel.
CSCvn39262	The client is moving to an exclusion state when VLAN is removed from the foreign.
CSCvn93414	APs are flapping after Stateful Switchover (SSO), when link aggregation (LAG) is enabled on the system and the APs are in flex mode.
CSCvo00177	The controller displays CPU hog message after running **show tech wireless** command.
CSCvo21047	Ethernet over GRE (EoGRE) throughput of the User Datagram Protocol (UDP) traffic is not load-balanced on the controller egress.
CSCvo22407	The **show ap upgrade** command output is not showing the correct software version after the rolling AP upgrade.
CSCvo30034	Client failed to get an IP address with the following reason: "CLIENT_DELETE_REASON_IPLEARN_CONNECT_TIMEOUT."
CSCvo39758	The SNMP warning messages that are shown for the smart licensing are incorrect.
CSCvo66241	The flex profile VLAN range in the controller and PI is not matching.
CSCvo66535	The format used to configure mac-filter for bridge-mode APs through commands and web UI are different.
CSCvo69646	The mesh root access points (RAP) are flapping during a switchover in the flex bridge.
CSCvo69679	SNMP *get* followed by *set* is returning old value for cLApDomainName.
CSCvo70896	Few APs are dropping off during SSO.
CSCvo81105	Frequent tracebacks are observed on the controller.
CSCvp08946	It is not possible to enable the conditional-web-redirect security using CLI.
CSCvp13505	Mesh APs are not joining with Extensible Authentication Protocol (EAP) external, when Identity Services Engine (ISE) is used as an authenticator.

Caveat ID	Description
CSCvp27127	The event manager CLIs under the **debug wireless mac***client-mac-add* command is failing for Terminal Access Controller Access-Control System (TACACS) users.
CSCvp27202	Setting an invalid channel on an AP results in a success message. However, the configuration is not applied.
CSCvp27269	Dynamic Host Configuration Protocol (DHCP) acknowledgment broadcast packet is causing a packet loop.
CSCvp41886	NAT translations are not being pushed to the AP.
CSCvp51506	Unsupported 802.11ax features: BSSID, Dynamic Fragment, bss-colorcode, bss-colormode, bss-partialcolor, downlink-mumimo, downlink-ofdma, target-waketime, twt-broadcast-support, uplink-mumimo, and uplink-ofdma.

Resolved Caveats

Caveat ID	Description
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.
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 multicast.
CSCvm64394	Issuing the **show tech-support wireless** command from web UI results in controller reload.
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.
CSCvm81999	The fully qualified domain name (FQDN) is not getting applied in datapath when being pushed from Identity Services Engine, post MAC Authentication Bypass (MAB).

Caveat ID	Description
CSCvm98232	APs are getting reset while adding or removing description.
CSCvn04716	Running the **show logging profile wireless internal filter mac** command pauses controller indefinitely.
CSCvn06041	Cisco Aironet 2800 subordinate APs are unable to download an image from the primary AP.
CSCvn09552	While upgrading, subordinate APs are not fetching image from the controller.
CSCvn11667	Client is excluded due to VLAN failure, when VLAN name is propagated from the VLAN Trunk Protocol (VTP) server.

Troubleshooting

For the most up-to-date, detailed troubleshooting information, visit the Cisco TAC website at:

https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/213949-wireless-debugging-and-log-collection-on.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 about the problem that you are experiencing.

Related Documentation

Information about Cisco IOS XE is available at:

https://www.cisco.com/c/en/us/products/ios-nx-os-software/ios-xe/index.html

Cisco Validated Designs documents are available at:

https://www.cisco.com/go/designzone

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use the Cisco MIB Locator found at:

http://www.cisco.com/go/mibs

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

The installation guide for your controller is available at:

- Hardware Installation Guides

For all Cisco Wireless Controller software-related documentation, see:

https://www.cisco.com/c/en/us/support/wireless/catalyst-9800-series-wireless-controllers/tsd-products-support-series-home.html

Cisco Catalyst 9800 Wireless Controller Data Sheets

- Cisco Catalyst 9800-CL Wireless Controller: https://www.cisco.com/c/en/us/products/collateral/wireless/catalyst-9800-cl-wireless-controller-cloud/nb-06-cat9800-cl-cloud-wirel-data-sheet-ctp-en.html
- Cisco Catalyst 9800-80 Wireless Controller: https://www.cisco.com/c/en/us/products/collateral/wireless/catalyst-9800-series-wireless-controllers/nb-06-cat9800-80-wirel-mod-data-sheet-ctp-en.html
- Cisco Catalyst 9800-40 Wireless Controller: https://www.cisco.com/c/en/us/products/collateral/wireless/catalyst-9800-series-wireless-controllers/nb-06-cat9800-wirel-cont-data-sheet-ctp-en.html
- Cisco Catalyst 9800-L Wireless Controller: https://www.cisco.com/c/en/us/products/collateral/wireless/catalyst-9800-series-wireless-controllers/datasheet-c78-742434.html

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 Products Comparison

- Use this tool to compare the specifications of Cisco wireless APs and controllers:

  https://www.cisco.com/c/en/us/products/wireless/wireless-lan-controller/product-comparison.html

- Wireless LAN Compliance Lookup:

  https://www.cisco.com/c/dam/assets/prod/wireless/wireless-compliance-tool/index.html

- AireOS to Catalyst 9800 Wireless Controller Feature Comparison Matrix

  https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-8/AireOS_Cat_9800_Feature_Comparison_Matrix.html

Cisco Prime Infrastructure

Cisco Prime Infrastructure Documentation

Cisco Connected Mobile Experiences

Cisco Connected Mobile Experiences Documentation

Cisco DNA Center

Cisco DNA Center Documentation

Communications, Services, and Additional Information

- 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.