Release Notes for Cisco Catalyst 9800 Series Wireless Controller, Cisco IOS XE 17.14.x

First Published: 2024-04-05

Release Notes for Cisco Catalyst 9800 Series Wireless Controller, Cisco IOS XE 17.14.x

Introduction to Cisco Catalyst 9800 Series Wireless Controllers

The Cisco Catalyst 9800 Series Wireless Controllers comprise next-generation wireless controllers (referred to as *controller* in this document) built for intent-based networking. The 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 controllers are enterprise ready to power your business-critical operations and transform end-customer experiences:

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

The Catalyst 9800 Series controllers are available in multiple form factors to cater to your deployment options:

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

Note All the Cisco IOS-XE programmability-related topics on the Cisco Catalyst 9800 controllers 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 17.14.1

Table 1: New and Modified Software Features

Feature Name	Description and Documentation Link
CAPWAP Message Aggregation	This feature aggregates the CAPWAP control messages of the same type waiting in the queue to be transmitted to the AP. The following command is introduced: • **capwap aggregation** For more information, see AP Configuration.
Cisco Catalyst 9800 Controller Automated Frequency Coordination (AFC) Support for Cisco Catalyst IW9167E Heavy Duty Access Point and Cisco Catalyst IW9167I Heavy Duty Access Point	Cisco Catalyst 9800 Series Wireless Controller serves as an AFC proxy to send the AP information to the AFC system.
Cisco Catalyst CW9800H1 and CW9800H2 Wireless Controllers	The Cisco Catalyst CW9800H1 and CW9800H2 Wireless Controllers are the next-generation Cisco Catalyst CW9800 Series Wireless LAN Controllers that boast up to a 36% increase in performance and consume up to 40% less power compared to their predecessors. Additionally, both the CW9800H1 and CW9800H2 models are built with a space-saving single RU design and support up to 6000 APs and 64,000 clients with 100 Gbps of maximum throughput. They also offer a choice of uplinks with either 4 x 25 Gbps (CW9800H1) or 2 x 40 Gbps (CW9800H2) configurations to meet the high throughput demands of next-generation wireless requirements. For more information, see *Cisco Catalyst CW9800H1 and CW9800H2 Wireless Controllers Hardware Installation Guide*

Feature Name	Description and Documentation Link
Cisco Catalyst CW9800M Wireless Controller	The Cisco Catalyst CW9800M Wireless Controller is the next generation Cisco Catalyst CW9800 Series Wireless LAN Controller built to deliver a 53% performance improvement while consuming 18% less power when compared to the previous generation models. Additionally, the Cisco Catalyst CW9800M Wireless Controller supports 3000 APs and 32000 clients to ensure better performance and scale for business-critical networks and provides up to 40 Gbps of forwarding throughput for both normal packet and encrypted packets while remaining a single RU designed to save you space and provide greater flexibility in your datacenters. For more information, see *Cisco Catalyst CW9800M Wireless Controller Hardware Installation Guide*
Enhancing AP using BLE support on Cisco Catalyst IW9167E and IW9167I Heavy Duty Series Access Points	You can configure an AP as Bluetooth Low Energy (BLE) gateway. Based on the type of AP, there are two types of BLE gateways: 1. **Base BLE Gateway**: This AP type allows you to choose between Transmit mode and Scan mode. 2. **Advanced BLE Gateway**: This AP type comes with an installed IOx application. You use this application to set up floor beacons on the Cisco-partnered Device Manager website. For Catalyst IW9167E AP, antenna 4 of 2.4 GHz and antenna 1 of 5 GHz shares the antenna with BLE radio. BLE antenna sharing restrictions: • When you enable BLE, the 2.4 GHz radio does not support the 4x4 antenna. • When you enable a 5 GHz single-band antenna in slot 4, the BLE radio is disabled. **Note** For Cisco Catalyst IW9167I AP, the BLE gateway enabling alignment is the same as that of Cisco Catalyst 9166 Series AP.
FlexConnect Central Web Authentication Central Switching L3 VLAN Override Support	From this release, L3 VLAN override in FlexConnect central web authentication (CWA) is supported for both local and guest clients.
gNMI: SubscribeResponse with sync_response	The sync_response is a boolean field that is part of the SubscribeResponse response message. The sync_response message is sent after the first update message. For more information, see *Programmability Configuration Guide*.

Feature Name	Description and Documentation Link
gNMI Telemetry Support: Stream Subscriptions with On-Change Mode	This feature introduces gNMI telemetry support on-change subscriptions on the same set of models as other telemetry protocols For more information, see *Programmability Configuration Guide*.
IOx Application support on Cisco Catalyst IW9167E and IW9167I Heavy Duty Series Access Points	The Cisco Internet of Experience (IOx) application enables and allows access points to run third-party applications in the CAPWAP mode. To enable IOx, you need an extra memory space up to 50 MB for DRAM and another 100 MB for each IOx application. You can install up to two applications on the AP. The memory size requirement is based on the following components: • Actual size of the application • Run-time data storage • Bundled IOx infrastructure into access point software (once IOx is bundled into the build, the file size increases by 9 MB) IOx application ensures a secure connection with IoT devices at the edge and integrates reliably with IoT sensors.
Israel Domain Changes	From this release, for indoor Wi-Fi 6E APs, Israel and Turkey are moved to the -E regulatory domain and support 6-GHz radio bands. For outdoor APs, Israel is moved from -ROW to the new -I regulatory domain.
Kernel Minidump and Trustzone Upgrade	From this release, the Kernel Minidump and Trustzone Upgrade feature offers a more effective method for diagnosing kernel issues. The following command is introduced: • **core-dump kernel type** For more information, see Kernel Minidump and Trustzone Upgrade.
New Countries for 6-GHz Radio Support	From this release, Argentina, Chile, Colombia, Dominican Republic, Israel, Mexico, Singapore, South Africa, Thailand, and Turkey are added to the list of countries that support 6-GHz radio band.

Feature Name	Description and Documentation Link
Optimizing Dual 5G Mode in AP for Serial Backhaul Support on Cisco Catalyst IW9167E Heavy Duty Series Access Point	This feature enhances the performance and efficiency of a wireless network by optimizing the use of dual 5G radios in an AP for backhaul. In this feature, AP operates in the dual 5G mode using two 5G radios. You can enable backhaul on two 5G radios. The two backhaul radios provide uplink and downlink access to maximize throughput over multiple mesh hops. **Note** • For the dual 5G serial backhaul, ensure that slot 2 operates in 5G mode when enabling mesh dual 5G serial backhaul. • When slot 2 operates in 6 GHz, AP is unable to be configured in mesh mode. The backhaul root AP (RAP) does not support multiple downlink channels. When you configure mesh mode in AP, block the 6G band for slot 2 as it does not support both backhaul and access. By default, the following actions are performed without any configuration change except enabling dual-5G: • Mesh access point (MAP) seeks for a primary device on all enabled radios. • MAP performs uplink and downlink on the same slot while other slots are in access mode.
Power Profile Support with 30-watts Power over Ethernet (PoE) on Cisco Catalyst IW9167I Heavy Duty Access Point	The AP power policy allows you to define the power budget utilization available for an AP, wherein, you can define a set of policies for different interfaces on an AP. From this release, Cisco Catalyst IW9167I Heavy Duty AP supports Power policy AP feature especially when AP works with 802.3at power. PoE+ is a new interface introduced in Cisco Catalyst IW9167I Heavy Duty AP, in addition to the Ethernet and LAN interfaces. AP is now powered by 30W through either 802.3at or 802.3bt standards, offering versatility in deployment and ensuring high-performance wireless connectivity. To enable flexible power policy, a power profile must be configured on the controller, extending the AP Join profile. The power profile supports local and FlexConnect modes but is unsupported in mesh mode.
Proto Encoding: Enhancements for Emulated On-Change Subscription	For more information, see *Programmability Configuration Guide*.

Feature Name	Description and Documentation Link
Quality of Service (QoS) Classification and Marking Support on WGB	WGB allows you to classify different packets from two wired ports and mark them to a different access control driver queue based on your configuration. In addition to TCP or UDP, WGB also supports configuring the ACL rules and QoS policies based on Ethernet type, transport layer port numbers or port range, and DSCP. During classification, the device performs a lookup and assigns a QoS label to the packet. The QoS label indicates all QoS actions to perform on the packet and identifies the queue from which the packet is sent. The feature is supported on the following APs: • Cisco Catalyst IW9167E Heavy Duty Access Point • Cisco Catalyst IW9165E Rugged Access Point For more information, see the Support for QoS ACL Classification and Marking sections of the *Cisco Catalyst IW9165E Rugged Access Point and Wireless Client Configuration Guide* and Cisco Catalyst IW9167E Heavy Duty Access Point Configuration Guide.
Radio Resource Management (RRM) Dynamic Channel Assignment (DCA) Support on Mesh Backhaul	Until the Cisco IOS XE 17.13.1 release, the RRM DCA optimized the root AP (RAP) backhaul radio channel of a mesh subtree by considering the noise, interference, load, and the RF parameter measurements only from the RAP. From this release, the RRM DCA on Mesh Backhaul feature enables DCA to make better channel assignments for a mesh subtree, by having continuous measurements and inputs from the whole mesh tree required to run DCA. The following command is introduced: • **show wireless mesh rrm dca changed** For more information, see Mesh Access Points.
SDA IPv6 Underlay Support	From this release, this feature provides a wireless SDA IPv6 underlay support to enable IPv6-based communications in a fabric domain.
Show Technical Diagnostics for Appliances	From this release, the **show tech-support diagnostic** command is supported. This command is introduced to display the diagnostic technical support information of a system. For more information about the command, see *Cisco Catalyst 9800 Sesries Wireless Controllers Command Reference*.

Feature Name	Description and Documentation Link

SNMP Support for WGB on Cisco Catalyst IW9165E Rugged Access Point and Wireless Client and Cisco Catalyst IW9167E Heavy Duty Access Point	The Work Group Bridge (WGB) now supports Simple Network Management Protocol (SNMP) configuration. This provides network administrators with direct access to a comprehensive range of states and counters from the WGB.
	
	With the SNMP interface, customers gain the ability to effortlessly monitor the health and performance of their WGBs deployed in the field. This enhancement ensures greater visibility and control over network infrastructure, facilitating proactive maintenance and optimizing operational efficiency.
	
	The supported SNMP configuration versions and levels supported are as follows:
	• Community-based SNMP Version 2 (SNMPv2c)
	• SNMP Version 3 allows you to combine users into groups of different authorization and access privileges. You can associate a group to the following security levels:
	  • AuthNoPriv: With a username and password for authentication
	  • AuthPriv: With a username and password for authentication and encryption
	
	For more information, see the Configuring and Validating SNMP with WGB section of the *Cisco Catalyst IW9165E Rugged Access Point and Wireless Client Configuration Guide* and Cisco Catalyst IW9167E Heavy Duty Access Point Configuration Guide

Support for Built-In GPS as Proxy GPS for other 6E APs on Cisco Catalyst IW9167E Heavy Duty Access Point and Cisco Catalyst IW9167I Heavy Duty Access Point	These APs function as anchor APs with GPS functionality and help in providing geolocation data for other APs that do not have direct GPS signals, in geo-location derivation within the network. Additionally, in the absence of GPS coverage, these APs can utilize other 6E APs with GPS to derive their location. APs report the geolocation data to the controller via Global Navigation Satellite System (GNSS), ensuring that the network management system has accurate location details for each AP. Cisco Catalyst IW9165E Rugged Access Point and Cisco Catalyst IW9165D Heavy Duty Access Point also support this feature.

Feature Name	Description and Documentation Link
Support for CAPWAP Mode on Cisco Catalyst IW9165E Rugged Access Point and Cisco Catalyst IW9165D Heavy Duty Access Point	This feature enables APs to use CAPWAP to communicate with the controller and other APs on the network. APs are now upgraded to support CAPWAP images, enabling mode conversion to CAPWAP. Supported Platforms and Modes: • Cisco Catalyst IW9165E Rugged Access Point: Supports CAPWAP, URWB, and WGB. • Cisco Catalyst IW9165D Heavy Duty Access Point: Supports CAPWAP and URWB. The following command is introduced: • **configure boot mode capwap** For more information, see *Cisco Catalyst IW9165E Rugged Access Point and Wireless Client Configuration Guide* and *Cisco Catalyst IW9165D Heavy Duty Access Point Configuration Guide*.
Support for Cisco CleanAir Pro Technology on Cisco Catalyst IW9167E Heavy Duty Access Point	The Cisco CleanAir Pro technology is designed to perform spectral scanning and interferer identification over Wi-Fi frequencies using the dedicated 2X2 scanning radio to get better outcomes for Radio Resource Management (RRM) features. The following CleanAir Pro functions are supported: • Provide reports on the different categories of non-Wi-Fi interference, for the 2.4-GHz, 5-GHz, and 6-GHz bands. • Reports the type of interferer, the severity of the interference, and the impacted channels to the controller, through Interference Device Reports (IDRs). • Establishes Air Quality for all interfaces on the AP.
Support for CW-ANT-D1-NS-00 Antenna on Cisco Catalyst 9163E Access Point	From this release CW-ANT-D1-NS-00 Antenna is supported on Cisco Catalyst 9163E Access Point. For more information, see *Cisco Catalyst 9163E Series Access Points Data sheet*.
Enable Secure Data Wipe Capabilities for Legacy Products	From this release, the **factory- reset all secure** command erases all user data and metadata from bootflash. For more information, see the Performing Secure Erase section of your respective controller installation guides. *Cisco Catalyst 9800-80 Wireless Controller Hardware Installation Guide* *Cisco Catalyst 9800-40 Wireless Controller Hardware Installation Guide*

Feature Name	Description and Documentation Link
Support for Scanning Radio on Cisco Catalyst IW9167E Heavy Duty Access Point	From this release, you can set up a dedicated scanning radio in your enterprise wireless network to scan multiple variables, such as RF interference, user density, AP failure, noise, rogue APs, and coverage. The following features are supported by the scanning radio: • Cisco Advanced Wireless Intrusion Prevention System (aWIPS) • Rogue • Radio Resource Management (RRM) • Fast Locate • Cisco Intelligent Capture (iCAP) • Spectrum Analysis • CleanAir Pro
Tier B/C/D Country Support for Cisco Catalyst 9166D1 Access Points	From this release, Australia, Austria, Belgium, Bulgaria, Canada, China, Croatia, Czech Republic, Cyprus, Denmark, Estonia, Finland, France, Germany, Gibraltar, Greece, Hungary, Iceland, Ireland, Italy, Japan, Korea, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Mexico, Monaco, Netherlands, New Zealand, Norway, Poland, Portugal, Romania, Slovak Republic, Slovenia, Spain, Sweden, Switzerland, United Kingdom, United States of America are added to the list of countries that support 2.4-GHz, 5-GHz, and 6-GHz radio bands.
Wi-Fi AP Automated Frequency Coordination (AFC) support for 6G Standard Power Mode on Cisco Catalyst IW9165E Rugged Access Point and Wireless Client, Cisco Catalyst IW9165D Heavy Duty Access Point, Cisco Catalyst IW9167E Heavy Duty Access Point, and Cisco Catalyst IW9167E Heavy Duty Access Point	APs support the AFC 6G in Standard Power mode. AFC system helps to allocate the channels and power levels to APs to operate in standard power mode in the 6-GHz frequency spectrum. The response is then sent back to the controller and assigns a standard power channel to the AP based on the allowed channel list returned by the AFC system. The APs support standard power mode only in the -B domain and are allowed to operate in the UNII-5 (5.925-6.425 GHz) and UNII-7 (6.525-7.125 GHz). With AFC 6G, APs can switch between 5G and 6G bands. The 6G band is only available in standard power mode with Self Identifiable Antenna. The following command is introduced to display the AFC request and response data: • **show rrm afc**
YANG RPC Support for **clear aaa counters** and **clear radius statistics** Commands.	From this release, YANG RPC is supported for the **clear aaa counters** and **clear radius statistics** commands so that they can clear all counters, or specified RADIUS server ID counters to the device.

Feature Name	Description and Documentation Link
YANG Support for Mutiple Next-Hops	From this release, a new container is added under the next-hop-options choice node to retrieve all next-hops for a given route or prefix. Also, an uptime leaf node is added to provide the timestamp for each next hop.

MIBs

The following MIBs are newly added or modified:

- CISCO-LWAPP-RF-MIB.my
- CISCO-LWAPP-REAP-MIB.my
- CISCO-LWAPP-TAGS-MIB.my
- CISCO-LWAPP-DOT11-MIB.my
- CISCO-LWAPP-WLAN-SECURITY-MIB.my
- CISCO-LWAPP-TC-MIB.my
- CISCO-LWAPP-AP-MIB.my
- CISCO-LWAPP-AP-MIB.my
- AIRESPACE-WIRELESS-MIB.my
- CISCO-LWAPP-QOS-MIB.my

Product Analytics

This feature allows for the collection of non-personal usage device systems information for Cisco products, which helps in continuous product improvements. This feature is supported on the Cisco Catalyst 9800 Series Wireless Controllers (9800-80, 9800-40, 9800-L, and 9800-CL). You can use the the **pae** command to enable or disable this feature.

The following commands are introduced as part of this feature:

- **pae**
- **show product-analytics kpi**
- **show product-analytics report**
- **show product-analytics stats**

Note Turning off Smart Licensing Device Systems Information does not impact other Systems Information collection including from Cisco Catalyst Center or vManage.

Important: Cisco is constantly striving to advance our products and services. Knowing how you use our products is key to accomplishing this goal. To that end, Cisco will collect device and licensing Systems Information through Cisco Smart Software Manager (CSSM) for product and customer experience improvement,

analytics, and adoption. Cisco processes your data in accordance with the General Terms and Conditions, the Cisco Privacy Statement and any other applicable agreement with Cisco. To modify your organization's preferences for device and licensing systems information, use the **pae** command. For more information, see *Cisco Catalyst 9800 Series Wireless Controller Command Reference*.

For additional information on this feature, see *Wireless Product Analytics FAQ*.

Behavior Change

- The Zero Wait Dynamic Frequency Selection feature is disabled on Cisco Catalyst 9136 Series APs when dual 5-GHz is enabled.
- The value for the **Disruptive Ranging Timer** in the Auto Location feature has been changed from 10 minutes to 15 minutes.
- The **ap tri-radio** command is applicable for Cisco Catalyst 9130, 9136, and 9124 APs.
- From this release, if the power requirement is similar or more than the maximum power in Low Power Mode (LPM), ensure that the power mode switches to Standard Power Mode.
- If you have configured CISCO_IDEVID_SUDI trustpoint in your configuration, you will need to replace it with CISCO_IDEVID_CMCA3_SUDI to avoid client connection and AP join issues. The reason for this change being the CISCO_IDEVID_SUDI changed from SW-SUDI certificate in previous releases to HW-SUDI certificate. The processing of HW-SUDI certificate is much slower than the SW-SUDI. Here, CISCO_IDEVID_CMCA3_SUDI is the new SW-SUDI certificate.

Interactive Help

The Cisco Catalyst 9800 Series Wireless Controller GUI features an interactive help that walks you through the GUI and guides you through complex configurations.

You can start the interactive help in the following ways:

- By hovering your cursor over the blue flap at the right-hand corner of a window in the GUI and clicking **Interactive Help**.
- By clicking **Walk-me Thru** in the left pane of a window in the GUI.
- By clicking **Show me How** displayed in the GUI. Clicking **Show me How** triggers a specific interactive help that is relevant to the context you are in.

  For instance, **Show me How** in **Configure** > **AAA** walks you through the various steps for configuring a RADIUS server. Choose **Configuration**> **Wireless Setup** > **Advanced** and click **Show me How** to trigger the interactive help that walks you through the steps relating to various kinds of authentication.

The following features have an associated interactive help:

- Configuring AAA
- Configuring FlexConnect Authentication
- Configuring 802.1x Authentication
- Configuring Local Web Authentication

- Configuring OpenRoaming
- Configuring Mesh APs

Note If the WalkMe launcher is unavailable on Safari, modify the settings as follows:

1. Choose **Preferences** > **Privacy**.
2. In the **Website tracking** section, uncheck the **Prevent cross-site tracking** check box to disable this action.
3. In the **Cookies and website data** section, uncheck the **Block all cookies** check box to disable this action.

Supported Hardware

The following table lists the supported virtual and hardware platforms. (See Table 4: Supported PIDs and Ports for the list of supported modules.)

Table 2: 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. The controller occupies a 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. The controller occupies a 1-rack unit space and provides four 1-GE or 10-GE uplink ports.
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 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 VMware ESXi, Kernel-based Virtual Machine [KVM], Microsoft Hyper-V, and Cisco Enterprise NFV Infrastructure Software [NFVIS] on Enterprise Network Compute System [ENCS] hypervisors), or in the public cloud as Infrastructure as a Service (IaaS) in Amazon Web Services (AWS), Google Cloud Platform (GCP) marketplace, and Microsoft Azure.

Platform	Description
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 Software Defined-Access (SDA), which is a highly secure solution for small campuses and distributed branches.
Cisco Catalyst CW9800M Wireless Controller	The Cisco Catalyst CW9800M Wireless Controller is the next generation Cisco Catalyst CW9800 Series Wireless LAN Controller built to deliver a 53% performance improvement while consuming 18% less power when compared to the previous generation models. Additionally, the Cisco Catalyst CW9800M Wireless Controller supports 3000 APs and 32000 clients to ensure better performance and scale for business-critical networks and provides up to 40 Gbps of forwarding throughput for both normal packet and encrypted packets while remaining a single RU designed to save you space and provide greater flexibility in your datacenters.
Cisco Catalyst CW9800H1 and CW9800H2 Wireless Controllers	The Cisco Catalyst CW9800H1 and CW9800H2 Wireless Controllers are the next-generation Cisco Catalyst CW9800 Series Wireless LAN Controllers that boast up to a 36% increase in performance and consume up to 40% less power compared to their predecessors. Additionally, the CW9800H1 and CW9800H2 models are built with a space-saving single RU design and support up to 6000 APs and 64,000 clients with 100 Gbps of maximum throughput. They also offer a choice of uplinks with either 4 x 25 Gbps (CW9800H1) or 2 x 40 Gbps (CW9800H2) configurations to meet high throughput demands of next-generation wireless requirements.

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

Table 3: Supported Host Environments for Public and Private Cloud

Host Environment	Software Version
VMware ESXi	• VMware ESXi vSphere 6.0, 6.5, 6.7, and 7.0 • VMware ESXi vCenter 6.0, 6.5, 6.7, and 7.0
KVM	• Linux KVM-based on Red Hat Enterprise Linux 7.6, 7.8, and 8.2 • Ubuntu 16.04.5 LTS, Ubuntu 18.04.5 LTS, Ubuntu 20.04.5 LTS
AWS	AWS EC2 platform
NFVIS	ENCS 3.8.1 and 3.9.1

Host Environment	Software Version
GCP	GCP marketplace
Microsoft Hyper-V	Windows 2019 Server and Windows Server 2016 (Version 1607) with Hyper-V Manager (Version 10.0.14393)
Microsoft Azure	Microsoft Azure

The following table lists the supported Cisco Catalyst 9800 Series Wireless Controller hardware models.

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. Running 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 a port. Only Cisco-supported SFPs (GLC-LH-SMD and GLC-SX-MMD) should be used on the route processor (RP) ports of C9800-80-K9 and C9800-40-K9.

Table 4: 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.
C9800-40-K9	Four 1/10-Gigabit Ethernet SFP or SFP+ ports and two power supply slots.
C9800-L-C-K9	• 4x2.5/1-Gigabit ports • 2x10/5/2.5/1-Gigabit ports
C9800-L-F-K9	• 4x2.5/1-Gigabit ports • 2x10/1-Gigabit ports
CW9800H1	• 8x1 GE/10 GE SFP ports • 4x25 GE SFP interfaces
CW9800H2	• 8x1 GE/10 GE SFP Ports • 2X 40 GE QSFP interfaces
CW9800M	• Four built-in 1 GE /10 GE SFP ports • Two built-in 25 GE SFP ports

The following table lists the supported SFP models.

Table 5: Supported SFPs

SFP Name	C9800-80-K9	C9800-40-K9	C9800-L-F-K9	CW9800H1	CW9800H2	CW9800M
COLORCHIP-C040-Q020-CWDM4-03B	Supported	—	—	—	—	—
DWDM-SFP10G-30.33	Supported	Supported	—	—	—	—
DWDM-SFP10G-61.41	Supported	Supported	—	—	—	—
FINISAR-LR – FTLX1471D3BCL [1]	Supported	Supported	Supported	—	—	—
FINISAR-SR – FTLX8574D3BCL	Supported	Supported	Supported	—	—	—
GLC-BX-D	Supported	Supported	Supported	Supported	Supported	Supported
GLC-BX-U	Supported	Supported	Supported	Supported	Supported	Supported
GLC-EX-SMD	Supported	Supported	—	Supported	Supported	Supported
GLC-LH-SMD	Supported	Supported	—	Supported	Supported	Supported
GLC-SX-MMD	Supported	Supported	Supported	Supported	Supported	Supported
GLC-T	Supported	—	—	—	—	—
GLC-TE	Supported	Supported	Supported	Supported	Supported	Supported
GLC-ZX-SMD	Supported	Supported	Supported	Supported	Supported	Supported
QSFP-100G-LR4-S	Supported	—	—	—	—	—
QSFP-100G-SR4-S	Supported	—	—	—	—	—
QSFP-40G-BD-RX	Supported	—	—	—	—	—
QSFP-40G-ER4	Supported	—	—	—	Supported	—
QSFP-40G-LR4	Supported	—	—	—	Supported	—
QSFP-40G-LR4-S	Supported	—	—	—	Supported	—
QSFP-40G-CSR4	—	—	—	—	Supported	—
QSFP-40G-SR4	Supported	—	—	—	Supported	—
QSFP-40G-SR4-S	Supported	—	—	—	Supported	—
QSFP-40GE-LR4	Supported	—	—	—	—	—
QSFP-H40G-ACU10M	—	—	—	—	Supported	—

SFP Name	C9800-80-K9	C9800-40-K9	C9800-L-F-K9	CW9800H1	CW9800H2	CW9800M
QSFP-H40G-CU1M	—	—	—	—	Supported	—
QSFP-H40G-CU2M	—	—	—	—	Supported	—
QSFP-H40G-CU3M	—	—	—	—	Supported	—
QSFP-H40G-CU4M	—	—	—	—	Supported	—
QSFP-H40G-CU5M	—	—	—	—	Supported	—
QSFP-H40G-CUO-5M	—	—	—	—	Supported	—
QSFP-H40G-AOC1M	—	—	—	—	Supported	—
QSFP-H40G-AOC2M	—	—	—	—	Supported	—
QSFP-H40G-AOC3M	—	—	—	—	Supported	—
QSFP-H40G-AOC5M	—	—	—	—	Supported	—
QSFP-H40G-AOC7M	—	—	—	—	Supported	—
QSFP-H40G-AOC10M	—	—	—	—	Supported	—
QSFP-H40G-AOC15M	—	—	—	—	Supported	—
QSFP-H40G-AOC20M	—	—	—	—	Supported	—
QSFP-H40G-AOC25M	—	—	—	—	Supported	—
QSFP-H40G-AOC30M	—	—	—	—	Supported	—
SFP-10G-AOC10M	Supported	Supported	—	—	—	—
SFP-10G-AOC1M	Supported	Supported	—	Supported	Supported	Supported
SFP-10G-AOC2M	Supported	Supported	—	Supported	Supported	Supported
SFP-10G-AOC3M	Supported	Supported	—	Supported	Supported	Supported
SFP-10G-AOC5M	Supported	Supported	—	Supported	Supported	Supported
SFP-10G-AOC7M	Supported	Supported	—	Supported	Supported	Supported
SFP-10G-ER	Supported	Supported	—	Supported	Supported	Supported
SFP-10G-LR	Supported	Supported	Supported	Supported	Supported	Supported
SFP-10G-LR-S	Supported	Supported	Supported	—	—	—
SFP-10G-LR-X	Supported	Supported	Supported	Supported	Supported	Supported
SFP-10G-LRM	Supported	Supported	Supported	—	—	—
SFP-10G-SR	Supported	Supported	Supported	Supported	Supported	Supported

SFP Name	C9800-80-K9	C9800-40-K9	C9800-L-F-K9	CW9800H1	CW9800H2	CW9800M
SFP-10G-SR-S	Supported	Supported	Supported	Supported	Supported	Supported
SFP-10G-SR-I	—	—	—	Supported	Supported	Supported
SFP-10G-SR-X	Supported	Supported	Supported	—	—	—
SFP-10G-ZR	Supported	Supported	—	—	—	—
SFP-10G-ZR-I	—	—	—	Supported	Supported	Supported
SFP-10G-T-X	—	—	—	Supported	Supported	Supported
SFP-25G-SR-S	—	—	—	Supported	—	Supported
SFP-25G-ER-I	—	—	—	Supported	—	Supported
SFP-10/25G-LR-I	—	—	—	Supported	—	Supported
SFP-10/25G-LR-S	—	—	—	Supported	—	Supported
SFP-10/25G-CSR-S	—	—	—	Supported	—	Supported
SFP-10/25G-BXD-I	—	—	—	Supported	—	Supported
SFP-10/25G-BXU-I	—	—	—	Supported	—	Supported
SFP-10/25G-BXU-I	—	—	—	Supported	—	Supported
SFP-H25G-CU1M	—	—	—	Supported	—	Supported
SFP-H25G-CU5M	—	—	—	Supported	—	Supported
SFP-25G-AOC1M	—	—	—	Supported	—	Supported
SFP-25G-AOC2M	—	—	—	Supported	—	Supported
SFP-25G-AOC3M	—	—	—	Supported	—	Supported
SFP-25G-AOC5M	—	—	—	Supported	—	Supported
SFP-25G-AOC7M	—	—	—	Supported	—	Supported
SFP-25G-AOC10M	—	—	—	Supported	—	Supported
SFP-H10GB-ACU10M	Supported	Supported	Supported	Supported	Supported	Supported
SFP-H10GB-ACU7M	Supported	Supported	Supported	Supported	Supported	Supported
SFP-H10GB-ACU10M	—	—	—	Supported	Supported	Supported
SFP-H10GB- CU1.5M	Supported	Supported	Supported	—	—	—
SFP-H10GB-CU1M	Supported	Supported	Supported	Supported	Supported	Supported
SFP-H10GB-CU2.5M	Supported	Supported	Supported	—	—	—

SFP Name	C9800-80-K9	C9800-40-K9	C9800-L-F-K9	CW9800H1	CW9800H2	CW9800M
SFP-H10GB-CU2M	Supported	Supported	Supported	Supported	Supported	Supported
SFP-H10GB-CU3M	Supported	Supported	Supported	Supported	Supported	Supported
SFP-H10GB-CU5M	Supported	Supported	Supported	Supported	Supported	Supported
SFP-H10GB-CU1-5M	—	—	—	Supported	Supported	Supported
Finisar-LR (FTLX1471D3BCL)	—	—	Supported	Supported	Supported	Supported
Finisar-SR (FTLX8574D3BC)	—	—	—	Supported	Supported	Supported

[1] The FINISAR SFPs are not Cisco specific and some of the features, such as DOM, may not work properly.

Optics Modules

The 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

Network Protocols and Port Matrix

Table 6: Cisco Catalyst 9800 Series Wireless Controller - Network Protocols and Port Matrix

Source	Destination	Protocol	Destination Port	Source Port	Description
Any	Cisco Catalyst 9800 Series Wireless Controller	TCP	22	Any	SSH
Any	Cisco Catalyst 9800 Series Wireless Controller	TCP	23	Any	Telnet
Any	Cisco Catalyst 9800 Series Wireless Controller	TCP	80	Any	HTTP
Any	Cisco Catalyst 9800 Series Wireless Controller	TCP	443	Any	HTTPS

Source	Destination	Protocol	Destination Port	Source Port	Description
Any	Cisco Catalyst 9800 Series Wireless Controller	UDP	161	Any	SNMP Agent
Any	Any	UDP	5353	5353	mDNS
Any	Cisco Catalyst 9800 Series Wireless Controller	UDP	69	69	TFTP
Any	DNS Server	UDP	53	Any	DNS
Any	Cisco Catalyst 9800 Series Wireless Controller	TCP	830	Any	NetConf
Any	Cisco Catalyst 9800 Series Wireless Controller	TCP	443	Any	REST API
Any	WLC Protocol	UDP	1700	Any	Receive CoA packets.
AP	Cisco Catalyst 9800 Series Wireless Controller	UDP	5246	Any	CAPWAP Control
AP	Cisco Catalyst 9800 Series Wireless Controller	UDP	5247	Any	CAPWAP Data
AP	Cisco Catalyst 9800 Series Wireless Controller	UDP	5248	Any	CAPWAP MCAST
AP	Cisco Catalyst Center	UDP	57778	Any	Intelligent capture and RF telemetry
AP	AP	UDP	16670	Any	Client Policies (AP-AP)

Source	Destination	Protocol	Destination Port	Source Port	Description
Cisco Catalyst 9800 Series Wireless Controller	Cisco Catalyst 9800 Series Wireless Controller	UDP	16666	16666	Mobility Control
Cisco Catalyst 9800 Series Wireless Controller	SNMP	UDP	162	Any	SNMP Trap
Cisco Catalyst 9800 Series Wireless Controller	RADIUS	UDP	1812/1645	Any	RADIUS Auth
Cisco Catalyst 9800 Series Wireless Controller	RADIUS	UDP	1813/1646	Any	RADIUS ACCT
Cisco Catalyst 9800 Series Wireless Controller	TACACS+	TCP	49	Any	TACACS+
Cisco Catalyst 9800 Series Wireless Controller	Cisco Catalyst 9800 Series Wireless Controller	UDP	16667	16667	Mobility
Cisco Catalyst 9800 Series Wireless Controller	NTP Server	UDP	123	Any	NTP
Cisco Catalyst 9800 Series Wireless Controller	Syslog Server	UDP	514	Any	SYSLOG
Cisco Catalyst 9800 Series Wireless Controller	NetFlow Server	UDP	9996	Any	NetFlow
Cisco Catalyst 9800 Series Wireless Controller	Cisco Connected Mobile Experiences (CMX)	UDP	16113	Any	NMSP

Source	Destination	Protocol	Destination Port	Source Port	Description
Cisco Catalyst Center	Cisco Catalyst 9800 Series Wireless Controller	TCP	32222	Any	Device Discovery

Supported APs

The following Cisco APs are supported in this release.

Indoor Access Points

- Cisco Catalyst 9105AX (I/W) Access Points
- Cisco Catalyst 9115AX (I/E) Access Points
- Cisco Catalyst 9117AX (I) Access Points
- Cisco Catalyst 9120AX (I/E/P) Access Points
- Cisco Catalyst 9130AX (I/E) Access Points
- Cisco Catalyst 9136 (I) Access Points
- Cisco Catalyst 9162 (I) Series Access Points
- Cisco Catalyst 9164 (I) Series Access Points
- Cisco Catalyst 9166 (I/D1) Series Access Points
- Cisco Aironet 1815 (I/W/M/T), 1830 (I), 1840 (I), and 1852 (I/E) Access Points
- Cisco Aironet 1800i Access Point
- Cisco Aironet 2800 (I/E) Series Access Points
- Cisco Aironet 3800 (I/E/P) Series Access Points
- Cisco Aironet 4800 (I) Series Access Points

Outdoor Access Points

- Cisco Aironet 1540 (I/D) Series Access Points
- Cisco Aironet 1560 (I/D/E) Series Access Points
- Cisco Industrial Wireless 3700 Series Access Points
- Cisco Catalyst Industrial Wireless 6300 Heavy Duty Series Access Point
- Cisco 6300 Series Embedded Services Access Point
- Cisco Catalyst 9124AX (I/D/E) Access Points
- Cisco Catalyst 9163 (E) Series Access Points

- Cisco Catalyst Industrial Wireless 9167 (I/E) Heavy Duty Access Points
- Cisco Catalyst Industrial Wireless 9165 (E/I) Heavy Duty Access Points

Integrated Access Points

- Integrated Access Point on Cisco 1100 ISR (ISR-AP1100AC-x, ISR-AP1101AC-x, and ISR-AP1101AX-x)

Network Sensor

- Cisco Aironet 1800s Active Sensor

Pluggable Modules

- Wi-Fi 6 Pluggable Module for Industrial Routers

Supported Access Point Channels and Maximum Power Settings

Supported access point channels and maximum power settings on Cisco APs are compliant with the regulatory specifications of channels, maximum power levels, and antenna gains of every country in which the access points are sold. For more information about the supported access point transmission values in Cisco IOS XE software releases, see the *Detailed Channels and Maximum Power Settings* document at https://www.cisco.com/c/en/us/support/ios-nx-os-software/ios-xe-17/products-technical-reference-list.html.

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 7: Compatibility Information

Cisco Catalyst 9800 Series Wireless Controller Software	Cisco Identity Services Engine	Cisco Prime Infrastructure	Cisco AireOS-IRCM Interoperability	Cisco Catalyst Center	Cisco Spaces: Connector	Cisco CMX
IOS XE 17.14.1 with CW9800M and CW9800H1 and CW9800H2 Support [2]	3.2 3.1 3.0 2.7 * all with latest patches	3.10.4 Update 03	8.10.196.0 8.10.190.0 8.10.185.0 8.10.183.0 8.10.182.0 8.10.181.0 8.10.171.0 8.10.162.0 8.10.151.0 8.10.142.0 8.10.130.0 8.5.176.2 8.5.182.104	See Cisco Catalyst Center Compatibility Information	3, May 2023 2.3.4 2.3.3 2.3.2 2.3.1 See Cisco Spaces Compatibility Matrix	11.0 10.6.3

[2] Cisco Catalyst CW9800M Wireless Controller and Cisco Catalyst CW9800H1 and CW9800H2 Wireless Controllers are supported from Cisco IOS XE 17.14.1 release.

GUI System Requirements

The following subsections list the hardware and software required to access the Cisco Catalyst 9800 Controller GUI.

Table 8: Hardware Requirements

Processor Speed	DRAM	Number of Colors	Resolution	Font Size
233 MHz minimum[3]	512 MB[4]	256	1280 x 800 or higher	Small

[3] We recommend 1 GHz.
[4] 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: Version 40 or later (on Windows)
- Safari: Version 10 or later (on Mac)
- Mozilla Firefox: Version 60 or later (on Windows and Mac)

Note Firefox Version 63.x is not supported.

The controller GUI uses Virtual Terminal (VTY) lines for processing HTTP requests. At times, when multiple connections are open, the default number of VTY lines of 15 set by the device might get exhausted. Therefore, we recommend that you increase the number of VTY lines to 50.

To increase the VTY lines in a device, run the following commands in the following order:

1. **device#** configure terminal
2. **device(config)#** line vty 50

   A best practice is to configure the service tcp-keepalives to monitor the TCP connection to the device.
3. **device(config)#** service tcp-keepalives-in
4. **device(config)#** service tcp-keepalives-out

Before You Upgrade

Ensure that you familiarize yourself with the following points before proceeding with the upgrade:

Caution During controller upgrade or reboot, if route processor ports are connected to any Cisco switch, ensure that the route processor ports are not flapped (shut/no shut process). Otherwise, it may lead to a kernel crash.

Cisco Wave 2 APs may get into a boot loop when upgrading software over a WAN link. For more information, see: https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/220443-how-to-avoid-boot-loop-due-to-corrupted.html.

The following Wave 1 APs are not supported from 17.4 to 17.9.2, 17.10.x, 17.11.x, 17.13.x, and 17.14.x:

- **Cisco Aironet 1700 Series Access Point**
- **Cisco Aironet 2700 Series Access Point**
- **Cisco Aironet 3700 Series Access Point**

Note

- Support for the above APs was reintroduced from Cisco IOS XE Cupertino 17.9.3.
- Support for these APs does not extend beyond the normal product lifecycle support. Refer to the individual End-of-Support bulletins on Cisco.com.
- Feature support is on parity with the 17.3.x release. Features introduced in 17.4.1 or later are not supported on these APs in the 17.9.3 release.
- You can migrate directly to 17.9.3 from 17.3.x, where x=4c or later.
- Although the Cisco Aironet 1570 Series APs are not supported in Cisco IOS XE 17.14.1, the APs can still join the network.

- From Cisco IOS XE Dublin 17.10.x, Key Exchange and MAC algorithms like diffie-hellman-group14-sha1, hmac-sha1, hmac-sha2-256, and hmac-sha2-512 are not supported by default and it may impact some SSH clients that only support these algorithms. If required, you can add them manually. For information on manually adding these algorithms, see the **SSH Algorithms for Common Criteria Certification** document available at: https://www.cisco.com/c/en/us/td/docs/routers/ios/config/17-x/sec-vpn/b-security-vpn/m_sec-secure-shell-algorithm-ccc.html
- If APs fail to detect the backup image after running the **archive download-sw** command, perform the following steps:

  1. Upload the image using the **no-reload** option of the **archive download-sw** command:

     ```
     Device# archive download-sw /no-reload tftp://<tftp_server_ip>/<image_name>
     ```

  2. Restart the CAPWAP process using **capwap ap restart** command. This allows the AP to use the correct backup image after the restart (reload is not required.)

     ```
     Device# capwap ap restart
     ```

Caution The AP will lose connection to the controller during the join process. When the AP joins the new controller, it will see a new image in the backup partition. So, the AP will not download a new image from the controller.

- Fragmentation lower than 1500 is not supported for the RADIUS packets generated by wireless clients in the Gi0 (OOB) interface.
- Cisco IOS XE allows you to encrypt all the passwords used on the device. This includes user passwords and SSID passwords (PSK). For more information, see the "Password Encryption" section of the Cisco Catalyst 9800 Series Configuration Best Practices document.
- While upgrading to Cisco IOS XE 17.3.x and later releases, if the **ip http active-session-modules none** command is enabled, you will not be able to access the controller GUI using HTTPS. To access the GUI using HTTPS, run the following commands in the order specified below:

  1. **ip http session-module-list pkilist OPENRESTY_PKI**
  2. **ip http active-session-modules pkilist**

- Cisco Aironet 1815T OfficeExtend Access Point will be in local mode when connected to the controller. However, when it functions as a standalone AP, it gets converted to FlexConnect mode.
- The Cisco Catalyst 9800-L Wireless Controller may fail to respond to the BREAK signals received on its console port during boot time, preventing users from getting to the ROMMON. This problem is observed on the controllers manufactured until November 2019, with the default config-register setting of 0x2102. This problem can be avoided if you set config-register to 0x2002. This problem is fixed in the 16.12(3r) ROMMON for Cisco Catalyst 9800-L Wireless Controller. For information about how to upgrade the ROMMON, see the Upgrading ROMMON for Cisco Catalyst 9800-L Wireless Controllers section of the Upgrading Field Programmable Hardware Devices for Cisco Catalyst 9800 Series Wireless Controllers document.
- 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. If required, you can change the block size value to 8192 to speed up the transfer process, using the **ip tftp blocksize** command in global configuration mode.
- We recommend that you configure the **password encryption aes** and the **key config-key password-encrypt** *key* commands to encrypt your password.
- If the following error message is displayed after a reboot or system crash, we recommend that you regenerate the trustpoint certificate:

  ```
  ERR_SSL_VERSION_OR_CIPHER_MISMATCH
  ```

  Use the following commands in the order specified below to generate a new self-signed trustpoint certificate:

  1. device# configure terminal
  2. device(config)# **no crypto pki trustpoint** *trustpoint_name*
  3. device(config)# **no ip http server**
  4. device(config)# **no ip http secure-server**
  5. device(config)# **ip http server**
  6. device(config)# **ip http secure-server**
  7. device(config)# **ip http authentication** *local/aaa*

- Do not deploy OVA files directly to VMware ESXi 6.5. We recommend that you use an OVF tool to deploy the OVA files.
- Ensure that you remove the controller from Cisco Prime Infrastructure 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 the mobility MAC address using the **wireless mobility mac-address** command is mandatory for both HA and 802.11r.

- If you have Cisco Catalyst 9120 (E/I/P) and Cisco Catalyst 9130 (E) APs in your network and you want to downgrade, use only Cisco IOS XE Gibraltar 16.12.1t. Do not downgrade to Cisco IOS XE Gibraltar 16.12.1s.
- The following SNMP variables are not supported:
  - CISCO-LWAPP-WLAN-MIB: cLWlanMdnsMode
  - CISCO-LWAPP-AP-MIB.my: cLApDot11IfRptncPresent, cLApDot11IfDartPresent
- If you are upgrading from Cisco IOS XE Gibraltar 16.11.x 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 the **license boot level advipservices** command is not available in Cisco IOS XE Gibraltar 16.12.1s and 16.12.2s.
- The Cisco Catalyst 9800 Series Wireless Controller has a service port that is referred to as *GigabitEthernet 0* port.

  The following protocols and features are supported through this port:
  - Cisco Catalyst Center
  - Cisco Smart Software Manager
  - Cisco Prime Infrastructure
  - Telnet
  - Controller GUI
  - HTTP
  - HTTPS
  - Licensing for Smart Licensing feature to communicate with CSSM
  - SSH
- During device upgrade using GUI, if a switchover occurs, the session expires and the upgrade process gets terminated. As a result, the GUI cannot display the upgrade state or status.
- From Cisco IOS XE Bengaluru 17.4.1 onwards, the telemetry solution provides a name for the receiver address instead of the IP address for telemetry data. This is an additional option. During the controller downgrade and subsequent upgrade, there is likely to be an issue—the upgrade version uses the newly named receivers, and these are not recognized in the downgrade. The new configuration gets rejected and fails in the subsequent upgrade. Configuration loss can be avoided when the upgrade or downgrade is performed from Cisco Catalyst Center.
- Communication between Cisco Catalyst 9800 Series Wireless Controller and Cisco Prime Infrastructure uses different ports:
  - All the configurations and templates available in Cisco Prime Infrastructure are pushed through SNMP and CLI, using UDP port 161.
  - Operational data for controller is obtained over SNMP, using UDP port 162.
  - AP and client operational data leverage streaming telemetry:

- Cisco Prime Infrastructure to controller: TCP port 830 is used by Cisco Prime Infrastructure to push the telemetry configuration to the controller (using NETCONF).
- Controller to Cisco Prime Infrastructure: TCP port 20828 is used for Cisco IOS-XE 16.10.x and 16.11.x, and TCP port 20830 is used for Cisco IOS-XE 16.12.x, 17.1.x and later releases.

- To migrate public IP address from 16.12.x to 17.x. ensure that you configure the **service internal** command. If you do not configure the **service internal** command, the IP address does not get carried forward.
- RLAN support with Virtual Routing and Forwarding (VRF) is not available.
- When you encounter the SNMP error *SNMP_ERRORSTATUS_NOACCESS 6*, it means that the specified SNMP variable is not accessible.
- We recommend that you perform a controller reload whenever there is a change in the controller's clock time to reflect an earlier time.

Note The DTLS version (DTLSv1.0) is deprecated for Cisco Aironet 1800 based on latest security policies. Therefore, any new out-of-box deployments of Cisco Aironet 1800 APs will fail to join the controller and you will get the following error message:

```
%APMGR_TRACE_MESSAGE-3-WLC_GEN_ERR: Chassis 1 R0/2: wncd: Error in AP Join, AP <AP-name>,
mac:<MAC-address>Model AIR-AP1815W-D-K9, AP negotiated unexpected DTLS version v1.0
```

To onboard new Cisco Aironet 1800 APs and to establish a CAPWAP connection, explicitly set the DTLS version to 1.0 in the controller using the following configuration:

```
config terminal
ap dtls-version dtls_1_0
end
```

Note that setting the DTLS version to 1.0 affects all the existing AP CAPWAP connections. We recommend that you apply the configuration only during a maintenance window. After the APs download the new image and join the controller, ensure that you remove the configuration.

To upgrade the field programmable hardware devices for Cisco Catalyst 9800 Series Wireless Controllers, see *Upgrading Field Programmable Hardware Devices for Cisco Catalyst 9800 Series Wireless Controllers*.

Important Before you begin a downgrade process, you must manually remove the configurations which are applicable in the current version but not in older version. Otherwise, you might encounter an unexpected behavior.

Upgrade Path to Cisco IOS XE 17.14.x

Table 9: Upgrade Path to Cisco IOS XE Dublin 17.14.x

Current Software	Upgrade Path for Deployments with 9130 or 9124	Upgrade Path for Deployments Without 9130 or 9124
16.10.x	—[5]	Upgrade first to 16.12.5 or 17.3.x and then to 17.14.x.
16.11.x	—	Upgrade first to 16.12.5 or 17.3.x and then to 17.14.x.
16.12.x	Upgrade first to 17.3.5 or later or 17.6.x or later, and then to 17.14.x.	Upgrade first to 17.3.5 or later or 17.6.x or later, and then to 17.14.x.
17.1.x	Upgrade first to 17.3.5 or later and then to 17.14.x.	Upgrade first to 17.3.5 or later and then to 17.14.x.
17.2.x	Upgrade first to 17.3.5 or later and then to 17.14.x.	Upgrade first to 17.3.5 or later and then to 17.14.x.
17.3.1 to 17.3.4	Upgrade first to 17.3.5 or later or 17.6.x or later, and then to 17.14.x.	Upgrade directly to 17.14.x.
17.3.4c or later	Upgrade directly to 17.14.x.	Upgrade directly to 17.14.x.
17.4.x	Upgrade first to 17.6.x and then to 17.14.x.	Upgrade directly to 17.14.x.
17.5.x	Upgrade first to 17.6.x and then to 17.14.x.	Upgrade directly to 17.14.x.
17.6.x	Upgrade directly to 17.14.x.	Upgrade directly to 17.14.x.
17.7.x	Upgrade directly to 17.14.x.	Upgrade directly to 17.14.x.
17.8.x	Upgrade directly to 17.14.x.	Upgrade directly to 17.14.x.
17.9.x	Upgrade directly to 17.14.x	Upgrade directly to 17.14.x
17.10.x	Upgrade directly to 17.14.x	Upgrade directly to 17.14.x
17.11.x	Upgrade directly to 17.14.x	Upgrade directly to 17.14.x
17.12.x	Upgrade directly to 17.14.x	Upgrade directly to 17.14.x
17.13.x	Upgrade directly to 17.14.x	Upgrade directly to 17.14.x
8.9.x or any 8.10.x version prior to 8.10.171.0	Upgrade first to 17.3.5 or later or 17.6.x or later, and then to 17.14.x	Upgrade directly to 17.14.x.

[5] The Cisco Catalyst 9130 and 9124 APs are not supported in 16.10.x and 16.11.x releases.

Upgrading the Controller Software

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

Finding the Software Version

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

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

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

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

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

Software Images

- **Release**: Cisco IOS XE 17.14.x
- **Image Names (9800-80, 9800-40, and 9800-L)**:
  - C9800-80-universalk9_wlc.17.14.x.SPA.bin
  - C9800-40-universalk9_wlc.17.14.x.SPA.bin
  - C9800-L-universalk9_wlc.17.14.x.SPA.bin
- **Image Names (9800-CL)**:
  - **Cloud**: C9800-CL-universalk9.17.14.x.SPA.bin
  - **Hyper-V/ESXi/KVM**: C9800-CL-universalk9.17.14.x.iso, C9800-CL-universalk9.17.14.x.ova
  - **KVM**: C9800-CL-universalk9.17.14.x.qcow2
  - **NFVIS**: C9800-CL-universalk9.17.14.x.tar.gz

Software Installation Commands

Cisco IOS XE 17.14.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.
activateauto-abort-timer]	Activates the file and reloads the device. The **auto-abort-timer** keyword automatically rolls back image activation.
commit	Makes changes that are persistent over reloads.
rollback to committed	Rolls back the update to the last committed version.
abort	Cancels file activation, and rolls back to the version that was running before the current installation procedure started.
remove	Deletes all unused and inactive software installation files.

Licensing

The Smart Licensing Using Policy feature is automatically enabled on the controller. This is also the case when you upgrade to this release. By default, your Smart Account and Virtual Account in Cisco Smart Software Manager (CSSM) are enabled for Smart Licensing Using Policy. For more information, see the "Smart Licensing Using Policy" chapter in the *Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide*.

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

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 10: Test Configuration for Interoperability

Hardware or Software Parameter	Hardware or Software Type
Release	Cisco IOS XE 17.14.x

Hardware or Software Parameter	Hardware or Software Type
Cisco Wireless Controller	See Supported Hardware.
Access Points	See Supported APs, on page 21.
Radio	• 802.11ac • 802.11a • 802.11g • 802.11n
Security	Open, PSK (WPA2-AES), 802.1X (WPA2-AES) (EAP-FAST, EAP-TLS)
RADIUS	See Compatibility Matrix, on page 22.
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 11: Client Types

Client Type and Name	Driver or Software Version
Laptops	
Acer Aspire E 15 E5-573-3870 (Qualcomm Atheros QCA9377)	Windows 10 Pro (12.0.0.832)
Apple Macbook Air 11 inch	macOS Sierra 10.12.6
Apple Macbook Air 13 inch	macOS High Sierra 10.13.4
Macbook Pro Retina	macOS Catalina
Macbook Pro Retina 13 inch early 2015	macOS Mojave 10.14.3
Macbook Pro OS X	macOS X 10.8.5
Macbook Air	macOS Sierra v10.12.2
Macbook Air 11 inch	macOS Yosemite 10.10.5
MacBook M1 Chip	macOS Catalina
MacBook M1 Chip	macOS Ventura 13.2.1
MacBook Pro M2 Chip	macOS Ventura 13.3 beta
MacBook Pro M2 Chip	macOS Ventura 13.1
Dell Inspiron 2020 Chromebook	Chrome OS 75.0.3770.129
Google Pixelbook Go	Chrome OS 97.0.4692.27

Client Type and Name	Driver or Software Version
HP chromebook 11a	Chrome OS 76.0.3809.136
Samsung Chromebook 4+	Chrome OS 77.0.3865.105
Dell Latitude (Intel AX210)	Windows 11 (22.110.x.x)
Dell Latitude 3480 (Qualcomm DELL wireless 1820)	Win 10 Pro (12.0.0.242)
Dell Inspiron 15-7569 (Intel Dual Band Wireless-AC 3165)	Windows 10 Home (21.40.0)
Dell Latitude E5540 (Intel Dual Band Wireless AC7260)	Windows 7 Professional (21.10.1)
Dell Latitude E5430 (Intel Centrino Advanced-N 6205)	Windows 7 Professional (15.18.0.1)
Dell Latitude E6840 (Broadcom Dell Wireless 1540 802.11 a/g/n)	Windows 7 Professional (6.30.223.215)
Dell XPS 12 v9250 (Intel Dual Band Wireless AC 8260)	Windows 10 Home (21.40.0)
Dell Latitude 5491 (Intel AX200)	Windows 10 Pro (21.20.1.1)
Dell XPS Latitude12 9250 (Intel Dual Band Wireless AC 8260)	Windows 10 Home
Dell Inspiron 13-5368 Signature Edition	Windows 10 Home (18.40.0.12)
FUJITSU Lifebook E556 Intel 8260 (Intel Dual Band Wireless-AC 8260 (802.11n))	Windows 8 (19.50.1.6)
Lenovo Yoga C630 Snapdragon 850 (Qualcomm AC 2x2 Svc)	Windows 10 Home
Lenovo Thinkpad Yoga 460 (Intel Dual Band Wireless-AC 9260)	Windows 10 Pro (21.40.0)
Note For clients using Intel wireless cards, we recommend that you to update to the latest Intel wireless drivers if the advertised SSIDs are not visible.	
Tablets	
Apple iPad Pro (12.9 inch) 6th Gen	iOS 16.4
Apple iPad Pro (11 inch) 4th Gen	iOS 16.4
Apple iPad 2021	iOS 15.0
Apple iPad 7the Gen 2019	iOS 14.0
Apple iPad MD328LL/A	iOS 9.3.5
Apple iPad 2 MC979LL/A	iOS 11.4.1
Apple iPad Air MD785LL/A	iOS 11.4.1

Client Type and Name	Driver or Software Version
Apple iPad Air2 MGLW2LL/A	iOS 10.2.1
Apple iPad Mini 4 9.0.1 MK872LL/A	iOS 11.4.1
Apple iPad Mini 2 ME279LL/A	iOS 11.4.1
Apple iPad Mini 4 9.0.1 MK872LL/A	iOS 11.4.1
Microsoft Surface Pro 3 13 inch (Intel AX201)	Windows 10 (21.40.1.3)
Microsoft Surface Pro 3 15 inch (Qualcomm Atheros QCA61x4A)	Windows 10
Microsoft Surface Pro 7 (Intel AX201)	Windows 10
Microsoft Surface Pro 6 (Marvell Wi-Fi chipset 11ac)	Windows 10
Microsoft Surface Pro X (WCN3998 Wi-Fi Chip)	Windows
Mobile Phones	
Apple iPhone 5	iOS 12.4.1
Apple iPhone 6s	iOS 13.5
Apple iPhone 7 MN8J2LL/A	iOS 11.2.5
Apple iPhone 8	iOS 13.5
Apple iPhone 8 Plus	iOS 14.1
Apple iPhone 8 Plus MQ8D2LL/A	iOS 12.4.1
Apple iPhone X MQA52LL/A	iOS 13.1
Apple iPhone 11	iOS 15.1
Apple iPhone 12	iOS 16.0
Apple iPhone 12 Pro	iOS 15.1
Apple iPhone 13	iOS 15.1
Apple iPhone 13 Mini	iOS 15.1
Apple iPhone 13 Pro	iOS 15.1
Apple iPhone SE MLY12LL/A	iOS 11.3
Apple iPhone SE	iOS 15.1
ASCOM i63	Build v 3.0.0
ASCOM Myco 3	Android 9
Cisco IP Phone 8821	11.0.6 SR4
Drager Delta	VG9.0.2
Drager M300.3	VG2.4
Drager M300.4	VG2.4

Client Type and Name	Driver or Software Version
Drager M540	DG6.0.2 (1.2.6)
Google Pixel 3a	Android 11
Google Pixel 4	Android 11
Google Pixel 5	Android 11
Google Pixel 6	Android 12
Google Pixel 7	Android 13
Huawei Mate 20 pro	Android 9.0
Huawei P20 Pro	Android 10
Huawei P40	Android 10
LG v40 ThinQ	Android 9.0
One Plus 8	Android 11
Oppo Find X2	Android 10
Redmi K20 Pro	Android 10
Samsung Galaxy S9+ - G965U1	Android 10.0
Samsung Galaxy S10 Plus	Android 11.0
Samsung S10 (SM-G973U1)	Android 11.0
Samsung S10e (SM-G970U1)	Android 11.0
Samsung Galaxy S20 Ultra	Android 10.0
Samsung Galaxy S21 Ultra 5G	Android 13.0
Samsung Galaxy S22 Ultra	Android 13.0
Samsung Fold 2	Android 10.0
Samsung Galaxy Z Fold 3	Android 13.0
Samsung Note20	Android 12.0
Samsung G Note 10 Plus	Android 11.0
Samsung Galaxy A01	Android 11.0
Samsung Galaxy A21	Android 10.0
Sony Experia 1 ii	Android 11
Sony Experia	Android 11

Client Type and Name	Driver or Software Version
Xiaomi Mi 9T	Android 9
Xiaomi Mi 10	Android 11
Spectralink 84 Series	7.5.0.x257
Spectralink 87 Series	Android 5.1.1
Spectralink Versity Phones 92/95/96 Series	Android 10.0
Spectralink Versity Phones 9540 Series	Android 8.1.0
Vocera Badges B3000n	4.3.3.18
Vocera Smart Badges V5000	5.0.6.35
Zebra MC40	Android 4.4.4
Zebra MC40N0	Android 4.1.1
Zebra MC92N0	Android 4.4.4
Zebra MC9090	Windows Mobile 6.1
Zebra MC55A	Windows 6.5
Zebra MC75A	OEM ver 02.37.0001
Zebra TC51	Android 6.0.1
Zebra TC52	Android 10.0
Zebra TC55	Android 8.1.0
Zebra TC57	Android 10.0
Zebra TC58	Android 11.0
Zebra TC70	Android 6.1
Zebra TC75	Android 10.0
Zebra TC520K	Android 10.0
Zebra TC8000	Android 4.4.3
Printers	
Zebra QLn320 Mobile Printer	LINK OS 5.2
Zebra ZT230 IndustrialPrinter	LINK OS 6.4
Zebra ZQ310 Mobile Printer	LINK OS 6.4
Zebra ZD410 Industrial Printer	LINK OS 6.4
Zebra ZT410 Desktop Printer	LINK OS 6.2
Zebra ZQ610 Industrial Printer	LINK OS 6.4
Zebra ZQ620 Mobile Printer	LINK OS 6.4
Wireless Module	

Client Type and Name	Driver or Software Version
Intel AX 411	Driver v22.230.0.8
Intel AX 211	Driver v22.230.0.8, v22.190.0.4
Intel AX 210	Driver v22.230.0.8, v22.190.0.4, v22.170.2.1
Intel AX 200	Driver v22.130.0.5
Intel 11AC	Driver v22.30.0.11
Intel AC 9260	Driver v21.40.0
Intel Dual Band Wireless AC 8260	Driver v19.50.1.6
Samsung S21 Ultra	Driver v20.80.80
QCA WCN6855	Driver v1.0.0.901

Issues

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

Note All incremental releases contain fixes from the current release.

Cisco Bug Search Tool

The Cisco Bug Search Tool (BST) allows partners and customers to search for software bugs based on product, release, and keyword, and aggregates key data such as bug details, product, and version. The BST is designed to improve the effectiveness in network risk management and device troubleshooting. The tool has a provision to filter bugs based on credentials to provide external and internal bug views for the search input.

To view the details of an issue, click the corresponding identifier.

Open Issues for Cisco IOS XE 17.14.1

Identifier	Headline
CSCwj02903	Controller CAPWAP Mobility Control and Data Path goes down as it fails to handle Path Maximum Transmission Unit (PMTU) acknowledgement.
CSCwj12705	Virtual Routing and Forwarding (VRF) mismatch between the Cisco 5520 Series Wireless Controller as anchor controller and the Cisco Catalyst 9800-80 Wireless Controller as foreign causes user connection failure.
CSCwj35416	Cisco Catalyst 9136 AP does not show neighbors in the Neighbor Discovery Protocol (NDP).

Identifier	Headline
CSCwi53570	Cisco Catalyst 9800-L Wireless Controller interface connecting to TenGigabitEthernet0/1/0 encounters input/overrun errors.
CSCwj04177	AP undergoing Extensible Authentication Protocol (EAP) fails if the password is more than 31 characters.
CSCwi39752	Cisco Catalyst 9800-40 Wireless Standby Controller unexpectedly becomes unresponsive with the last reload reason 'Critical software exception'.
CSCwj13944	AAA override VLAN is not applied upon roaming in local authentication as the user is placed back in the default VLAN.
CSCwj03060	Cisco Aironet 1815w AP encounters kernel unresponsiveness on image version 17.9.4.205.
CSCwi96176	Cisco Catalyst 9130 and 9166 APs show high channel utilization with one single client connected.
CSCwi99566	Cisco Catalyst 9124AXI-E AP becomes unresponsive due to channel 36 not being supported in the Jordan regulatory domain.
CSCwj00465	Active controller becomes ActiveRecovery when the redundancy port link is down.
CSCwj16668	Wired clients behind a WGB lose network connectivity when doing IRCM roaming from Cisco Catalyst 9800 Wireless Controller to Cisco 5520 Wireless Controller.
CSCwi53998	Cisco Aironet 1815 APs report 0 dBm as the Received Signal Strength Indicator (RSSI) for neighboring APs.
CSCwi99296	Cisco Catalyst 9120 AP encounters kernel unresponsiveness with the PC due to wlc_bmac_suspend_mac_and_wait.
CSCwj08558	Cisco Catalyst 9124 APs do not assign the correct channels where 2.4 GHz is set for clients.
CSCwj25187	Controller does not display the redundancy details on the Web-UI, only on the Command Line Interface (CLI).
CSCwj13842	Controller causes IP theft and client deletion via Address Resolution Protocol (ARP) with DHCP required enabled.
CSCwj29389	Controller encounters memory leak at the CAPWAP control message fragmentation issue.
CSCwj13190	Inventory app shows "Internal Error" for controller that was in Catalyst Center for several releases.
CSCwi83037	Cisco Aironet 4800 AP: Radio Core data files generated Radio 1 During the Longevity testing.
CSCwi04855	Cisco Catalyst 9115 APs disjoin repeatedly with controller traceback.

Identifier	Headline
CSCwj14376	Cisco Catalyst 9800-40 Wireless Controller's mobility tunnels go down after upgrading via In-Service Software Upgrade (ISSU).
CSCwj03495	Cisco Aironet 1562 as Mesh AP (MAP) recognizes Cisco Catalyst 9124 Root AP (RAP) as a parent and completes authentication, but fails in the CAPWAP join because Mesh Adjacency messages are undetected by the RAP.
CSCwj11366	Cisco Wave 2 APs in FlexConnect do not decrypt traffic after Opportunistic Key Caching (OKC) fast roaming is enabled.
CSCwh52553	Cisco Catalyst 9105 AP encounters high utilization and performance issues due to high mDNS traffic.
CSCwj26196	Controller running the IOS XE software encounters an unexpected reset while trying to validate the MAC address with the EWLC_APP_INFRA_ID_MAGIC.
CSCwj34379	Cisco Catalyst 9800-80 Wireless Controller encounters Wireless Network Control daemon (WNCd) issues when accessing Crimson Database.
CSCwj35579	Clients require IP DHCP smart-relay support for controller.
CSCwj45544	Cisco Aironet 4800 AP fails to extract IOx app package.

Resolved Issues for Cisco IOS XE 17.14.1

Identifier	Headline
CSCwh88320	Cisco Catalyst 9800-40 Wireless Controller encounters false jammer alerts.
CSCwf30701	Cisco Aironet 2800 and Cisco Catalyst 9120 APs as supplicants do not initiate the Extensible Authentication Protocol (EAP) process until a static IP address is assigned.
CSCwf99932	Cisco Catalyst 9120 AP Radio1 becomes unresponsive.
CSCwh57076	Controller does not forward broadcast Address Resolution Protocol (ARP) request to the wireless client.
CSCwj01916	Cisco Catalyst 9162 AP in FlexConnect mode constantly disjoins the controller.
CSCwh63270	Cisco Catalyst 9130AXI APs unexpectedly become unresponsive due to radio failure.
CSCwf79175	Pairwise Master Key Identification (PMKID) mismatch between FlexConnect central authentication Wave 2 AP and controller for 802.11X-SHA256 on roaming clients.
CSCwf92148	Cisco Catalyst 9120 AP dual 5 GHz allow clients to connect to slot 0 as High Efficiency (HE) clients when 802.11ax is disabled in all WLANs and to slot 1 with the same WLANs HE disabled.
CSCwf13107	Cisco Catalyst 9105 AP becomes unresponsive during longevity test because of Single Client Bridge (SCB) mismatch.

Identifier	Headline
CSCwf10839	Cisco Embedded Wireless Controller sends bursts of Virtual Router Redundancy Protocol (VRRP) traffic, causing the switch port to be down due to the storm-control action configuration on the switch port side.
CSCwh81332	Cisco Catalyst 9130APs encounter kernel unresponsiveness after upgrading to 17.6.6.
CSCwh68219	Cisco Catalyst 91xx AP does not process the Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) server Hello.
CSCwh09642	IP Theft observed due to the zone ID being 0x00000000.
CSCwi64010	Controller accepts the reserved IPv6 multicast address to be configured as a mobility multicast IPv6 address.
CSCwf83278	Controller client traffic fails in N+1 mode when AP sends CLIENT_DEL_STOP_REASSOC.
CSCwi96508	Cisco Wave 2 APs allowing SKC roam cause client deletion with the reason as INVALID_PMKID.
CSCwf53520	Cisco Aironet 1815 AP encounters kernel unresponsiveness.
CSCwi18057	Controller encounters a 4-way handshake failure and a missing M3 packet.
CSCwf68131	Cisco Catalyst 9105AXW APs detect bad block monitoring and repair.
CSCwi20933	FlexConnect client is unable to perform Secure Agile Exchange (SAE) authentication due to the controller rejecting assoc-req with a Pairwise Master Key Identification (PMKID) mismatch.
CSCwh92425	Cisco Catalyst 9130 and 9136 APs do not honor power saving mode.
CSCwh54762	Cisco Catalyst 9120 AP encounters kernel unresponsiveness due to not syncing: assert:"0" failed: file "wlc_fifo.c:960".
CSCwh20306	Cisco Wave 2 APs hyperlocation is broken if aWIPS is enabled.
CSCwi22895	Controller becomes unresponsive within Radio Resource Management (RRM) service due to ReloadReason=Critical process rrm fault on rp_0_0 (rc=134).
CSCwi64652	802.11ax APs running IoT application do not reset the BLE interface after 100 attempts.
CSCwi08147	Controller's GUI does not allow modifying QoS policies without having the "QoS Service Set Identifier (SSID) policy" automatically set on the policy profile.
CSCwf07384	Wired clients behind the Cisco Catalyst 9105 AP RLAN face limited connectivity and can't pass any traffic.
CSCwf65794	Cisco Aironet 1852 AP reloads unexpectedly due to radio failure.
CSCwh74663	Cisco Aironet 2800, 3800, 4800, 1560 APs and Cisco Catalyst IW6300 AP do not send QoS data frames downstream.

Identifier	Headline
CSCwh29924	Cisco Catalyst 9105, 9115, and 9120 AP WGB Antenna-a encounters a malfunction if the configuration is ab-antenna.
CSCwf52815	Cisco Wave 2 APs improve the PMTU Discovery mechanism to be able to honor the ICMP unreachable MTU value and recalculate the AP PMTU.
CSCwf72320	Cisco Catalyst IW916x APs and Cisco Catalyst 9105, 9130, and 9136 APs become unresponsive with the reason LED_APP or sxpd.
CSCwi48980	Controller local password policy does not take effect on GUI login as expected.
CSCwi04705	Controller does not send the broadcast Gratuitous Address Resolution Protocol (gARP) on behalf of the client on inter-controller roaming events.
CSCwh89539	Controller queues CAPWAP messages for longer than x seconds with client throttling turned on.
CSCwh30996	PDU type in the transmit (Tx) packet for iBeacon in dual mode needs to be changed to adv_non_connectable_ind.
CSCwh59543	Cisco Catalyst 9120 AP becomes unresponsive leading to a Capwapd Crash during Scale Longevity.
CSCwf91557	Cisco Wave 2 APs stop the PMTU Discovery mechanism after reaching the maximum hardcoded value.
CSCwi35946	Cisco Catalyst 9120 AP encounters kernel unresponsiveness.
CSCwf12301	Watchdog Reset (wcpd) Transmit (Tx) retry number is not MAC Service Data Unit (MSDU)-based.
CSCwh74415	FlexConnect local switching APs per client rate limit do not work.
CSCwf85025	9166 Regulatory Domain (ROW) local mode AP for the United Kingdom decreases Transmit (tx) power after channel change, causing connection failure for the client.
CSCwi88967	Cisco Catalyst 9120 APs disconnect due to Port Status Monitor (PSM) microcode watchdog CS00012333933.
CSCwf78066	APs managed by the controller display the "No radios in the selected band" message in the Cisco Catalyst Center heat map.
CSCwf13804	APs fail to onboard new client associations with ‘No buffer space available’ messages.
CSCwh56147	Controller is missing Simple Network Management Protocol (SNMP) Object ID (OID) for AP Location Tag.
CSCwh92459	Controller unexpectedly becomes unresponsive with ReloadReason "Critical process wncd fault on rp_0_0".
CSCwh20944	Cisco Catalyst 9120 AP encounters kernel unresponsiveness - not syncing: assert:"done" failed: file "phy_ac_radio.c:6141.

Identifier	Headline
CSCwi34051	Cisco Aironet 2800 AP encounters FIQ/NMI reset due to PC at wl_get_staid_info.
CSCwi95945	Cisco Catalyst 9130 APs stop forwarding router advertisements for FlexConnect Local Switching/Local Authentication after 4-6 hours of uptime.
CSCwi49666	Cisco Catalyst 9136 APs encounter fluctuations in ambient temperature reports.
CSCwe52756	Cisco Catalyst 9120 AP sends Ready to Send (RTS) with 6 Mbps when this rate is configured as unsupported (CS00012284859).
CSCwi07401	Controller encounters an unexpected reboot while collecting wireless client stats with the Embedded Event Manager (EEM) script.
CSCwh49810	Audit session ID changes and client loses network access after inter- Wireless Network Control Daemon (WNCD) roam.
CSCwh82872	Cisco Catalyst 9115AXI-S AP association request dropped on the Cisco Catalyst 9800-80 Wireless Controller.
CSCwh87903	Cisco Catalyst 9120 AP sends authorization response failures for specific MAC addresses due to "suppressed by MAC filter".
CSCwi69251	Cisco Catalyst 9800-40 Wireless Controller becomes unresponsive on Critical process Radio Resource Management (RRM) fault on rp_0_0.
CSCwf95868	Single Band Broadcom (BCM) WGB Radio 0 Transmit (Tx) power decreased by nearly 20 dBm while configuring antenna number.
CSCwf83292	Cisco Catalyst 9130 AP does not send DHCP Offer and Acknowledgement (ACK) Over the Air (OTA) through the radio interface to the client.
CSCwj10697	Cisco Catalyst 9124AX AP experiences image upgrade failure.
CSCwf44441	Cisco Catalyst 9166 AP becomes nonoperational due to radio firmware failure.
CSCwi67013	Cisco Aironet 2800 AP on Taiwan domain is unable to send Wi-Fi signals on channels 52, 120, 124 and 128.
CSCwi69093	Controller GUI shows incorrect number of clients connected to the AP.
CSCwi19804	Cisco Catalyst 9105, 9115, 9120 APs experience radio misconfiguration after AP reloads in admin state down.
CSCwh75431	Cisco Aironet 1830, 1850 APs report false high channel utilization, which causes performance isues on 5 GHz band.
CSCwi52692	Cisco Catalyst 9130 AP moves Universal PoE spare pair to turn off over CDP.
CSCwh27366	Cisco Aironet 3800 AP radio firmware becomes nonoperational with reset code 2.
CSCwh62342	mDNS gateway does not respond correctly when Location Specefic Services filter is enabled in the 5-GHz band on FlexConnect AP.

Identifier	Headline
CSCwf50177	Cisco Catalyst 9105AXW AP experiences large count of bad physical eraseblocks.
CSCwh31966	Controller becomes nonoperational on WNCd process during database termination.
CSCwh18613	Encrypted wireless mesh pre-shared key changes when "password encryption aes" is in use.
CSCwi28174	Layer 3 multicast packets are sent on native VLAN when VLAN ID 1 is selected on policy profile with AAA override.
CSCwf93992	Cisco Aironet 2800 FlexConnect APs are unable to process EAP-TLS fragmented packets if delay is more than 50ms.
CSCwi28172	Cisco Catalyst 9120 AP experiences kernel panic with PC at wlc_bmac_suspend_mac_and_wait+0x3c/0x488 [wl] CS00012321648.
CSCwf81866	Radio 0 WGB configuration is not backed up correctly when doing a TFTP backup of the configuration.
CSCwf63818	Cisco Aironet 1832 AP running on release IOS XE Cupertino 17.9.2 experiences kernel panic.
CSCwh58099	Controller allows client reconnection after client deletion and Change of Authorization (CoA) termination.
CSCwf83132	Controller does not send 802.11r mobility payload on mobility group name change to FlexConnect AP causing MDID mismatch.
CSCwi35699	Cisco Catalyst 9120 AP detects its BSSID as malicious after channel resets.
CSCwi47294	Per client rate limit with FlexConnect AP is not functioning.
CSCwf40553	Cisco Catalyst 9115, 9120AX APs do not allow channel 165 for -Z domain.
CSCwh81071	Slot 2 is down for GB country after performing factory reset.
CSCwi08442	APs are unable to join when CBAR is configured on controller.
CSCwj01446	Personal Identity Verification (PIV) authentication requires an additional backslash in the redirection URL to work successfully.
CSCwi07094	Apple clients are unable to connect to FlexConnect AP when WPA3 is enabled.
CSCwi06785	Controller does not send IPv4 GARPs or IPv6 NA for wireless clients in RUN state after a switchover.
CSCwf59348	Cisco Catalyst 9105, 9115, and 9120 APs set the maximum transmit power level to -128 dBm in Country IE.
CSCwh09879	Cisco Wave 2 APs in FlexConnect mode do not allow clients to connect and sends association-response failure after changing country code.

Identifier	Headline
CSCwf61881	Cisco Catalyst 9166 AP changes country code to UX domain while encountering issues using standard power mode.
CSCwh30078	Cisco Wave 2 APs become nonoperational repeatedly in throughput testing.
CSCwh88100	Cisco Aironet 3800 AP becomes nonoperational due to kernel panic with PC at skb_unlink+0x40/0x54.
CSCwe24263	Cisco Catalyst 9130 experiences inconsistent transmission power levels advertised in the country information of beacon frame causing client-side issues.
CSCwf94863	Cisco Catalyst 9115 AP becomes nonoperational due to kernel panic with PC/LR is at drop_pagecache_sb+0x78/0x110.
CSCwh88246	AP does not allow to apply URL filter after invalid configuration.
CSCwi72191	VLAN change on the AP port results in unsuccessful update of IPv6 routes on Wave 2 AP.
CSCwf91445	Controller shares accounting information for PSK local authentication WLANs.
CSCwi75759	Controller reloads due to critical process WNCd fault.
CSCwi11182	Memory leak occurs when no RADIUS server is reachable.
CSCwh27425	Cisco Catalyst 9115AX AP does not forward a part of the CAPWAP data packets to the uplink direction.
CSCwi42112	MAC address of wired clients are being learned from the Cisco Catalyst 9124 MAP.
CSCwi08073	Controller receives false notifications for reaching maximum client limit.
CSCwh59048	APs in the 5-GHz band remains in down state for -A domain access points in Guatemala.
CSCwi19481	Cisco Catalyst 9130 APs stop forwarding router advertisements after 4-6 hours of operation.
CSCwi83124	Pop-ups are not displayed correctly in dark mode in the controller.
CSCwh37783	Controller is unable to load lobby admin page.
CSCwf62051	Access point unexpectedly reloads due to kernel panic with mDNS enabled.
CSCwi11038	Cisco Catalyst 9115 OEAP experiences kernel unresponsiveness.
CSCwh35072	Cisco Aironet 3800 AP reloads unexpectedly due to FIQ/NMI reset.
CSCwh99036	Controller experiences WNCd abnormalities when processing the AP supported channels.
CSCwh42002	Controller becomes nonoperational with WNCd core while processing CAPWAP data.
CSCwh61011	Cisco Catalyst 9120 and 9115 APs unexpectedly disjoin from the controller and do not establish DTLS again.

Identifier	Headline
CSCwf42824	Cisco Catalyst 9105AXW APs do not recover after upgrade.
CSCwh68360	Cisco Catalyst 9120 AP experiences kernel panic due to wlc_key_set_data in 17.9.4 CS00012316343.
CSCwh59420	Cisco Catalyst 9136 AP becomes nonoperational on IOS XE Cupertino 17.9.x.
CSCwi96089	Cisco Wave 2 APs do not plumb keys after session timeout reauthentication.
CSCwh50681	New SSID arp0v0 is broadcast only after a Cisco IOS-XE Cupertino 17.9.3 wireless upgrade.
CSCwf67316	Cisco Aironet 2800, 3800, 4800, 1560, IW6300 APs may not detect radar on the required levels after CAC time.
CSCwe81775	Apple devices are not deleted after sending EAP messages.
CSCwf69377	Controller might become nonoperational within IOSd during an update to SPAN source ports.
CSCwh68768	Controller displays public cloud 17.9.3 error while configuring basic wireless setup.
CSCwi03442	Cisco Catalyst 9130 AP does not honor U-APSD trigger frame resulting in RTP stream disruption.
CSCwh08625	Cisco Catalyst 9105, 9115, 9120 APs experience kernel panic with PC at _raw_spin_unlock CS00012303664.
CSCwi50732	VLAN Group Support for DHCP and Static IP Clients feature does not work on FlexConnect Central Switching mode.
CSCwh91254	Monitoring PHY Health check on Broadcom APs
CSCwh20334	Change of Authorization (CoA) server key appears blank on the controller GUI.
CSCwh49406	Cisco Catalyst 9130 AP generates excessive CleanAir syslogs.
CSCwh60483	Cisco Catalyst 9136 Series AP shows abnormal temperature readings.
CSCwh33190	Cisco Catalyst 9115 AP in local mode becomes nonoperatioanl due to kernel panic.
CSCwh61007	Controller becomes nonoperational when provisioning multiple APs.
CSCwh33056	Policy tag description disappears after deleting WLAN location entries.
CSCwf83515	Inconsistent transmission power levels advertised in Country information of beacon frame causes client-side issue.
CSCwf45495	Cisco Catalyst 9130 APs do not start CAPWAP due to interface reset while waiting for IP address from DHCP.
CSCwi92439	Cisco Aironet 1815 APs report high channel utilization in the 5-Ghz band.
CSCwi55714	Controller unexpectedly reboots when handling NMSP TLS connection.

Identifier	Headline
CSCwf53130	Cisco Catalyst 9166 AP becomes nonoperational on IOS XE Cupertino 17.9.2 and sends PC at __qdf_bug and LR at qdf_mem_set (SF 06663975).
CSCwe58841	PoE negotiation does not process on both ports in Cisco Catalys 9136 AP.
CSCwi28382	Controller experiences unexpected resets with the following message: Log message: %PMAN-3-PROCHOLDDOWN: R0/7: wncd: The process wncd has been helddown (rc 134)
CSCwf64009	Cisco Aironet 1815 AP leaks RLAN VLAN traffic with looped port.
CSCwi54064	APs in same controller classify each other as rogue and sends "AP Impersonation" alert.
CSCwh76420	Controller becomes nonoperational while performing ISSU upgrade.
CSCwi81972	Cisco Wave 2 APs should check CAPWAP payload sanity before deleting it.
CSCwj04904	Cisco Catalyst 9300LM switch is not compatible with Cisco Aironet 1815 AP when it is connected on a port with Cisco Unified IP Phone 7945G.
CSCwh44793	Cisco Catalyst 9130 AP on IOS XE Amsterdam 17.3.6 fails to join with error to set FT data in BSSID after site-tag is changed on controller.
CSCwi22270	Cisco Catalyst 9120 AP experiences radio unresponsiveness during longevity run test on IOS XE 17.13.
CSCwh20934	Cisco Catalyst 9120 AP and Cisco Aironet 2800 AP reboot repeatedly due to Systemd critical process unresponsiveness when joining controller that runs on IOS XE Amsterdam 17.9.3.
CSCwi05672	Wireless Driver is unable to decrypt ICAP packets in Cisco Catalyst 9130 AP.
CSCwh01589	Cisco Catalyst 9120AXE AP remains at u-boot and with multiple failure messages.
CSCwi66582	Controller returns with error while uploading backup file with FTP on GUI.
CSCwi22847	Controller becomes nonoperational after receiving analytics from AP.
CSCwi69217	IW916x WGB DL MC2UC traffic forwarding five minutes then interrupted in non-native VLAN.
CSCwj12136	COS uWGB: Duplicate IP address detected on wired devices connected to it.
CSCwc06025	By disabling 'Backhaul Client Access' on IW9167EH Root AP, Mesh APs cannot associate to Root AP.

Troubleshooting

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

Related Documentation

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

Cisco Wireless Controller

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

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

The installation guide for your controller is available at:

- Hardware Installation Guides

All Cisco Wireless Controller software-related documentation

Cisco Catalyst 9800 Wireless Controller Data Sheets

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

Cisco Embedded Wireless Controller on Catalyst Access Points

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

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

Wireless Product Comparison

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

Cisco Access Points–Statement of Volatility

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

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

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

Cisco Prime Infrastructure

Cisco Prime Infrastructure Documentation

Cisco Connected Mobile Experiences

Cisco Connected Mobile Experiences Documentation

Cisco Catalyst Center

Cisco Catalyst Center Documentation

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business 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 DevNet.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a gateway to the Cisco bug-tracking system, which maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. The BST provides you with detailed defect information about your products and software.

Documentation Feedback

To provide feedback about Cisco technical documentation, use the feedback form available in the right pane of every online document.