Release Notes for Cisco Catalyst 9800 Series Wireless Controller, Cisco IOS XE 17.17.x

First Published: 2025-03-31

Release Notes for Cisco Catalyst 9800 Series Wireless Controller, Cisco IOS XE 17.17.x

Introduction to Cisco Catalyst 9800 Series Wireless Controllers

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

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

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

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

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

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

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

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

What's New in Cisco IOS XE 17.17.1

Table 1: New and Modified Software Features

Feature Name	Description and Documentation Link
Support for Cisco Wireless 9172H Series Wi-Fi 7 Access Points (CW9172H)	The 9172H AP is an enterprise-class tri-band (2.4 GHz, 5 GHz, 6 GHz) access point. The AP supports full interoperability with leading 802.11ax and 802.11ac clients and a hybrid deployment with other APs and controllers. **Note** For more information about all the supported countries for the APs, see https://www.cisco.com/c/dam/assets/prod/wireless/wireless-compliance-tool/index.html.
Cisco Advanced Wireless Intrusion Prevention System (aWIPS) Enhancements for Common Criteria	The Cisco aWIPS new capabilities include: • SSID Monitoring: Keep track of Service Set Identifiers (SSIDs) to ensure compliance • Connection Monitoring: Observe connections from authorized clients to unauthorized APs and vice versa, ensuring that only permitted devices access the network • Policy Violation Monitoring: Monitor the wireless network for any traffic that violates established policies, maintaining security and integrity

Feature Name	Description and Documentation Link
Off-Channel PMF Rogue Containment	From this release onwards, off-channel PMF rogue containment detection is possible on off-channel radios or non-serving radios. The following commands are introduced: • **pmf-offchannel** • **show wireless wps rogue stats** • **show wireless wps rogue containment summary** For more information, see Managing Rogue Devices.
AnyLocate Enhancements - Ultra-Wideband (UWB) Downlink Time Difference of Arrival (DL-TDoA)	This release introduces beta support for Ultra-Wideband (UWB) Downlink Time Difference of Arrival (DL-TDoA). UWB DL-TDoA enables high-accuracy mobile device wayfinding, which can substantially improve the indoor navigation experience. Other indoor location technologies are generally limited to a level of precision no better than 2m, but UWB DL-TDoA can improve that to a sub-meter. The following are the benefits of the increased accuracy: • **Healthcare**: Allows you to navigate to the correct room when there are multiple adjacent doorways. • **Retail**: Offers a personalized shopping experience, directing customers to a specific shelf, aisle, or product rather than just a general section of the store. • **Manufacturing**: Automated ground vehicles (AGV) can benefit from the increased accuracy by avoiding collisions and optimize their paths. • **Transportation**: Airports and transit hubs use UWB DL-TDoA to assist passengers with disabilities or those in a hurry, by providing exact directions to gates, restrooms, or lounges.

Feature Name	Description and Documentation Link
AP Certificate Auto-Renewal (LSC)	The AP Certificate Renewal (LSC) feature allows the renewal of Locally Significant Certificates (LSCs) for APs before their expiry. The feature ensures that the APs can continue to provide seamless services by renewing their certificates in a timely manner. The controller orchestrates this process to minimize service disruption, particularly focusing on automatic renewal mechanisms that do not require manual intervention. The following commands are introduced: • **ap lsc-provision** • **ap lsc-provision renew due-time** • **ap lsc-provision renew one-shot** • **ap lsc-provision renew staggered timeout** • **ap lsc-provision renew schedular** • **ap lsc renew due-time** • **show ap lsc-provision info** For more information, see AP Certificate Renewal (LSC).
Automated Frequency Coordination (AFC) Support for Canada and US	From this release, AFC Standard Power Mode is enabled for Canada and the U.S.
UNII-3 Support (low power) for –E Regulatory Domain	In this release, UNII-3 channels (from 149 to 173) for the –E domain are disabled by default. As the UNII-3 channels operate at low power, when the RRM selects a UNII-3 channel for an AP, it could result in coverage gaps. To address this issue, an option is provided to enable or disable the UNII-3 channels. The following commands are introduced: • **show ap rf-profile name test5 detail** • **show ap dot11 5ghz channel** • **channel unii3-low-power-channels** • **ap dot11 5ghz rrm channel unii3-low-power-channels** **Note** UNII-3 channels are certified for use **only** with access points under the the ETSI regulatory domain. For more information, see the *Restrictions* and *Supported Access Points* sections in UNII-3 channels in the –E domain.

Feature Name	Description and Documentation Link
Automated Frequency Coordination (AFC) Support on Cisco Wireless 9172H Series Wi-Fi 7 Access Points (CW9172H) and Cisco Wireless 9172I Series Wi-Fi 7 Access Points (CW9172I)	From this release, AFC is supported on CW9172H APs and CW9172I Access Points.
Tier B/C/D Country Support for Cisco Wireless 9178I Series Wi-Fi 7 Access Points (CW9178I)	From this release, Cisco Wireless 9178I Series Wi-Fi 7 Access Points are supported in 96 more countries. **Note** For more information about all the supported countries for the AP, see Countries and Regulations.
Tier B/C/D Country Support for: • Cisco Wireless 9176I Series Wi-Fi 7 Access Points (CW9176I) • Cisco Wireless 9176D Series Wi-Fi 7 Access Points (CW9176D)	From this release, Cisco Wireless 9176I and 9176D Series Wi-Fi 7 Access Points are supported in 96 more countries. **Note** For more information about all the supported countries for the AP, see Countries and Regulations.
Tier B/C/D Country Support for: • Cisco Wireless 9163E Series Wi-Fi 6E Access Points (CW9163E) • Cisco Catalyst 9124AX Series Wi-Fi 6 Access Points (C9124AXI/AXD/AXE)	From this release, • Cisco Wireless 9163E Series Wi-Fi 6E Access Points are supported in 81 more countries • Cisco Catalyst 9124AX Series Wi-Fi 6 Access Points are supported in 20 more countries **Note** For more information about all the supported countries for the AP, see Countries and Regulations.
Support for Dual-Band (XOR) Radio in Cisco Wireless 9176 Series Wi-Fi 7 Access Points (CW9176I/D)	From this release, dual-band (XOR) radio is supported when operating in 2.4-GHz or 5-GHz low band mode (UNII 1-2A), on Cisco Wireless 9176 Series Wi-Fi 7 APs.
Support for Access Ports with Dual Port Authentication in Cisco Catalyst 9136 Series Access Points and Cisco Wireless 9178 Series Access Points (CW9178I)	From this release, access ports with dual port authentication is supported in Cisco Catalyst 9136 and CW9178I Series APs. For more information about access ports with dual port authentication support, see Security.

Feature Name	Description and Documentation Link
Support for Terminal Doppler Weather Radar (TDWR) for All Regulatory Domains in Wi-Fi 6E and Wi-Fi 7 Access Points	From this release, TDWR is supported for all regulatory domains in the Wi-Fi 6E and Wi-Fi 7 APs.

Table 2: New and Modified GUI Features

Feature Name	GUI Path
Off-Channel PMF Rogue Containment	• **Configuration** > **Tags & Profiles** > **AP Join**
AP Certificate Auto-Renewal (LSC)	• **Configuration** > **Wireless** > **Access Points** > **LSC Provision** • **Configuration** > **Wireless** > **Bulk AP Provisioning**

MIBs

The following MIBs are newly added or modified:

- CISCO-LWAPP-QOS-MIB.my
- CISCO-LWAPP-DOT11-MIB.my
- AIRESPACE-WIRELESS-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, 9800-CL, CW9800M, and CW9800H1/H2). 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: We are 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) and other channels 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

Behavior Change for Cisco IOS XE 17.17.1

- From this release, the show memory leak packet and debug memory leak packet commands are not supported.
- You can set the Cisco Catalyst 9166 AP XOR 5/6-GHz radio slot 2 to 6-GHz, even if 6-GHz is not supported in the country and slot 2 is disabled. This allows the AP to use the full band (channels 36 to 173) in 5-GHz slot1.
- The **ip proxy-arp** configuration is disabled by default under VLAN interfaces for the controller.

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.

Important Notes

Description: Cisco Wireless Series APs encounter WCPD crash due to memory leak in the RRM module.

WCPD crash is seen in AP platforms with scan radio, where FastLocate or Hyperlocation is enabled along with **All Channels** in RRM. This issue is seen in Cisco Wireless 9176D1, 9176I, 9178I, 9172I Series APs and Cisco Catalyst 9163 Series APs.

Workaround: Address radio availability status post recovery or re-configuration.

Supported Hardware

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

Table 3: 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.

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 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.
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.

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

Table 4: Supported Host Environments for Public and Private Cloud

Host Environment	Software Version
VMware ESXi	
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
GCP	GCP marketplace
Microsoft Hyper-V	Windows Server 2019, 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 5: 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

The following table lists the supported SFP models.

Table 6: 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	—	—	—	—	—

SFP Name	C9800-80-K9	C9800-40-K9	C9800-L-F-K9	CW9800H1	CW9800H2	CW9800M
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	—
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	—

SFP Name	C9800-80-K9	C9800-40-K9	C9800-L-F-K9	CW9800H1	CW9800H2	CW9800M
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-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-H25G-CU1M	—	—	—	Supported	—	Supported
SFP-H25G-CU5M	—	—	—	Supported	—	Supported

SFP Name	C9800-80-K9	C9800-40-K9	C9800-L-F-K9	CW9800H1	CW9800H2	CW9800M
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- CU1.5M	Supported	Supported	Supported	—	—	—
SFP-H10GB-CU1M	Supported	Supported	Supported	Supported	Supported	Supported
SFP-H10GB-CU2.5M	Supported	Supported	Supported	—	—	—
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	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/c/en/us/support/interfaces-modules/transceiver-modules/products-device-support-tables-list.html

Network Protocols and Port Matrix

Table 7: 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
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.

Source	Destination	Protocol	Destination Port	Source Port	Description
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	TCP	32626	Any	Intelligent capture and RF telemetry
AP	AP	UDP	16670	Any	Client Policies (AP-AP)
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

Source	Destination	Protocol	Destination Port	Source Port	Description
Cisco Catalyst 9800 Series Wireless Controller	NTP Server	UDP	123	Any	NTP
Cisco Catalyst 9800 Series Wireless Controller	Syslog Server	UDP	514	Any	SYSLOG
AP	Cisco Catalyst 9800 Series Wireless Controller	HTTPS	8443	Any	Out of Band AP Image Download Cisco CleanAir Spectral Capture
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
Cisco Catalyst Center	Cisco Catalyst 9800 Series Wireless Controller	TCP	32222	Any	Device Discovery
Cisco Catalyst Center	Cisco Catalyst 9800 Series Wireless Controller	TCP	25103	Any	Telemetry Subscriptions

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 9136AX 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 Wireless 9172 (I) Series Wi-Fi 7 Access Points
- Cisco Wireless 9172 (H) Series Wi-Fi 7 Access Points
- Cisco Wireless 9176 (I/D1) Series Wi-Fi 7 Access Points
- Cisco Wireless 9178 (I) Series Wi-Fi 7 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 Aironet 1570 (I/D/E) 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 9165E Rugged Access Point
- Cisco Catalyst Industrial Wireless 9165D Heavy Duty Access Point

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

- Cisco Wi-Fi Interface Module (WIM)

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. For more information, see Cisco Wireless Solutions Software Compatibility Matrix

Table 8: Compatibility Information

Cisco Catalyst 9800 Series Wireless Controller Software	Cisco Identity Services Engine	Cisco Prime Infrastructure	Cisco AireOS-IRCM Interoperability	Cisco Catalyst Center	Cisco CMX
IOS XE 17.17.1	3.4 3.3 3.2 3.1 3.0 2.7 * all with latest patches	3.10.6 security update 02 (base version) **Note** Base release of Cisco Prime Infrastructure that supports corresponding Cisco Catalyst 9800 Series Wireless Controller platform release and its features.	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	11.1.0 11.0.1 11.0.0 10.6.3

GUI System Requirements

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

Table 9: 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: 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:

- When you upgrade from Cisco IOS XE 17.9.5 or 17.12.2 to Cisco IOS XE 17.15.x, the controller WebUI does not support images greater than 1.5 GB.

  Workaround:

  - Upgrade using the CLI commands, or,
  - Upgrade to a fixed release first, and then upgrade to 17.15.x.

- Kernel panic is observed in CW9176 while disabling few of the associated clients.
- Kernel panic is observed in CW9176 and CW9178 during configuration change, after the initial bootup.

  After upgrading the controller image, the AP joins the controller and reboots. Kernel panic is observed when the policy tag is changed for the first time. This is seen only the first time after build upgrade.

- When you upgrade from Cisco IOS XE Dublin 17.12.3 to 17.12.4 or Cisco IOS XE 17.15.1, the Cisco Catalyst Wi-Fi 6 APs fail to upgrade the AP image.

  Workaround:

  - Reboot the impacted APs through the power cycle.

  For more information, see CSCwm08044

⚠ **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, 17.14.x, and 17.15.x:

- **Cisco Aironet 1570 Series Access Point**
- **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.

- 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.

- The Cisco Centralized Key Management (CCKM) feature was deprecated in Cisco IOS XE 17.10.x, but currently remains supported. However, support for CCKM will be removed in a future release. Therefore, we recommend that you migrate to Fast Transition (FT) with 802.1X authentication and validate the configuration with supported key caching mechanisms.
- 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 17.17.x

Table 10: Upgrade Path to Cisco IOS XE Dublin 17.17.x

Current Software	Upgrade Path for Deployments with 9130 or 9124	Upgrade Path for Deployments Without 9130 or 9124
16.10.x	—[4]	Upgrade first to 16.12.5 or 17.3.x and then to 17.17.x.
16.11.x	—	Upgrade first to 16.12.5 or 17.3.x and then to 17.17.x.
16.12.x	Upgrade first to 17.3.5 or later or 17.6.x or later, then to 17.9.6 or later or 17.12.x or later, and then to 17.17.x.	Upgrade first to 17.3.5 or later or 17.6.x or later, and then to 17.17.x.
17.1.x	Upgrade first to 17.3.5 or later, then to 17.9.6 or later or 17.12.x or later, and then to 17.17.x.	Upgrade first to 17.3.5 or later and then to 17.17.x.
17.2.x	Upgrade first to 17.3.5 or later, then to 17.9.6 or later or 17.12.x or later, and then to 17.17.x.	Upgrade first to 17.3.5 or later and then to 17.17.x.
17.3.1 to 17.3.4	Upgrade first to 17.3.5 or later or 17.6.x or later, then to 17.9.6 or later or 17.12.x or later, and then to 17.17.x.	Upgrade directly to 17.17.x.
17.3.4c or later	Upgrade to 17.9.6 or later or 17.12.x or later, and then to 17.17.x.	Upgrade directly to 17.17.x.
17.4.x	Upgrade first to 17.6.x and then to 17.17.x.	Upgrade directly to 17.17.x.
17.5.x	Upgrade first to 17.6.x and then to 17.17.x.	Upgrade directly to 17.17.x.
17.6.x	Upgrade to 17.9.6 or later or 17.12.x or later, and then to 17.17.x.	Upgrade directly to 17.17.x.
17.7.x	Upgrade to 17.9.6 or later or 17.12.x or later, and then to 17.17.x.	Upgrade directly to 17.17.x.
17.8.x	Upgrade to 17.9.6 or later or 17.12.x or later, and then to 17.17.x.	Upgrade directly to 17.17.x.

Current Software	Upgrade Path for Deployments with 9130 or 9124	Upgrade Path for Deployments Without 9130 or 9124
17.9.1 to 17.9.5	Upgrade to 17.9.6 or later or 17.12.x or later, and then to 17.17.x	Upgrade directly to 17.17.x
17.9.6 or later	Upgrade directly to 17.17.x	Upgrade directly to 17.17.x
17.10.x	Upgrade to 17.12.x or later, and then to 17.17.x	Upgrade directly to 17.17.x
17.11.x	Upgrade to 17.12.x or later, and then to 17.17.x	Upgrade directly to 17.17.x
17.12.x	Upgrade directly to 17.17.x	Upgrade directly to 17.17.x
17.13.x	Upgrade directly to 17.17.x	Upgrade directly to 17.17.x
17.14.x	Upgrade directly to 17.17.x	Upgrade directly to 17.17.x
17.15.x	Upgrade directly to 17.17.x	Upgrade directly to 17.17.x
17.16.x	Upgrade directly to 17.17.x	Upgrade directly to 17.17.x
8.9.x or any 8.10.x version prior to 8.10.171.0	Upgrade first to 8.10.171.0 or later, 17.3.5 or later or 17.6.x or later, then to 17.9.6 or later or 17.12.x or later, and then to 17.17.x	Upgrade directly to 17.17.x.

[4] 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 17.17.x
- **Image Names (9800-80, 9800-40, and 9800-L)**:
  - C9800-80-universalk9_wlc.17.17.x.SPA.bin
  - C9800-40-universalk9_wlc.17.17.x.SPA.bin
  - C9800-L-universalk9_wlc.17.17.x.SPA.bin
- **Image Names (9800-CL)**:
  - **Cloud**: C9800-CL-universalk9.17.17.x.SPA.bin
  - **Hyper-V/ESXi/KVM**: C9800-CL-universalk9.17.17.x.iso, C9800-CL-universalk9.17.17.x.ova
  - **KVM**: C9800-CL-universalk9.17.17.x.qcow2
  - **NFVIS**: C9800-CL-universalk9.17.17.x.tar.gz

Software Installation Commands

Cisco IOS XE 17.17.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

Cisco Wireless Licences

Cisco Wireless licenses, a part of the Cisco Networking Subscription licensing model, is a software license that helps you to deploy your Wi-Fi 7 Access Points in an on-premise, hybrid, or a cloud managed network. From Cisco IOS XE 17.15.2, Cisco Wireless licenses are supported on Wi-Fi 7 Access Points (APs) and later models.

The Cisco Wireless licenses consist of the following tiers:

- **Cisco Wireless Essentials**: The tier that provides fundamental features and functionalities that are essential to manage a network.
- **Cisco Wireless Advantage**: The tier that supports additional features and capabilities, and includes all the essential capabilities in addition to the advanced capabilities to manage a network.

For more information, see Cisco Wireless Licensing.

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 11: Test Configuration for Interoperability

Hardware or Software Parameter	Hardware or Software Type
Release	Cisco IOS XE 17.17.x
Cisco Wireless Controller	See Supported Hardware, on page 8.
Access Points	See Supported APs, on page 16.
Radio	• 802.11ac • 802.11a • 802.11g • 802.11n • 802.11be (Wi-Fi 7)
Security	Open, PSK (WPA2-AES), 802.1X (WPA2-AES) (EAP-FAST, EAP-TLS)
RADIUS	See Compatibility Matrix, on page 18.
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 12: 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
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)

Client Type and Name	Driver or Software Version
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
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

Client Type and Name	Driver or Software Version
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	VG3.0
Drager M300.4	VG3.0
Drager M540	VG4.2
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

Client Type and Name	Driver or Software Version
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
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

Client Type and Name	Driver or Software Version
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	
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
PhoenixContact FL WLAN 2010	Firmware version: 2.71

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 17.17.1

Identifier	Headline
CSCwn18885	Cisco Catalyst 9136 series APs encounter kernel unresponsiveness with last reload reason 'unknown'
CSCwn36778	Cisco Catalyst 9800-80 controller displays low memory leak potentially in the 'ipv4_addr' field
CSCwn83970	Cisco Catalyst 9162 AP does not respond to open authorization request on 5-GHz band
CSCwn92827	Secondary controller fails with rsync error
CSCwo04380	Cisco Catalyst 9162 AP's beacons get stuck on Radio 1 after upgrading to 17.12.4.158
CSCwo35645	NETCONF over SSH fails to return all the records for wireless-client-oper and shows 'invalid XML' before everything is returned
CSCwo38789	Cisco Catalyst 9176 AP encounters watchdog reset (WCPD) kernel unresponsiveness due to memory leak in RRM module
CSCwo44274	Cisco Catalyst 9115 AP does not answer association requests in 17.12.4 + APSP4
CSCwo48783	SSIDs stop broadcasting and drop clients from network after pushing telemetry updates from Catalyst Center to controller
CSCwk53741	Anchor controller drops mobility tunnel even when keepalive timers aren't hit
CSCwn33501	Controller connected to the AP does not give any output while executing the #show ap summary sort name command
CSCwn42563	Controller experiences kernel unresponsiveness on WNCD process on 17.9.4

Identifier	Headline
CSCwn76129	Controller fails to handle loadbalance discovery message and stale AP entries are seen
CSCwn79857	Cisco Catalyst 9130 AP URL with multiple IPs does not work in FlexConnect local switching
CSCwn83397	Wired Mesh AP (MAP) client flaps between VLAN 0 and numbered native VLAN on Root AP (RAP)
CSCwn94159	Controller with 6 GHz support AP's radio channel bandwidth changes due to DCA happening frequently
CSCwo04476	Cisco Catalyst 9130AX AP experiences kernel unresponsiveness
CSCwo05017	Cisco Catalyst 9162 AP undergoes unbounded/tmp causing OOM reset
CSCwo07767	Controller's active chassis get stuck in active recovery state on 17.12.4
CSCwo13339	Cisco Catalyst 9130 AP experiences kernel unresponsiveness due to OOM
CSCwo16038	Cisco Catalyst 9124 WGB becomes unreachable after connecting to Cisco Aironet 2800 Root AP (RAP) when WMM is disabled
CSCwo19011	Controller SISF undergoes kernel unresponsiveness with WNCD core
CSCwo19025	Cisco Catalyst 9166D AP reports high channel utilization
CSCwo20395	Controller's rogue classification rules do not apply configured classifications
CSCwo30925	Cisco Wi-Fi 6 and above APs do not support disabling WMM on radios that support 802.11n/11ac/11ax operation
CSCwo32255	Anchor controller's AVC statistics show in the controller's CLI but not in the Web UI
CSCwo37156	Cisco Catalyst IW9167I AP does not derive geolocation data from neighbor AP
CSCwo37680	Controller initiates client deletion with code: CO_CLIENT_DELETE_REASON_DOT11_MAX_STA
CSCwo37756	Cisco Aironet 1815t AP does not receive an internal DHCP IP address when connected to LAN3
CSCwo38070	Controller display mismatch in Guest OS on ESXi
CSCwo38719	APs in controller running 17.12.4 drop post a switchover and during HA sync
CSCwo41248	Controller display wrong message when configuring 2 radios on the same UNII band (100 - 144)
CSCwo41946	Cisco Catalyst 9130 APs experiences kernel unresponsiveness with SLUB enabled
CSCwo43599	Cisco Catalyst CW9162I-E AP's beacon intermittently misses all WLANs, resulting in no client join

Identifier	Headline
CSCwo43801	AP duplicates DHCP request packets when using FlexConnect mode with Central Switching WLAN
CSCwo45788	Controller running 17.9.5 version generates system report and CCP core file
CSCwo46493	Cisco Catalyst 9136 AP encounters dual ethernet failover reboots
CSCwo50044	HA does not form after reload triggered by SMU installs

Resolved Issues for Cisco IOS XE 17.17.1

Identifier	Headline
CSCwn06222	Cisco Catalyst IW9167 wired 1 interface is not functioning with non 1-Gbps clients via GLC-T-RGD SFP Module
CSCwo36407	WGB mode sets incorrect transmit power values after receiving a beacon with CSA IE from a non-associated AP
CSCwm53286	Controller unable to reach terminal redundancy state while performing ISSU
CSCwj84377	Client detail for 'Associated' Client does not display some info element when using Cisco Spaces with Connector
CSCwk24352	Wireless clients are unable to receive the splash page and gets stuck due to webauth requirement
CSCwk39866	Client page is stuck in loading state
CSCwk58326	Controller sends multicast packets with previous WMI
CSCwk64840	Controller unexpectedly reboots due to memory depletion due to mobility process
CSCwk71592	Intermittent multicast and unicast traffic encounter failure post roaming on an IRCM testbed with mobility enabled
CSCwk81946	Controller experiences kernel unresponsiveness due to tdl memory corruption
CSCwk84121	Local switching clients are assigned to Zone ID 0 when IP overlap is configured and FlexConnect VLAN central switching
CSCwm03016	Controller experiences kernel unresponsiveness abnormally pointing to client_orch
CSCwm28021	Configurations are removed from APs after ISSU upgrade from Cisco IOS XE Dublin 17.12.4 to Cisco IOS XE Amsterdam 17.1.5.1
CSCwm29051	Controller experiences kernel unresponsiveness two times due to Critical process WNCd fault on rp_0_0 (rc=139)
CSCwm29437	Controller reboots handling AP radio payloads due to Critical process wncd fault on rp_0_0 (rc=139)
CSCwm36607	Controller displays fman_rp memory leak in FMAN_RP_DB at /tmp/rp/tdldb
CSCwm40646	Clients stuck in IP learning state as DHCP option 82 field is left empty with EoGRE tunnel enabled

Identifier	Headline
CSCwm48283	Controller is stuck in internal-error state after upgrade to HP5
CSCwm67254	Accounting start and stop messages are missing CUI attributes
CSCwm67710	Cisco Catalyst 9800-80 controller encounters critical process WNCd failure (rc 0)
CSCwm73020	Controller relays unicast DHCP requests
CSCwm74071	Controller encounters kernel unresponsiveness due to client being stuck in 802.11r preauth and BSSID/AP going down at the same time
CSCwm86679	Cisco Catalyst 9800-40 controllers encounter kernel unresponsiveness and reboot unexpectedly at rogue_start_containers
CSCwm89346	Controller encounters kernel unresponsiveness post telemetry update from Cisco Catalyst Center
CSCwn06627	Controller encounters kernel unresponsiveness with geolocation config pointing towards geo_cloudm_graph_shortest_path
CSCwn10992	DTLS timeout because of improper client load balancing
CSCwn13406	Controller RA trace fails to stop, displaying can't read "strr": no such variable
CSCwn15048	Replace Expansion Module's SN field with empty value before sending invalid characters to Cisco Catalyst Center
CSCwn26561	Sequence number missed on NMSPD for RFID measurement during RFID stats collection window
CSCwn35094	Cisco Catalyst 9500 Switch encounters kernel unresponsiveness while profile download
CSCwn36115	iPhone 16 device listed as unclassified in the iOS 18.0.1
CSCwn46684	Controller unexpectedly reloads and becomes unresponsive during the upgrade process
CSCwn51207	Cisco Catalyst 9800-40 controller encounters kernel unresponsiveness after upgrade from 17.3.6 to 17.12.3ESW05
CSCwn61980	Rogue AP fails to connect with UI/Rest AP when detected by a dual band radio AP
CSCwn77030	Controller is not processing analytics action frames received from MLD for MLO clients
CSCwn83626	Client is stuck in association while changing WLAN from central switching profile to local profile
CSCwn90360	Controller is unable to start EAP process due to the delay of packet transmission from AP
CSCwn90874	Guest anchor controller shows error message when creating anchor-export-ACK
CSCwn92477	Controller unexpectedly reboots during WNCd process due to assertion failed with invalid BSSID
CSCwn98574	Corrupt vrf name causes client to frequent disconnects and get stuck at mobility while roamining
CSCwn99763	Noise floor value is always displayed as 0 for a few x-paths

Identifier	Headline
CSCwo02178	FT-SAE clients fails to roam between controller in same mobility group due to PMKID mismatch
CSCwo39523	Cisco Wireless 9176I AP receives GPS/GNSS data but it is not provisioning country code
CSCwi48178	Cisco Catalyst 9800-40 controller displays WNCd error in SafeC Validation for memcmp_s: dmax
CSCwj96788	Controller accepts only multicast IPv6 address which starts on ff00
CSCwk52366	Controller encounters fix flow control display issue
CSCwk70598	Event-Driven RRM is unresponsive on 6-GHz band
CSCwk77862	AP does not disjoin automatically when the AP-name is changed in the Regex filter
CSCwk94110	NMSP config related timers are not initialised post process restart
CSCwm00075	DCA cycle runs for 900 seconds in 5 GHz band even though the algorithm interval is set to 600 seconds
CSCwm08261	Controller RADSEC fix using a Samsung device displays wrong Acct-Terminate-Code when manually disabling Wi-Fi
CSCwm14401	Controller experiences an unexpected reset of WNCd
CSCwm28542	OKC roam fails after a brief WAN drop
CSCwm31586	AP in FlexConnect mode reports an erroneous client count
CSCwm35342	Controllers logs daily errors for WNCd with no operational impact
CSCwm36501	Controller encounters kernel unresponsiveness due to TLB miss
CSCwm40875	Controller is unable to fetch DNS entries for DNS with VRF
CSCwm48458	Detecting radar on 5 GHz CH100 causes controller to mismatch to CM66 and switch dual mode from 6 GHz to 5 GHz
CSCwm57534	Controller experiences kernel unresponsiveness due to Critical process WNCd fault
CSCwm76794	Creating a VRF with double quotes causes pages associated with VRF to not list any VRF
CSCwm80472	Controller's UI and CLI fail to delete a mobility peer due to 'invalid transversal ctx for walker next rec'
CSCwm88527	New username consisting of string "ipassword" or "isecret" throw multiple issues
CSCwm92779	Cisco Catalyst Center client assurance dashboard shows no data for average latency
CSCwm93080	IP address of the TACACS server disappears when the GUI timeout is changed
CSCwm96234	WebUI fails when special character combinations are used in the login banner on the device's general page
CSCwm98000	Cisco Catalyst 9105 AP displays Short Preamble "Allowed" but then rejects association with SP "Not Allowed"

Identifier	Headline
CSCwn00375	Controller does not generate AP disjoin event message syslog after the AP is disconnected
CSCwn05795	Cisco Catalyst 9120AXI-I AP's 2.4-GHz band does not activate due to a 'Regulatory domain check failed' error
CSCwn10016	Default DHCP lease time option is not visible in the controller's GUI
CSCwn14199	Controller reloads unexpectedly while deleting an object from client database
CSCwn16547	CSR pop does not appear on the controller's GUI while trying to generate it
CSCwn20875	Re-authentication is required of guest users prior to sleeping client timeout
CSCwn34998	6 GHz radios move from LP to SP mode after ranging due to neighbor loss
CSCwn39428	Error message "Flow Monitor is Required" is shown even flow monitor name is available
CSCwn45000	There is no output for "show ap name < AP Name > wlan dot11 5ghz" command
CSCwn45670	Controller GUI FlexConnect configuration page fails after upgrade to Cisco IOS XE 17.15.1
CSCwn85374	Memory usage is increasing in the CloudM process
CSCwn93586	9176 AP is operating in XOR mode, Channel and CW changes are not pushed post the DCA cycle
CSCwn94511	The `factory-reset all` command is unsecure but functions as if it has a secure option
CSCwo00821	IoT Orchestrator is unable to start after an upgrade or a reload
CSCwo09824	Cisco Wireless 9176 AP unable to join controller after GUAP
CSCwo21938	AFC is using manual geolocation co-ordinates
CSCwo29017	wncmgrd kernel unresponsiveness after issue command \u2018show ap config slots\u2019
CSCwo35816	After IoT Orchestrator Day 0 onboarding, the gRPC channels are not coming up
CSCwn17412	The FlexConnect local switching traffic is centralized randomly during a web-auth SSID
CSCwj84554	IOx app installation fails due to incorrect mounting
CSCwj91255	Cisco Catalyst 9120AXI-E AP does not acknowledge frames sent from iOS devices
CSCwk12169	Cisco Catalyst 9105/9115/9120 AP fails for clients connected in 5G slot
CSCwk26966	Cisco Aironet 3802 AP displays false radar detection only on UNI-II after upgrading the software
CSCwk79057	AP does not failover to the RADIUS server in FlexConnect Local Switching Local Authentication
CSCwk82371	Cisco Catalyst 9120AXI-S AP does not detect the RFIDs in Monitor mode
CSCwk98117	Cisco Catalyst 9166D APs are unable to transmit NDP packets over the air

Identifier	Headline
CSCwm07499	Cisco Catalyst 91xx AP does not rotate awipsd.log causing an upgrade issue "tar: write error: No space left on device"
CSCwm08044	APs do not upgrade without a power cycle displaying error: unlzma: write: No space left on device
CSCwm31864	Cisco Wave APs experience kernel unresponsiveness due to memory leak reason OOM
CSCwm38838	Cisco Catalyst 9136 AP's awipsd.log grows in /tmp/var/log causing "tar: write error: No space left on device"
CSCwm49467	FlexConnect APs disable u-APSD in the assoc request if clients don't have it enabled
CSCwm52551	Cisco Catalyst 9124 AP in FlexConnect mode with the FlexConnect EoGRE tunnel enabled leaves the Option 82 field unfilled
CSCwm58430	Cisco Catalyst 9115 AP experiences kernel unresposiveness due to: Beacon Stuck Reset Radio
CSCwm66129	Cisco Wave 2 APs 2800, 3800, and 4800 display duplicate entries for stale clients in the Wi-Fi driver
CSCwm79348	IOX-APP fails to detect USB and is stuck in the activate state
CSCwn03468	Clients encounter slow speeds while connecting to slot 2 operating in the 5-GHz band on CM66
CSCwn09549	Cisco Catalyst 9124 MAP fails to join and intermittently disconnects with Cisco Catalyst 9124 RAP
CSCwn10606	Cisco Catalyst 9120 AP fails to report RFID packets to the controller intermittently
CSCwn44287	Multiple Cisco Wave 2 and Cisco Catalyst APs detect CAPWAPd cores
CSCwn48861	Cisco Catalyst IW9167E AP unexpectedly displays reduced Transmit power on 2.4GHz in -Z Regulatory Domain
CSCwn52205	AP remains stuck in the activate state without progressing to RUN when IOX-APP starts before USB detection
CSCwn66225	Invalid Tx power on beacon frame causes disconnect for iPhone and Mac laptop users
CSCwn81268	IOX-APP using USB in RUN state ends up in activated state after switch reload
CSCwn82037	Cisco Catalyst 9120 AP fails to report RFID packets to the controller intermittently
CSCwn87525	Cisco Catalyst 917X APs Wi-Fi 7 MLO clients drop DS traffic due to 5ghz channel change during CAC
CSCwo04318	Cisco Catalyst IW9167EH-F Mesh AP (MAP) watchdog reset (WCPD) experiences kernel unresponsiveness while using wireless backhaul

Identifier	Headline
CSCwo13129	Cisco Catalyst 9176D AP's UART msm experiences kernel unresponsiveness during DMA activity
CSCwj03060	Cisco Aironet 1815w AP encounters kernel unresponsiveness on image version 17.9.4.205
CSCwj66264	Cisco Catalyst 9300 and 9400 switches' mGig port displays half-duplex mismatch messages
CSCwj69642	Cisco Catalyst 9166 APs stop forwarding traffic for some seconds
CSCwj72174	Cisco Aironet 2800 AP connected to the same controller detects other connected 2800 APs as rogue
CSCwk77222	Cisco Aironet 2802 AP encounters kernel unresponsiveness after upgrading to 17.9.5.47
CSCwk80486	APs mark own BSSID as rogue in 2.4 GHz and in 5 GHz
CSCwk93880	Cisco IW-6300H-AC-E-K9 APs encounter kernel unresponsiveness due to FIQ/NMI reset
CSCwm00078	Cisco Catalyst 9136 AP sends M5 with incorrect index 0, resulting in Apple Macbooks not responding
CSCwm04379	Cisco Catalyst 9115AX displays BcmRadioStats error : Failed to add multicast MAC address for RRM as dot11_client entry
CSCwm34600	AAA override VLAN does not apply upon roaming in FlexConnect local authentication
CSCwm37410	Cisco Catalyst 9120 AP does not forward large packets when MTU=1500
CSCwm49168	Cisco Catalyst 9164I-ROW AP VAP driver drops EAP identity requests packet intermittently
CSCwm50811	AP displays BSSID as rogue intermittently, causing the control packet to be considered for impersonation detection
CSCwm61128	AAA override VLAN is not used for FT 11R roam-in local authentication
CSCwm65107	Cisco Catalyst 9130 AP encounters kernel unresponsiveness due to OOM
CSCwm73271	Cisco Wave 2 AP does not send syslog messages if the receiver is using an IPv6 address
CSCwn08479	Cisco Catalyst 9120 Wi_Fi 6 AP experiences kernel unresponsiveness due to wlc_bsscfg_find_by_target_bssid+0xb8/0xe0
CSCwn14495	Cisco Catalyst 91XX AP detects its own BSSID as rogue
CSCwn15002	Cisco Catalyst 9120 AP encounters kernel unresponsiveness at wlc_low_txq_enq
CSCwn43094	Locally switched RLAN clients info is unavailable in controller client table
CSCwn48978	AP incorrectly send ARP requests for the DHCP IP address even after a DHCP release packet

Identifier	Headline
CSCwn55534	IP theft is observed on the controller when the client receives a second DHCP offer following DORA
CSCwn96529	Cisco Catalyst 9136I-ROW AP in Site-Survey mode cannot add country code "IN"
CSCwn99070	Cisco Catalyst 9105 AP does not generate radio core properly

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 Series Wireless Controller Data Sheets

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

Cisco Embedded Wireless Controller on Catalyst Access Points

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

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

Wireless Product Comparison

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

Cisco Access Points–Statement of Volatility

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

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

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

Cisco Prime Infrastructure

Cisco Prime Infrastructure Documentation

Cisco Connected Mobile Experiences

Cisco Connected Mobile Experiences Documentation

Cisco Catalyst Center

Cisco Catalyst Center Documentation

Communications, services, and additional information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business 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.