Release Notes for Cisco Catalyst 9800 Series Wireless Controller, Cisco IOS XE Gibraltar 16.12.x

First Published: 2019-07-31

Last Modified: 2020-08-10

Release Notes for Cisco Catalyst 9800 Series Wireless Controller, Cisco IOS XE Gibraltar 16.12.x

Introduction to Cisco Catalyst 9800 Series Wireless Controllers

Cisco Catalyst 9800 series are next-generation wireless controllers built for intent-based networking. The Catalyst 9800 Series 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 Catalyst switch or Catalyst AP.
- The controllers can be managed using Cisco DNA Center, Programmability interfaces (for example, NETCONF/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-*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
- Catalyst 9800 Embedded Wireless Controller for Switch

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.

What's New in Cisco IOS XE Gibraltar 16.12.4a

There are no new features in this release.

What's New in Cisco IOS XE Gibraltar 16.12.3

There are no new features in this release.

In Cisco IOS XE Gibraltar 16.12.3, the semantic version number for the YANG models is not updated and is therefore not accurate. However, this limitation does not impact the functionality of the YANG models.

Unsupported SFPs:

From this release, only supported SFPs will work. If you use a nonsupported SFP, the port will not function.

What's New in Cisco IOS XE Gibraltar 16.12.2s

Behavior Change in WLAN Mapping to default-policy-profile

From Cisco IOS XE Gibraltar 16.12.2s, automatic WLAN mapping to the default policy profile under the default policy tag has been removed. If you are upgrading from a release earlier than Cisco IOS XE Gibraltar 16.12.2s, and if your wireless network uses default policy tag, it will go down due to the default mapping change. To restore the network operation, add the required WLAN to policy mappings under the default policy tag.

MIB

To download MIBs for Cisco IOS XE Gibraltar 16.12.2s release, use the following link.

https://software.cisco.com/download/home/286321396/type/280775088/release/16.12.2s

In this release, support is introduced for the following new access points:

Cisco Catalyst 9120 Access Points

- Cisco Catalyst 9120E Access Points (C9120AX-e)
- Cisco Catalyst 9120P Access Points (C9120AX-p)

Cisco Catalyst 9120 Access Points provide a seamless wireless experience anywhere and goes beyond the Wi-Fi 6 (802.11ax) standard. The access points provide integrated security, resiliency, and operational flexibility as well as increased network intelligence.

In the Cisco's intent-based networks of all sizes, the Cisco Catalyst 9120 APs scale to the growing demands of IoT devices while fully supporting the latest innovations and new technologies.

For more information about Cisco Catalyst 9120 APs, see:

https://www.cisco.com/c/en/us/products/collateral/wireless/catalyst-9120ax-series-access-points/datasheet-c78-742115.html

Cisco Catalyst 9130 Access Points (C9130AX-i)

Extending Cisco's intent-based network and perfect for networks of all sizes, the Cisco Catalyst 9130 Series scales to meet the growing demands of IoT while fully supporting the latest innovations and new technologies. The 9130 Series is also a leader in performance, security, and analytics.

For more information about Cisco Catalyst 9130 APs, see:

https://www.cisco.com/c/en/us/products/collateral/wireless/catalyst-9100ax-access-points/nb-06-cat-9130-ser-ap-ds-cte-en.html

What's New in Cisco IOS XE Gibraltar 16.12.1t

There are no new features in this release.

The following Cisco Catalyst APs are not allowed to join unsupported controller versions. If you have the following APs in your network and you want downgrade to an earlier version, we recommend that you use only Cisco IOS XE Gibraltar 16.12.1t. Do not downgrade to Cisco IOS XE Gibraltar 16.12.1s.

- Cisco Catalyst 9120E AP
- Cisco Catalyst 9120I AP
- Cisco Catalyst 9120P AP

To view the open and resolved caveats applicable to this release, see Caveats, on page 22 section.

What's New in Cisco IOS XE Gibraltar 16.12.1s

There are no new features in this release.

This release is bundled with the latest 802.11ax software version.

We recommend that you use Cisco DNA Center version 1.3.1 for this release.

What's New in Cisco IOS XE Gibraltar 16.12.1

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

Wi-Fi 6 features

OFDMA Support for 11ax APs: The 802.11ax APs support transmission to or reception of more than one client simultaneously using Orthogonal Frequency Division Multiplexing (OFDMA). The IEEE 802.11ax

protocol offers two options to create wide channels - 160-MHz channels. For more information, see the OFDMA Support for 11ax APs chapter.

Software Features

Air Time Fairness on Mesh: The Air Time Fairness (ATF) on Mesh feature is conceptually similar to the ATF feature for local APs. ATF is a form of wireless QoS that regulates downlink airtime (as opposed to egress bandwidth). For more information, see the Air Time Fairness on Mesh chapter.

Best Practices for Cisco Catalyst 9800 Series Wireless Controller: The Best Practices monitoring window reports the status of the best practices and provides a one-click Fix It or Manual Configuration option to enable (or roll back) the practices. For more information, see Best Practices chapter or click **Online Help** on the web UI.

Custom IPv6 Pre-auth ACL support for EWA and LWA: Support for Fabric mode is added for FlexConnnect Client IPv6 Support with WebAuth Pre and Post ACL.

Deny Wireless Client Session Establishment Using Calendar Profiles: This feature allows the controller to stop the client session establishment of a client at a particular time. This helps control the network in an efficient and controlled manner without any manual intervention.

In a Cisco Catalyst 9800 Series Wireless Controller, you can deny the establishment of a wireless client session based on the following recurrences:

- Daily
- Weekly
- Monthly

For more information, see the Deny Wireless Client Session Establishment Using Calendar Profiles chapter.

Enhanced Support for Public Cloud: A public cloud supports 6000 Cisco APs and 64000 clients for flex local switching. For more information, see the Deployment guide for Cisco Catalyst 9800 Wireless Controller for Cloud (C9800-CL) on Amazon Web Services (AWS).

Hotspot 2.0: The Hotspot 2.0 feature, also known as HS2 and Wi-Fi Certified Passpoint, is based on the IEEE 802.11u and Wi-Fi Alliance Hotspot 2.0 standards. It provides a better bandwidth and services-on-demand to end users. The Hotspot 2.0 feature allows mobile devices to join the Wi-Fi network automatically and also during roaming, when the devices enter a Hotspot 2.0 area. For more information, see the Hotspot 2.0 chapter.

IPv6 Multicast-to-Unicast: Support for IPv6 Multicast-to-Unicast was added from Cisco IOS XE Gibraltar 16.12.1. You can use IPv6 multicast addresses in place of IPv4 multicast addresses to enable media stream on the IPv6 networks. For more information, see the IPv6 Multicast-to-Unicast chapter.

IPv6 PI support for Cisco Catalyst 9800 Wireless Controllers: Support for Cisco Prime Infrastructure is added for IPv6-enabled Cisco Catalyst 9800 Series Wireless Controllers. You should configure static IPv6 on the Cisco Prime Infrastructure device, if IPv6- enabled Wireless Controllers are added to Cisco Prime Infrastructure.

Management Frame Protection: Management Frame Protection (MFP) provides security for the management messages passed between access points and clients. MFP provides both infrastructure and client support. For more information, see the Management Frame Protection chapter.

Security-Enhanced (SE) Linux Permissive Mode: This mode makes the practical implementation of the “principle of least privilege” possible by enforcing Mandatory Access Control (MAC) on the Cisco IOS-XE platform. SE Linux provides the capability to define policies to control the access from an application process to a resource object, thereby allowing clear definition and confinement of process behavior.

An operation in permissive mode is available with the intent of confining specific components (process or application) of the Cisco IOS-XE platform. In the permissive mode, access violation events are detected and system logs are generated, but the event or operation itself is not blocked. The solution operates mainly in an access violation detection mode.

In the enforcement mode, the loaded policy is enforced, and if a policy violation is detected, the event or operation is blocked in Cisco IOSd.

Note that no user configuration is required to enable this feature.

To display the SE Linux audit logs, use the **show platform software audit** command in privileged EXEC mode. For more information about this command, see the Cisco Catalyst 9800 Series Wireless Controller Command Reference.

Sensor support for TLS1.2 EAP PEAP and EAP TLS: The Cisco Aironet 1800 Series Access Points sensor supports TLS1.2 EAP PEAP and EAP TLS from this release onwards.

Support for –P Domain: The Cisco Catalyst 9800 Series Wireless Controller supports –P domain for Japan.

The following are the –P domain-compliant Cisco APs in this release:

- AP3802P
- AP1562E

For current approvals and regulatory domain information, see:
https://www.cisco.com/c/dam/assets/prod/wireless/wireless-compliance-tool/index.html.

Support for IPv6-enabled Cisco Catalyst 9800 Series Wireless Controller added to Cisco Prime Infrastructure: When an IPv6 enabled controller is added to Cisco Prime Infrastructure, you should configure a static IPv6 on Cisco Prime Infrastructure.

Support for Installing Cisco Catalyst 9800 Wireless Controller for Cloud on Google Cloud Platform (GCP): Support for installing Cisco Catalyst 9800 Wireless Controller for Cloud on GCP was introduced from this release. For more information, see the Cisco Catalyst 9800-CL Cloud Wireless Controller Installation Guide.

Wi-Fi Protected Access 3: WPA3 is the latest version of Wi-Fi Protected Access (WPA), which is a suite of protocols and technologies that provide authentication and encryption for Wi-Fi networks. For more information, see Wi-Fi Protected Access 3 chapter.

Wi-Fi Alliance Agile Multiband: The Wi-Fi Alliance Agile Multiband (MBO) feature enables better use of Wi-Fi network resources. This feature is built on the fundamental premise that both WiFi network and client devices have information that can aid in making roaming decisions and improve the overall performance of the WiFi network and user experience. For more information, see WiFi Alliance Agile Multiband (MBO) chapter.

Wired Guest: The Wired Guest Access feature enables guest users of an enterprise network that supports both wired and wireless access to connect to the guest access network from a wired Ethernet connection. For more information, see Wired Guest chapter.

Hardware Features

Cisco Catalyst 9800-L Wireless Controller: The Cisco Catalyst 9800-L Wireless Controller is the first low-end controller that provides a significant boost in performance and features from the Cisco 3504 Wireless Controller.

The following are the two variations of the controller:

- Cisco Catalyst 9800-L Copper Series Wireless Controller (9800-L-C RJ45)
- Cisco Catalyst 9800-L Fiber Series Wireless Controller (9800-L-F SFP)

For more information, see the Cisco Catalyst 9800-L Wireless Controller Hardware Installation Guide.

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.
- 9800-L: To view all the features supported on the Cisco Catalyst 9800-L Wireless Controller models.

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/16121. 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.

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.
- High-Availability pairing using different SKUs of the Cisco Catalyst 9800-L Series Wireless Controller isn't supported, for example, C9800-L-F-K9 and C9800-L-C-K9. HA pairing should be done only with the same SKUs, for example, C9800-L-F-K9 and C9800-L-F-K9 or C9800-L-C-K9 and C9800-L-C-K9.

- 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:

See Table 3: Supported PIDs and Ports, on page 9 for the list of supported modules.

Table 1: Supported Virtual and Hardware Platforms

Platform	Description
Cisco Catalyst 9800-80 Wireless Controller	A modular wireless controller with up to 100-GE modular uplinks and seamless software updates. Controller occupies 2-rack unit space and supports multiple module uplinks.
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.

Platform	Description
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) in AWS and GCP Marketplace.
Cisco Catalyst 9800 Embedded Wireless Controller for Switch	The Catalyst 9800 Wireless Controller software for the Cisco Catalyst 9000 switches 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 APs only in Fabric mode.
Cisco Catalyst 9800-L Wireless Controller	The Cisco Catalyst 9800-L Wireless Controller is the first low-end controller that provides a significant boost in performance and features.
Cisco Embedded Wireless Controller on Catalyst Access Points	The Cisco Embedded Wireless Controller on Catalyst Access Points is a virtualised version of the Cisco IOS XE-based controller software on Catalyst access points.

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
GCP	GCP Marketplace

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.

Note that unsupported SFPs will bring down the port. Only Cisco supported SFPs (GLC-LH-SMD and GLC-SX-MMD) are supported on the RP port of C9800-80-K9 and C9800-40-K9.

Table 3: Supported PIDs and Ports

Controller Model	Description
C9800-CL-K9	Cisco Catalyst Wireless Controller as an infrastructure for Cloud.
C9800-80-K9	Eight 1/10-Gigabit Ethernet SFP or SFP+ ports and two power supply slots The following SFPs are supported: • GLC-BX-D • GLC-BX-U • GLC-LH-SMD • GLC-SX-MMD • GLC-ZX-SMD • GLC-TE
	The following enhanced SFPs are supported: • SFP-10G-SR • SFP-10G-SR-S • SFP-10G-SR-X • SFP-10G-LR • SFP-10G-LRM • SFP-10G-LR-X • SFP-10G-ER • SFP-10G-ZR • SFP-H10GB-ACU7M • SFP-H10GB-ACU10M • DWDM-SFP10G-30.33 - DWDM-SFP10G-61.41

Controller Model	Description
	The following QSFP+ are supported: • QSFP-40G-SR4 • QSFP-40G-LR4 • QSFP-40GE-LR4 • QSFP-40G-ER4 • QSFP-40G-SR4-S • QSFP-40G-LR4-S • QSFP-40G-SR-BD • QSFP-40G-BD-RX • QSFP-100G-SR4-S • QSFP-100G-LR4-S
C9800-40-K9	Four 1/10-Gigabit Ethernet SFP or SFP+ ports and two power supply slots The following SFPs are supported: • GLC-BX-D • GLC-BX-U • GLC-LH-SMD • GLC-SX-MMD • GLC-ZX-SMD • GLC-TE

Controller Model	Description
	The following enhanced SFPs are supported: • SFP-10G-SR • SFP-10G-SR-S • SFP-10G-SR-X • SFP-10G-LR • SFP-10G-LRM • SFP-10G-LR-X • SFP-10G-ER • SFP-10G-ZR • SFP-H10GB-ACU7M • SFP-H10GB-ACU10M • DWDM-SFP10G-30.33 - DWDM-SFP10G-61.41
C9800-L-C-K9	• 4x2.5/2-Gigabit ports • 2x10/5/2.5/1-Gigabit ports The following SFPs are supported: • GLC-BX-D • GLC-BX-U • GLC-LH-SMD • GLC-SX-MMD • GLC-ZX-SMD • GLC-TE

Controller Model	Description
C9800-L-F-K9	• 4x2.5/2-Gigabit ports • 2x10/1-Gigabit ports The following SFPs are supported: • GLC-BX-D • GLC-BX-U • GLC-SX-MMD • GLC-ZX-SMD • GLC-TE • SFP-10G-SR • SFP-10G-SR-X • SFP-H10GB-ACU7M • SFP-H10GB-ACU10M

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

Compatibility Matrix

The following table provides software compatibility information.

Table 4: Compatibility Information

Cisco Catalyst 9800 Series Wireless Controller Software	Cisco Identity Services Engine	Cisco CMX	Cisco Prime Infrastructure	Cisco AireOS-IRCM Interoperability	Cisco DNA Center
Gibraltar 16.12.4a	2.6 2.4 2.3	10.6.2 10.6 10.5.1	3.7	8.10.112.0 8.10.105.0 8.9.111.0 8.9.100.0 8.8.125.0 8.8.120.0 8.8.111.0 8.5.164.0 IRCM	1.3.1
Gibraltar 16.12.3	2.6 2.4 2.3	10.6.2 10.6 10.5.1	3.7	8.10.112.0 8.10.105.0 8.9.111.0 8.9.100.0 8.8.125.0 8.8.120.0 8.8.111.0 8.5.164.0 IRCM	1.3.1
Gibraltar 16.12.2s	2.6 2.4 2.3	10.6.2 10.6 10.5.1	3.7	8.9.111.0 8.9.100.0 8.8.125.0 8.8.120.0 8.8.111.0 8.5.164.0 IRCM	1.3.1
Gibraltar 16.12.1s Gibraltar 16.12.1t	2.6 2.4 2.3	10.6.2 10.6 10.5.1	3.7	8.9.111.0 8.9.100.0 8.8.125.0 8.8.120.0 8.8.111.0 8.5.164.0 IRCM	1.3.1

Cisco Catalyst 9800 Series Wireless Controller Software	Cisco Identity Services Engine	Cisco CMX	Cisco Prime Infrastructure	Cisco AireOS-IRCM Interoperability	Cisco DNA Center
Gibraltar 16.12.1	2.6 2.4 2.3	10.6.2 10.6 10.5.1	3.7	8.9.111.0 8.9.100.0 8.8.125.0 8.8.120.0 8.8.111.0 8.5.164.0 IRCM	1.3.0[1]

[1] Support is limited only to n-1 features.

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[2]	512 MB[3]	256	1280 x 800 or higher	Small

[2] We recommend 1 GHz.
[3] 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)
- Firefox Version 63.x is not supported.

To configure VLAN through the Web UI, you must change the Virtual Terminal (VTY) lines to 50. At times, when multiple connections are open, the default VTY lines of 15 set by the device gets exhausted.

Note To increase the VTY lines in a device, run the following command in the configuration mode:

```
Device# configure terminal
Device(config)# service tcp-keepalives in
Device(config)# service tcp-keepalives out

Device# configure terminal
Device(config)# line vty 16-50
```

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
- Cisco Catalyst 9120AX-e Access Points - supported from 16.12.2s
- Cisco Catalyst 9120AX-p Access Points- supported from 16.12.2s
- Cisco Catalyst 9130AX-i Access Points- supported from 16.12.2s

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.

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 might have stored in flash memory.

Software Images

- **Release**: Cisco IOS XE Gibraltar 16.12.x
- **Image**: Universal
- **File Name**: C9800-universalk9_wlc.16.12.x.SPA.bin

Software Installation Commands

Cisco IOS XE Gibraltar 16.12.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, abort, or remove the installation file, run the following command: device# **install ?** **Note** We recommend that you use the web UI for installation.

Cisco IOS XE Gibraltar 16.12.x	
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.

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.
- Mobility NAT is not supported when the following conditions are met:
  - Data DTLS is turned on.
  - Packets sent from the controller are bigger than minimum Path MTU packets (576B in case of IPv4) with network PMTU >= 1485.
  - PAT is configured on the router or firewall.

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

- Firefox Version 63.x is not supported.
- 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.
- SIP media session snooping is not supported on 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.
- Configuring mobility MAC address (**wireless mobility mac-address**) is mandatory for both High-Availability and 802.11r.
- 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.
- Starting with Cisco IOS XE Gibraltar 16.12.1, the Cisco Catalyst 9800 Series Wireless Controller does not support satellite server for licensing reporting. You should use the Cisco Smart Software Manager (CSSM) for any licensing reporting.
- If you are upgrading from Cisco IOS XE Gibraltar 16.12.2 or an earlier release, ensure that you unconfigure the *advipservices* boot level licenses on both the active and standby controllers using the **no license boot level advipservices** command before the upgrade. Note that this command is not available on the Cisco Catalyst 9800 Wireless Controller for Cloud (9800-CL).

Interoperability with Clients

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

The following table describes 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 16.12.x
Cisco Wireless Controller	See Supported Hardware, on page 7.
Access Points	See Supported Cisco Access Point Platforms, on page 15.
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	See Compatibility Matrix, on page 12.
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/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

Client Type and Name	Driver/Software Version
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
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

Client Type and Name	Driver/Software Version
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
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

Client Type and Name	Driver/Software Version
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 for Cisco IOS XE Gibraltar 16.12.4a

Caveat ID	Description
CSCvs70701	APs are randomly taking longer time for off-channel scanning.
CSCvs77557	Cisco Aironet 3802 AP is not able to acknowledge EAP frames (EAP-TLS).
CSCvt52832	Cisco Catalyst 9120 AP reloads unexpectedly after few days of uptime.
CSCvt68112	Cisco Catalyst 9130 AP: OEAP GUI is not accessible.
CSCvt79194	Clients associated to Wave 2 AP having local switching WLAN with native VLAN is not able to resolve ARP.
CSCvt94052	Controller crashes while changing the password for an existing user.
CSCvu18085	Cisco Catalyst 9117 AP: Dot1x authentication is not working for clients.

Caveat ID	Description
CSCvu38986	Memory leak is observed under wncd_x due to CAPWAP messaging.
CSCvu40287	Cisco Catalyst 9120 AP reloads unexpectedly with watchdog_last.status reason:14.
CSCvu42653	Controller is not showing correct antenna mode.
CSCvu47560	Client goes into *exclusionlist* even when client exclusion is disabled.
CSCvu50834	Cisco Aironet 3802 AP: No Rx packets are seen for 5-GHz radio.
CSCvu54413	RFID OIDs are failing when AIRESPACE-WIRELESS-MIB RFID MIBs are used.
CSCvu55303	Cisco Catalyst 9120 AP: Kernel panic crash is observed due to sockets_in_use.
CSCvu57562	Cisco Catalyst 9130 AP is not discovering controller using the IP address returned in DHCP option 43 or DNS.
CSCvu58139	Cisco DNA Center 1.3.3.4: Default RF profile channel is configured as Best in Fabric-In-A-Box installation.
CSCvu58564	AP uses non-allowed channel on dual radio when setting is changed to 5Ghz.
CSCvu60464	Deletion and creation of second Control Plane IP is failing due to RPC ordering.
CSCvu66043	Cisco Catalyst 9130 AP is not sending DHCP messages over the air.
CSCvu71736	Cisco Catalyst 9100 Series AP: AXI-H AP models have 5Ghz radio operationally down with regulatory domain not supported for -H.
CSCvu71871	Cisco Catalyst 9800-80 controller crashes with SIGSEGV while removing timer RB tree color.
CSCvu73873	Cisco Catalyst 9800-80 controller is sending client traffic out of AP manager interface.
CSCvu75017	Cisco Catalyst 9115 AP: Syslog is only seen when using \"Kern\" facility value in AP join profile.
CSCvu78070	wncd crash is observed on Cisco IOS XE 16.12.3ES3.
CSCvu80092	RADIUS attribute [80] Message-Authenticator is not included for AP authorization.

Caveat ID	Description
CSCvu87637	Controller reloads unexpectedly due to double-linked list corruption.
CSCvu89996	AP disjoins after a client connects to SSID using LDAP with mode secure.

Open Caveats for Cisco IOS XE Gibraltar 16.12.3

Caveat ID	Description
CSCvk79897	The **show ap dot11 {24ghz | 5ghz} cleanair air-quality summary** command is displaying empty AP names.
CSCvp76426	DCA anchor time setting is not considering the timezone.
CSCvr10714	The dhcp-tlv-caching enables DHCP required on the AP. However, this prevents the AP from not forwarding the traffic.
CSCvr24930	The following message is displayed during ISSU flow: `ewlc:seeing wncd crash@ewlc_dgram_msg_and_msgbuf_free`
CSCvr68729	High Availability fails to initialize NVRAM after multiple power cycles.
CSCvs00593	Cisco Aironet 3800 AP is failing to send NDP Tx on 5GHz.
CSCvs11453	DNS resolution for RADIUS and TACACS is getting delayed for scale after a power cycle.
CSCvs22835	Cisco AP with SHA2 MIC certificate fails to join the controller configured with **config ap cert-expiry-ignore mic enable** command.
CSCvs29013	Controller is not sending SNMP traps when AP is reset using GUI or CLI.
CSCvs39458	AP Link Latency Feature is not working on the controller.
CSCvs45249	Unable to enter a valid URL in the urlfilter.
CSCvs52266	Cisco Catalyst 9800 Wireless Controller for Cloud is displaying wrong AVC data on the web UI page.
CSCvs55383	Cisco Aironet 3700 AP reloads unexpectedly.

Caveat ID	Description
CSCvs63467	IPv6 dual stack is not working on the controller.
CSCvs73952	Client count is shown as zero on the **show ap dot11 {24ghz | 5ghz} load-info** command output when Coverage Hole Detection (CHD) is disabled.
CSCvs75087	Global AP pre-image download is not working.
CSCvs82976	Cisco Discovery Protocol (CDP) entries are not displayed on the controller.
CSCvs83590	The AP Policy, RF, and Site tags are set to UNKNOWN.
CSCvs83955	Controller control packets are not honoring mobility PMTU.
CSCvs87163	Lobby Admin with external Radius Authentication is not working.
CSCvs93903	Controller restart: WNCd process is down due to assert for BSSID magic check.
CSCvs94544	The AP mode count in the **show wireless summary** output is incorrect.
CSCvt12015	QoS rate limiting input under QoS policy should be in Kilobytes and not in Kilobits.
CSCvt17820	Client gets excluded after VLAN change following machine and user authentication.
CSCvt28610	License goes to Unregistered/Evaluation after multiple switchover.

Open Caveats for Cisco IOS XE Gibraltar 16.12.2s

Caveat ID	Description
CSCvg73161	The kernel USB driver shows error logs after disabling unused USB 2.0.
CSCvm75074	The severity level of the logs generated by smart-agent is not correct.
CSCvn97793	The iPSK/MAC filtering configuration should not be pushed to the flex mode.
CSCvo64942	Move Away Table allocation to software (instead of TCAM).

Caveat ID	Description
CSCvo70439	Client is not able to associate or authenticate while validating DHCP option-82 feature on the Cisco Catalyst 9800-40 and 9800-80 Series Controllers.
CSCvp70226	ESXI 6.5 OVA: Failing to deploy an ova "deploy type" above "small".
CSCvp90090	After unmapping the policy tag ap, IOS APs are not joining the controller.
CSCvq45372	WLAN local switching (central-auth) fails for Apple clients (Macbook, iphone, and so on).
CSCvq95927	PUBD memory leak is observed on the controller.
CSCvr23906	The **show wireless summary** command output shows negative radio count and monitor count.
CSCvr25112	Wave 1 APs are observing a loss of network communication and is not be able to join the controller.
CSCvr27520	Unable to update openconfig access points, if manually configured WLANs exist on the system.
CSCvs02781	Controller is not sending redirect URL for webauth clients.
CSCvs23163	Regulatory domain for slot 0/2.4Ghz radio is read as unknown on the web UI.
CSCvs39458	AP Link Latency Feature is not working on the controller.
CSCvs49476	Cisco Aironet 1815w AP reloads unexpectedly with radio0FW coredumps.
CSCvs61547	Client dashboard is not loading on the web UI.
CSCvs62464	Unable to edit a site-tag with more than 4000 APs.
CSCvs63467	IPv6 dual stack is not working on the controller.
CSCvs68062	Cisco Catalyst 9800-40 Series Controller excludes spectralink clients due to "Wrong PSK" or "Excluded by Mobility Peer".
CSCvs68187	WLC-AP Primary Controller name and IP address mismatch.
CSCvs73459	Cisco Catalyst 9800-CL Controller reloads after running the **show redundancy trace main** command.

Caveat ID	Description
CSCvs75087	Global AP pre-image download is not working.
CSCvs75734	iOS clients are experiencing unstable wireless connection when both WPA2 and WPA3 are enabled on the Wave 2 AP.
CSCvs77734	Frequent channel change occurs on the Cisco Aironet 4800 AP on slot 0 radio using 5Ghz.
CSCvs80189	Default config register on the controller disables breaking into ROMMON thus preventing password recovery.
CSCvs81826	Upgrading to Cisco IOS XE 16.12.2s release deletes WLAN to policy profile mapping under the default-policy-tag.
CSCvs82411	Cisco Catalyst 9120 APs are unable to see neighboring APs on the controller when FIPS is enabled.
CSCvs83096	Cisco Aironet 2802 AP unexpectedly crashes.
CSCvp93355	Web UI pages are not responding when huge files are being downloaded.
CSCvq18783	Client VLAN missing is from client properties on the web UI.
CSCvq20611	Data DTLS is tearing down when port randomization is enabled on the firewall and client.
CSCvq23530	The **show wireless interface summary** command is not showing NAT public IP.
CSCvq42695	Android clients (having OS version below 8) are not able to join WPA2 802.1x WLAN when PMF is set as optional.
CSCvq45614	AP is broadcasting the wrong SSID after configuring new WLAN.
CSCvq46034	New active pubd reloads unexpectedly on Cisco 9800-40 series controller (after user induced switchover).
CSCvq46582	Clients are not able to join the Cisco 802.11AX AP.
CSCvq48656	Channel and Interference radio statistics graphs are not populated.
CSCvq52693	It is possible to configure more than 5 flow-exporters.

Caveat ID	Description
CSCvq63168	Cisco Trustpoint is not configured using Day0 in an instance launched in Google Cloud Platform (GCP).

Open Caveats for Cisco IOS XE Gibraltar 16.12.1, 16.12.1s, and 16.12.1t

Caveat ID	Description
CSCvg73161	The kernel USB driver shows error logs after disabling unused USB 2.0.
CSCvm75074	The severity level of the logs generated by smart-agent is not correct.
CSCvn97793	The iPSK/MAC filtering configuration should not be pushed to the flex mode.
CSCvo64942	Move Away Table allocation to software (instead of TCAM).
CSCvo70439	Client is not able to associate or authenticate while validating DHCP option-82 feature on the Cisco Catalyst 9800-40 and 9800-80 Series Controllers.
CSCvp70226	Esxi 6.5 ova: Failing to deploy an ova "deploy type" above "small".
CSCvp90090	After unmapping the policy tag ap, IOS APs are not joining the controller.
CSCvp93355	Web UI pages are not responding when huge files are being downloaded.
CSCvq18783	Client VLAN missing is from client properties on the web UI.
CSCvq19751	KERNEL crash is observed during a system reboot on Cisco 9115 AP.
CSCvq20611	Data DTLS is tearing down when port randomization is enabled on the firewall and client.
CSCvq21383	qfp crash @ epoll_wait after running **show idb** command on the console.
CSCvq23530	The **show wireless interface summary** command is not showing NAT public IP.
CSCvq27229	Multiple client entries are observed in a single client RA.

Caveat ID	Description
CSCvq31854	The Method field shows blank for some of the client entries in the **show wireless client summary** output.
CSCvq33391	Controller is not sending public IP in the discovery response.
CSCvq39356	RLAN AP disjoins when the RLAN client joins and further client join is not happening.
CSCvq39713	Controller console logs are flooding with "%CPPOSLIB-3-ERROR_NOTIFY" tracebacks.
CSCvq42695	Android clients (having OS version below 8) are not able to join WPA2 802.1x WLAN when PMF is set as optional.
CSCvq45614	AP is broadcasting the wrong SSID after configuring new WLAN.
CSCvq46034	New active pubd reloads unexpectedly on Cisco 9800-40 series controller (after user induced switchover).
CSCvq46525	Memory leak is observed on the Cisco 9800-L series controller.
CSCvq46582	Clients are not able to join the Cisco 802.11AX AP.
CSCvq48656	Channel and Interference radio statistics graphs are not populated.
CSCvq52693	It is possible to configure more than 5 flow-exporters.
CSCvq63168	Cisco Trustpoint is not configured using Day0 in an instance launched in Google Cloud Platform (GCP).

Resolved Caveats for Cisco IOS XE Gibraltar 16.12.4a

Caveat ID	Description
CSCvi48253	Self-signed certificates cannot be created after the time expires.
CSCvt23051	Cisco 9120AX AP: AP does not use the correct data rates.
CSCvt51865	Unable to restrict the Guest User account to a specific SSID.
CSCvu34313	Cisco Catalyst 9800-80 Controller crashes frequently with corrupted stack ending in Sanet function.

Caveat ID	Description
CSCvs87163	Lobby admin with external RADIUS authentication is not working.
CSCvt75852	New AP joins an anchor controller with a different mobility group name.
CSCvu30088	Slow memory leak due to WNCD kernel process.
CSCvr55603	Cisco Aironet 3700 AP with HALO experiences unexpected reloads.
CSCvt17820	Client gets excluded after VLAN changes post machine and user authentication.
CSCvt37835	Client is unable to associate due to DOT11_STATUS_DENIED_RATES when extended rates are used.
CSCvt29596	Current Tx rate for 802.11AX clients are displayed incorrectly.
CSCvt63940	Authentication fails in Zebra clients, when local authentication is configured in the policy profile.
CSCvu37330	Client is getting deleted due to DOT11_STATUS_DENIED_RATES.
CSCvt47787	Roaming is not successful when NAC is enabled in the policy profile.
CSCvu04970	Cisco Catalyst 9800-CL Controller running IOS XE Gibraltar 16.12.2s wncd crashes due to CPU HOG.
CSCvu41863	Controller does not send the discovery response with its public IP after reboot.
CSCvr46316	Controller does not populate AP load information in the discovery response.
CSCvs39458	AP Link Latency feature is not working.
CSCvs60927	Frequent AP channel changes are observed on 5GHz band radio.
CSCvt19281	XOR channel changes frequently when band configuration is static.
CSCvs72078	Values of client retries and Rx packets on Cisco DNA-C are different from the values seen on the AP.
CSCvt55482	Controller shows incorrect number of interferers.

Caveat ID	Description
CSCvs93903	WNCd process down due to assert for BSSID magic check.
CSCvt34987	Cisco Catalyst 9800-80 Controller HA running 'wncd' crashes frequently.
CSCvu19379	Do not present "host mode" configuration options when the RLAN profile is set to open.
CSCvs62246	The WebUI is not showing 2.4GHz channels 12, 13, or 14 for radios in country's that support these channels.
CSCvt00145	Optimize SVI/VLAN page loading.
CSCvt40291	Controller GUI: AP page is stuck in buffering mode (refresh to recover the page) when filters are applied.
CSCvs94544	AP mode count is incorrect in the **show wireless summary** output.
CSCvr24930	Observed wncd crash@ewlc_dgram_msg_and_msgbuf_free with ISSU flow in scale.
CSCvu37389	Traceback: When AP's interface operational status goes down, SNMP trap triggers, and device reloads.
CSCvu15936	FlexConnect local-sw client is not assigned to VLAN1 when VLAN assignment is done through AAA.
CSCvp76426	Controller does not honour timezone when configuring DCA anchortime.
CSCvs77734	Frequent channel changes on the Cisco AP Aironet 4800 AP slot 0 radio using 5GHz.
CSCvs83955	Control packets not honoring Mobility PMTU.
CSCvu04994	Controller GUI: SNMPv3 privilege and authentication credentials are swapped when adding a user.
CSCvs81893	SNMP v3: Users page on the GUI does not allow configuration of passwords with special characters.
CSCvt19605	Guest anchor fails to load balance clients across anchors.
CSCvt23733	AP CAC GUI parameter displays incorrect unit. Displays bytes instead of "medium time".
CSCvt34247	AAA page does not load after upgrading to IOS XE Gibraltar 16.12.2s.

Caveat ID	Description
CSCvt34307	FT gets enabled during static WEP WLAN creation - WLAN modification throws error.
CSCvt55181	Unable to configure SNMP settings through the GUI in Japanase mode.
CSCvt64768	Unable to delete or deauthenticate excluded clients through the GUI.
CSCvt96188	Deleting a policy profile that is mapped under a policy tag should display a warning.
CSCvr91736	Tri Radio: Controller GUI does not display slot-2 details in the 360 degree view.
CSCvs73952	Client count shows zero in the **show ap dot11 5ghz/2.4ghz load-info** command output while CHD is disabled.
CSCvu23990	Controller displays that 802.11ac is not supported on XOR radios of APs.
CSCvt83553	Cisco Catalyst 9800-40 Controller: Stale FMAP-FP/CPP tunnel issue.
CSCvp88342	Controller may reload as WNCD process is held down with scaled clients.
CSCvs03712	Data rates need to be updated when the client is moving from one AP to another.
CSCvt24635	CAPWAP DTLS session is closed for AP, because of the DTLS server session shutdown.
CSCvt63822	AP sends lower bytes of packets while performing PMTU negotiations.
CSCvt73263	DTLS teardown is observed on 9120, 9115, and 9105 series of APs.
CSCvs68187	Controller-AP: Primary controller name and IP address mismatch.
CSCvs83590	AP Policy/RF/Site tags set to UNKNOWN unless tag-config is explicitly written from the controller.
CSCvs63467	IPv6 dual stack does not work.
CSCvr68729	HA failed to initialize NVRAM after multiple power cycles.
CSCvs03177	Client stuck in IP learn state with FlexConnect local switching + central DHCP + DHCP required.

Caveat ID	Description
CSCvs11453	When the power box is reset, DNS resolution for Radius and TACACS is delayed for scale.
CSCvs50944	Controller loses smart licensing registration if integrated with DNA spaces after a reboot.
CSCvt06125	Cisco Aironet 1570 series AP crashes if WLAN with ID >= 17 is configured in the policy tag.
CSCvt08645	Multicast replicates over CAPWAP with global multicast disabled
CSCvt31138	Controller goes down and reloads when AVC is enabled.
CSCvt31798	Cisco 9800 running IOS XE Gibraltar 16.12.3 does not send RSSI messages over NMSP.
CSCvt34850	CWA GA scenario client removed after export anchor response received from WLC due profile plumb.
CSCvt41053	Controller is assigned to native VLAN instead of client VLAN.
CSCvt75205	Controller crashes on WMM action, while roaming.
CSCvt83796	APs do not apply client QoS policy in FlexConnect local-sw and local-auth.
CSCvs75087	Global AP pre-image download is not working.
CSCvs82976	CDP entries are not showing up on the controller.
CSCvt27421	Cannot remove AdvIPServices license.
CSCvt27712	Critical Syslog notification support required when unsupported SFPs are connected.
CSCvt29373	9800-40/80 UDP Port 5246 based ACL filter fails to select DTLS encrypted CAPWAP control packets.
CSCvt30657	Controller crashed with the following reason "Critical process cpp_cp_svr fault on fp_0_0 (rc=134)".
CSCvt47898	Controller reloads when processing AVC or FNF.
CSCvt52436	Controller is unable to downgrade license: Device is not authorized to use the given license level.
CSCvt61509	Cisco Aironet 3700 APs are unable to join controller as the VLAN interface name exceeds character limit in flex profile.

Caveat ID	Description
CSCvt62706	Require MAB username delimiter with single hypen.
CSCvt79712	Client is deleted due to the CO_CLIENT_DELETE_REASON_NOOP reason code.
CSCvt80690	ARP request comes from a formerly active controller on HA with split brain scenario.
CSCvt31484	Controller may crash when an AP joins and does not report the correct radios.
CSCvt33624	Cisco Aironet 2800 AP - XOR in 5g: Clients unable to join, AP deauth reason "Invalid group cipher (0x0012)?".
CSCvt49983	Invalid values for AP performance profile.
CSCvs89556	Pubd crash observed just after SSO.
CSCvs06271	RRM AP transmit power is not moving into the maximum or minimum configured power.
CSCvu31306	CWA ACL is removed from the existing flex AP, when a new flex profile is created with same ACL.
CSCvt01659	Cisco Wave1 AP: Client traffic is stuck after client is in RUN state for CWA/LWA.
CSCvt70299	Radius server password field shows no value (blank) in the GUI.
CSCvr86115	Controller GUI has no option to configure AP LED state for IOS APs.
CSCvt17800	Unable to map the attribute map to a user through the GUI.
CSCvu36251	CleanAir Admin Status is displayed as DISABLED on controller Japanese GUI.
CSCvt18875	Basic Wireless setup error, "Use of default ACL preauth v4 is not permitted".
CSCvt13127	Cisco Catalyst 9800-CL Controller is unable to display medium power when AP sends 25W POE message.
CSCvt17801	Cisco Aironet AP 2800/3800/4800/1560 and Cisco IW 6300 AP gets into a loop after attempting to join controller with FIPS enabled.
CSCvm68624	Cisco Wave 1 AP console displays 'DTX DUMP' logs.

Caveat ID	Description
CSCvn25452	Cisco Aironet 2800/3800/4800/1560 APs unexpectedly reloads.
CSCvo10708	Cisco Aironet 2800 and 3800 APs exhibit choppiness during the multicast voice call.
CSCvo83091	FlexConnect AP in standalone mode gets stranded and does not send CAPWAP discovery.
CSCvp54103	Cisco Wave 1 APs reload unexpectedly with 'Unexpected exception to CPU' in logs.
CSCvp70382	Kernel panic is observed.
CSCvp86151	Cisco Wave 1 AP: Radio is reset with code 44.
CSCvq27679	Cisco Aironet 1572 AP: Radio is reset due to pak count mismatch, false detection.
CSCvq76143	Cisco Aironet 2800 AP reloads unexpectedly on Sxpd process.
CSCvq81388	Cisco Wave 1 AP: Radio is reset with code 44.
CSCvq95330	Cisco Wave 2 APs: Workgroup bridge (WGB) does not send Internet Access Point Protocol (IAPP) message in static IP config.
CSCvr10424	Cisco FlexConnect AP drops UDP packet (port 2598).
CSCvr50874	Cisco Aironet 3800 AP: Kernel panic crash is observed.
CSCvr75831	Cisco Wave 1 AP: Clients are losing connectivity while roaming.
CSCvr76299	Decipher radio reset code 44 to more specific reason codes.
CSCvr87573	Cisco Aironet 2800/3800/4800/1560 series AP stops sending broadcast address resolution protocol (ARP) to wireless.
CSCvr93760	VLAN bridging problem on Cisco Aironet 1810W AP with Remote LAN (RLAN).
CSCvr97142	Root Access Point (RAP) drops radio connection, causing the Mesh Access Point (MAP) to drop. After restoring the connection, switches are not able to pass traffic.
CSCvs00593	Cisco Aironet 3800 AP is failing to send Neighbor Discovery Protocol (NDP) Tx on 5GHz.

Caveat ID	Description
CSCvs02759	Beacon is stuck followed by firmware assert. The AP radio is on channel 36 while controller thinks it's on different channel.
CSCvs12223	Cisco Aironet 3802 AP crash on watchdog reset (wcpd).
CSCvs19137	Authentication failure Extensible Authentication Protocol (EAP) timeout on a Cisco Aironet 1852 AP with data Datagram Transport Layer Security (DTLS) encryption isenabled.
CSCvs22835	Cisco AP with SHA2 message integrity check (MIC) certificate fails to join controller.
CSCvs28459	Low Received Signal Strength Indicator (RSSI) on 2.4GHz for Cisco Catalyst 9120AX-E AP as compared Cisco Aironet 2800 AP.
CSCvs41893	Cisco Aironet 3702 AP reloads unexpectedly.
CSCvs52266	Cisco Catalyst 9800-CL Controller is displaying wrong Application Visibility and Control (AVC) data on the GUI page.
CSCvs70502	Cisco Wave 1 AP reloads unexpectedly which relates to fast roaming state machine.
CSCvs72354	Cisco Catalyst 9130E AP: NSS reloads unexpectedly causing AP to be stuck in continuous loop.
CSCvs81190	AP crash is observed due to kernel panic triggered by Dynamic Frequency Selection (DFS) channel use.
CSCvs82874	Flex standalone with 11r Fallback FT Auth response code change to 53.
CSCvs88238	Client ARP and DHCP failures are observed after roaming among Cisco Wave 1 APs.
CSCvs89410	Cisco Aironet 3602 AP image corruption issue.
CSCvs93660	Frequent radio resets are observed during continuous roam (11r-OTA).
CSCvs95922	Cisco Catalyst 9120 AP: All clients are loosing connectivity on flex standalone.
CSCvt03401	AVC status is getting disabled while configuring service-policy input from DNA.
CSCvt03983	Intel clients are experiencing latency or drops when connected to Cisco Catalyst 9120 APs.

Caveat ID	Description
CSCvt04454	Cisco Catalyst 9120 AP: Flex connected to standalone; clients are loosing data.
CSCvt04710	Cisco Aironet 3700 AP: FlexConnect deauth status code is changed from 28 to 53 if 11r Pairwise Master Key (PMK) is not present.
CSCvt08586	Flex connected mode: Incorrect PMK ID causes delay in client association (Local Switch, Central Auth).
CSCvt09218	Flex connected mode: After continuous roam, client takes a longer time to reconnect.
CSCvt16983	Cisco Aironet 2700 AP: In flex standalone mode, the AP send identity request only once; need to send more.
CSCvt22353	Cisco Aironet 2800/3800/4800/1560 APs are not transmitting data frames over the air.
CSCvt26140	Clients cannot connect to Cisco Wave 1 APs with dot1x-sha256 received assoc-resp 20.
CSCvt37863	Rate limiting is not working for downstream traffic when ACL is pushed from ISE.
CSCvt38486	EAP-PEAP flex authentication fails occasionally because of low eap-timeout.
CSCvt40272	Clients connected to 2 different autonomous APs with ISE VLAN override cannot ping in 5GHz radio.
CSCvt44004	Cisco Aironet 2800 AP: Dual-Band (XOR) radio does not beacon after few iterations of moving from AUTO to 5G.
CSCvt53819	CPU exceeds 90 % with high volume traffic.
CSCvt68068	Cisco Wave 1 AP reports itself as a threat and logs \"AP Impersonation\" alerts.
CSCvt73463	Cisco Aironet 1800 AP unexpectedly reloads.
CSCvt75359	Cisco Wave 1 APs are not sending deauth rc 7 after rx frame from non assoc client.
CSCvt81606	Cisco Aironet 1832 AP kernel panic crash.
CSCvt84649	Cisco Aironet 2700 and 3800 APs are dropping ARP_REPLY packets.
CSCvt92754	Cisco Aironet 1532 AP: Ethernet interface is loosing packets.

Caveat ID	Description
CSCvu44330	Memory leak is observed under process SACRcvWQWrk2 when Smart Licensing is enabled.
CSCvu49805	Cisco Catalyst 9115AXI AP reloads unexpectedly with a kernel panic.
CSCvu78679	Cisco Aironet 2800 AP is dropping from the controller.
CSCvq81315	Cisco Aironet 2700 AP PCI0 reloads unexpectedly when Cisco CleanAir is enabled.
CSCvq98797	Traceroute fails: /bin/sh: /usr/bin/traceroute: not found.
CSCvr11240	Cisco Aironet 1815T AP is leaking client MAC from LAN3 to WAN port.
CSCvr33340	Wave 2 APs in FlexConnect mode are sending Auth Request to AAA without Local Auth Enabled.
CSCvr36185	Cisco Aironet 2800 APs are using 802.11n rates with WPA+TKIP only WLAN.
CSCvr36693	WLC 8540 OID returns small number than actual traffic size.
CSCvr39587	MAPs failing mesh_sec_auth and excluding Parent upon RAP failure.
CSCvr50653	Cisco Aironet 1562 AP in UWGB mode is unable to associate when powered up outside wireless coverage area.
CSCvr61717	WGB wired client is not getting IP when associating to Cisco Catalyst 9130 AP.
CSCvs05669	Clients connected to same SSID using different autonomous Cisco 2702 APs can not ping each other.
CSCvs09716	Cisco AP is not handling EXPIRE_MIC_PAYLOAD message.
CSCvs14548	Trustpoint configuration fails on Wave 2 APs in WGB.
CSCvs29874	802.11v Directed Multicast Service (DMS) is not shown as supported within beacon of Cisco Aironet 1852 AP.
CSCvs40887	Cisco Aironet 4800/3800/2800/1562 APs are stuck in "BootROM: Image checksum verification FAILED".

Caveat ID	Description
CSCvs50731	Cisco Catalyst 9130I and Cisco Aironet 1852 APs \"{watchdogd} Process syslogd gone for 60s\" & \" can't open '3410/maps'\".
CSCvs67811	Cisco APs acting as MAPs are not able to see RAPs.
CSCvs71672	Cisco AP fails to attach the VLAN tag when client user ID changes from central to local switching.
CSCvs81424	Cisco IW3702 AP: Samsung S10 client fails to associate on flex:local auth+local switch in 11r security.
CSCvs89401	Cisco Wave 2 AP beacons disabled SSID.
CSCvt01409	Dual-band static channel configuration switches to DCA after AP rejoin.
CSCvt06414	Cisco Catalyst 9130 AP: Kernel panic at cisco_wlan_crypto_decap.
CSCvt10962	Clients cannot connect to Cisco Aironet 1800 AP with 2.4 GHz with hidden SSID.
CSCvt15152	Cisco Aironet 4800 APs stopped supporting European weather band 5600-5650MHz- channels 120,124, and 128.
CSCvt17006	Cisco Aironet 1850AP: Clients are unable to connect to the AP.
CSCvt28616	Flexconnect reap count for current users not getting decremented causing new Wi-Fi client disconnect.
CSCvt53637	EWC conversion fails for Cisco Catalyst 9115AX AP with -T domain.
CSCvt55612	Cisco Catalyst 9120 power is lower than Cisco Aironet 2800/3800 APs with CCK rates disabled(2.4GHz).
CSCvt64308	Cisco OfficeExtend access point (OEAP) configuration doesn't get saved to AP flash.
CSCvt87401	Cisco Catalyst 9120 AP is not applying trust-dscp-upstream and CAPWAP traffic marked with UP to DSCP.
CSCvt87904	2.4GHz throughput does not change based on the number of streams.
CSCvt89989	Mesh AP: With ACL blocks ping to gateway, AP can't join controller if it doesn't complete within 45sec.

Caveat ID	Description
CSCvu03384	Cisco Wave 2 APs silver UP 00 to DSCP upstream mapping not capped by bronze profile.
CSCvu24770	Various models of Android 10 devices fail to associate.
CSCvu25264	AIR-AP2802I-H-K9 WCPd crash: AP is failing to decode discovery response and reboot with flash core.

Resolved Caveats for Cisco IOS XE Gibraltar 16.12.3

Caveat ID	Description
CSCvc80047	Cisco AP reloads unexpectedly.
CSCvq72812	Cisco Wave 2 APs are dropping CAPWAP keepalive messages and are unable to join the controller.
CSCvr04258	Controller does not accept RADIUS attribute for VNID overwrite in Fabric mode.
CSCvr22918	Cisco Catalyst 9115AX and 9120AX APs: When non-broadcasted SSID is configured, beacons are corrupted.
CSCvr23173	Cisco Catalyst 9117 AP: Invalid radar detection on the non-serving channel.
CSCvr25112	Cisco Aironet 2700 and 3700 APs: In Flex Profile, Native VLAN 1 and VLAN mapping to 1 causes loss of network connectivity.
CSCvr33062	Samsung s10 client is not able to connect to the WPA2+WPA3-SAE+PSK+FT PSK+PSK-SHA2 mixed mode.
CSCvr34339	Cisco AP unexpectedly reloads with watchdog reset(wcpd).
CSCvr57415	Cisco Catalyst 9130 AP does not send disassociate message when CAPWAP resets.
CSCvr57817	Cisco Aironet 3702 AP is adding C0 to the association ID in assoc-resp when configured as FlexConnect central association.
CSCvr60395	Wncd unexpected reboot.
CSCvr73095	After AES encryption is enabled, entering plain aaa dynamic-author keys corrupts key.

Caveat ID	Description
CSCvr85760	Cisco AP is sending invalid association ID.
CSCvr92606	When attempting to broadcast the same exact SSID on the controller and on the Cisco Catalyst 9120-AX AP, the controller sees CPUHOG alerts for EPM and crashes.
CSCvr95253	Cisco Catalyst 9120 AP PSM TX-STUCK detection fired continuously in a loop.
CSCvs00138	Cisco Aironet 2802 AP: Association ID allocation failed for slot 0.
CSCvs02781	Controller is not sending redirect URL for webauth clients.
CSCvs17014	Cisco Aironet 1832 AP has zero Rx neighbors.
CSCvs31212	Cisco Aironet 3800 APs: MIC errors are observed for CCKM roams in FlexConnect local switch mode.
CSCvs32307	Cisco Wave 2 APs with FT standalone mode: Roam traffic is blackholed when PMK is present.
CSCvs33919	In Cisco Catalyst 9130 AP tri-radio slot 1 and 2, the maximum client count is limited to 255.
CSCvs36177	Cisco Wave 2 APs are sending the EAP identity request with incorrect BSSID.
CSCvs45014	Wireless client is unable to get ipv6 address when associated to Cisco Catalyst 9130ax AP.
CSCvs48680	HA: When switchover occurs, first 11r client roam fails to authenticate.
CSCvs52625	btman process is stuck at 100% while running **show tech** command.
CSCvs55102	Wcnd reboots unexpectedly after association failure.
CSCvs63593	Cisco Aironet 3802-P-k9 AP Transmit Power Adjustment with AIR-ANT2513P4M-N (13dBi) W52 Japan Outdoor.
CSCvs66107	Cisco Catalyst 9115AX AP: Rogue containment is not working if AP is in monitor mode.
CSCvs66411	Flex AP is sending RADIUS packets to AAA server when in local-auth mode.
CSCvs70091	-Q domain APs in Japan advertise J4 as the country in beacon instead of JP.

Caveat ID	Description
CSCvs71784	Cisco Catalyst 9800-40 Wireless Controller crashes on receiving invalid username with 246 characters.
CSCvs75832	Cisco Catalyst 9115 APs: Rogue containment in monitor mode is not working as expected.
CSCvs77251	Controller is unable to send proper sequence number and burst rate upstream breaking RFID.
CSCvs77468	AP must send status 53 when PMKID is not found during FT-AUTH processing.
CSCvs89951	Controller running Cisco IOS XE 16.12.2s is not showing any clients in CMX when filtered by associated clients.

Resolved Caveats for Cisco IOS XE Gibraltar 16.12.2s

Caveat ID	Description
CSCvp65565	Add clear install state command.
CSCvp75687	The packet callbacks are not cleared for the transmission scan frames.
CSCvp82631	The CleanAir sensor is down.
CSCvq03763	Cisco Aironet 2800, 3800, and 4800 series APs are doing Channel Availability Check (CAC) after radio reset in the Dynamic Frequency Selection (DFS) channel.
CSCvq07516	Cisco Catalyst 9120 AP crashes unexpectedly.
CSCvq09845	Cisco Catalyst 9115 and 9120 APs: Duplex mismatch is discovered on the AP connected port.
CSCvq20611	AP loses data Datagram Transport Layer Security (DTLS) tunnel when port randomization is enabled on the firewall and a client connects to the AP.
CSCvq24468	Wireless clients are unable to connect to SSIDs on the Cisco Catalyst 9117 AP after 24 hours.
CSCvq26161	POE power request from Cisco Aironet 1815m and 1542 APs are different from the AP data sheet.
CSCvq33391	AWS NAT: Controller is not sending public IP in the discovery response.

Caveat ID	Description
CSCvq39356	RLAN AP disjoins when the RLAN client joins and further client join is not happening.
CSCvq39713	Controller console logs are flooded with "%CPPOSLIB-3-ERROR_NOTIFY" tracebacks.
CSCvq41013	Cisco DNA Centre: Web authentication client traffic stops working after an intra-controller roaming.
CSCvq46525	Memory leak is observed in the Cisco Catalyst 9800-L Series Wireless Controller.
CSCvq46906	Cisco Catalyst 9120 AP crashes due to kernel panic.
CSCvq50344	MESH adjacency SNR reports 252dB.
CSCvq64296	Controller and AP provisioning fails while using the **do ap name <ap-name> location** command.
CSCvq65396	Cisco Catalyst 9800 Series Wireless Controller for Cloud is unable to save the configuration.
CSCvq66084	Wncd crash is observed after switchover in Cisco Catalyst 9800-L Series Wireless Controller.
CSCvq72804	A Wave 2 AP that is behind a NAT device doing NAT and PAT drops the controller when Data DTLS is enabled.
CSCvq85769	APs are experiencing radio 0 FW crash.
CSCvq86040	Switch with an embedded wireless controller reloads unexpectedly.
CSCvq88051	Cisco Catalyst 9130 AP reloads unexpectedly in a loop.
CSCvq99561	Controller is sending 5 GHz band as 2.4 GHz band for an associated client to Cisco CMX.
CSCvr11358	Wncd process is crashing on the newly active controller immediately after the switchover.
CSCvr12823	APs are not joining after configuring LAG.
CSCvr26984	GC is stuck because of NMSPD spectrum and is not moving to read the cursor.
CSCvr27555	5 GHz radios are going down when the country code is changed to MK.
CSCvr35371	Cisco Catalyst 9800-L Series Wireless Controller in HA mode is crashing continuously.

Caveat ID	Description
CSCvr40230	Client is showing a health score of four even after getting deleted from the controller.
CSCvr43898	Anyconnect 4.7 clients are sending IPv6 RS with FE00 address causing clients to disconnect due to IP theft.
CSCvr48265	Cisco Catalyst 9120 AP: Coverage hole problem is causing client connectivity issues.
CSCvr65834	Cisco Catalyst 9120 AP: Configuration to change beamforming is not working from the controller.
CSCvr66201	System reloads unexpectedly and loses partial configuration due to wncd and cpp-mcplo failure.
CSCvr75431	Clients are getting disconnected due to the stale association IDs on the Cisco Catalyst 9130ax AP.
CSCvr96514	Cisco Catalyst 9130 AP reloads unexpectedly on softlockup.
CSCvk79864	The **show ap config slots** command output is showing Modulation and Coding Scheme (MCS) rates as disabled on the AP.
CSCvk79888	Export log feature is not working, if the directory name does not have a terminating forward slash.
CSCvk79907	The **show tech wireless** command displays the list of clients connected to the controller.
CSCvn54898	User is unable to edit default policy tag.
CSCvp30786	The **show client summary detail** command output requires 802.11k/v/w/u/WMM details.
CSCvq19985	Add **show wireless client summary detail {ipv4 | ipv6}** command.
CSCvq27229	RA collected for a specific client is showing logs for other clients as well.
CSCvq31854	The method field is empty for few clients in the **show wireless client summary** command output.
CSCvq53396	During roaming, the APs are sending deauthentication message after sending reassociation request, when FT is set to enable or adaptive.
CSCvq63188	OFDM parameters are shown as *automatic* even after manual allocation.

Caveat ID	Description
CSCvq76529	Controller web UI is not allowing to configure the Antenna Gain field.
CSCvq78055	The **show wireless country channels** command output is not showing channels greater than or equal to 100.
CSCvq80295	Add last SSID to the parent structure st_rogue_data.
CSCvq81875	Add MAC address theft as a reason for client exclusion.
CSCvr06136	Flexconnect WLAN-VLAN tag is not working for VLAN names created without numbers.
CSCvr16670	The **show ap name <ap-name> config slot** command output displays inconsistent MCS data.
CSCvr25656	CWDB sync is missing when tx power is changed by Tx Power Control (TPC).

Resolved Caveats for Cisco IOS XE Gibraltar 16.12.1t

Caveat ID	Description
CSCvr62980	Remove support for Cisco Catalyst 9120 and 9130 series APs.

Note All the caveats listed in **Resolved Caveats for Cisco IOS XE Gibraltar 16.12.1s** section are applicable for Cisco IOS XE Gibraltar 16.12.1t release as well, in addition to the caveat given above.

Resolved Caveats for Cisco IOS XE Gibraltar 16.12.1s

Caveat ID	Description
CSCvp99818	Cisco DNA Center is showing four-way key timeout text descriptions for mic error and RC mismatch.
CSCvq31842	Radio utilization is not reported accurately for the wireless clients.
CSCvq38420	STA Denied Rate Events are not incrementing on the AP for anomaly rate-mismatch.
CSCvq41631	Pubd process reloads unexpectedly after connecting to Cisco Prime Infrastructure.
CSCvq45977	AP drops data packets due to stale AP entries.

Caveat ID	Description
CSCvq53396	During roaming, the APs are sending deauthentication message after sending reassociation request, when FT is set to enable or adaptive.
CSCvq63168	Cisco Trustpoint is not configured via Day0 configuration in an instance that is launched in GCP.
CSCvq65131	Regulatory domain channels mismatch for the Japan domain (J4).
CSCvq65530	Cisco DNA Center: AP reachability status is not getting updated.
CSCvq77641	Controller is not sending the correct reason code to Cisco DNA Center when triggering an invalid RSNIE during the association request.
CSCvq80728	APs are continuously flapping after the second switch over.
CSCvq84971	Inter-wncd fast-roam re-association response is not going out.
CSCvq95642	Multicast IPv6 packets that are received from the clients are causing a loop, which results in a major uplink bandwidth utilization issue.
CSCvr08701	APs are unable to form a tunnel due to Interprocessor Communication (IPC) channel back pressure.

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 at:

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

Cisco Wireless Controller

For more information about the Cisco Wireless Controllers, 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 particular controller:

- 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 the following link:

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

- Product Approval Status:

  https://prdapp.cloudapps.cisco.com/cse/prdapp/jsp/externalsearch.do?action=externalsearch&page=EXTERNAL_SEARCH

- Wireless LAN Compliance Lookup:

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