Release Notes for Cisco Catalyst 9800 Series Wireless Controller, Cisco IOS XE 17.16.x

First Published: 2024-12-11

Release Notes for Cisco Catalyst 9800 Series Wireless Controller, Cisco IOS XE 17.16.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
  - Cisco Catalyst 9800-80, Catalyst 9800-40, and Catalyst 9800-L Wireless Controllers
  - Cisco Catalyst CW9800H1 and CW9800H2 Wireless Controllers
  - Cisco Catalyst CW9800M Wireless Controller
- 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 17.16.1

Important

- Cisco Wireless Embedded Wireless Controller (EWC) on Access Point will not be supported from Cisco IOS XE 17.16.1 onwards, as Cisco announces the end-of-sale and end-of-life dates for the Cisco Wireless Embedded Wireless Controller (EWC) on Access Point. Cisco IOS XE 17.15.x will be the final IOS-XE software supporting EWC-AP.

  EWC running on Catalyst switches in Software Defined Access (SDA) mode will continue to be supported.

  For more information, see https://www.cisco.com/c/en/us/products/collateral/wireless/embedded-wireless-controller-catalyst-access-points/wireless-ewc-access-point-eol.html.

- Cisco Wireless Wi-Fi 7 Access Points are not supported in Cisco IOS XE 17.16.1.
- Cisco Network Subscription is not supported in Cisco IOS XE 17.16.1: Cisco Wireless licenses, a part of the Cisco Networking Subscription licensing model, is not supported in Cisco IOS XE 17.16.1.

Table 1: New and Modified Software Features

Feature Name	Description and Documentation Link
CLI Support to Display Configured Trustpoint for NETCONF Yang.	The **show netconf-yang ssh trustpoint** was introduced to display the certificate used by NETCONF over SSH session. For more information, see *Programmability Command Reference Guide*.
Cloud Monitoring: Support for System Failover/Switchover Count and RP Status to Meraki dashboard in Operational Telemetry	In this release, the controller provides system failover or switchover count to Meraki dashboard in operational telemetry.

Feature Name	Description and Documentation Link
Support for 10 Mbps Speed Port on Cisco IW9167EH WGB	This feature supports 10 Mbps speed on the wired Ethernet 0 ports of the Cisco Catalyst IW9167EH Workgroup Bridge (WGB) AP. It allows existing 10 Mbps Ethernet devices to connect to the IW9167EH WGB APs. For more information, see *10 Mbps Speed Port Support on Cisco IW9167EH WGB*
Port Address Translation on WGB AP	This feature enables you to configure and manage the Port Address Translation (PAT) on the WGB AP. When configured, PAT on the WGB AP translates a host device's IP address and TCP or UDP port number into unique public IP addresses and their respective TCP or UDP port numbers. PAT configuration supports both upstream and downstream data flow. The feature is supported on the following APs: • Cisco Catalyst IW9165E Rugged Access Point • Cisco Catalyst IW9167E Heavy Duty Series Access Points For more information, see Port Address Translation on WGB AP on *Cisco Catalyst IW9165E Rugged Access Point and Wireless Client Configuration Guide* and *Cisco Catalyst IW9167E Heavy Duty Access Point Configuration Guide*.
Port Address Translation on uWGB AP	This feature enables you to configure and manage PAT on the Universal WGB (uWGB) AP. When configured, PAT on the uWGB AP translates a host device's IP address and TCP or UDP port number into unique public IP addresses and their respective TCP or UDP port numbers. The PAT configuration supports both upstream and downstream data flow. The feature is supported on the following APs: • Cisco Catalyst IW9165E Rugged Access Point • Cisco Catalyst IW9167E Heavy Duty Series Access Points For more information, see Port Address Translation on WGB AP on *Cisco Catalyst IW9165E Rugged Access Point and Wireless Client Configuration Guide* and *Cisco Catalyst IW9167E Heavy Duty Access Point Configuration Guide*

MIBs

The following MIBs are newly added or modified:

- AIRESPACE-WIRELESS-MIB.my
- CISCO-LWAPP-DOT11-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

- Fast Transition Adaptive is not supported for WPA3 SAE.
- Cisco Wireless Wi-Fi 7 Access Points are not supported in Cisco IOS XE 17.16.1.
- Reducing duplicate information for AP configuration and AP slot configuration commands: The output for **show ap config slots** and **show ap config general** commands are duplicate. To reduce the duplicate output, the **show ap config slots** command is modified to display only the per AP general information.
- When a country using channels 1, 5, 9, and 13 is added to the controller, the 2.4-GHz RF profiles automatically update to include these channels, leading to inconsistencies. The behaviour is observed in Cisco IOS XE Amsterdam 17.3.x, Cisco IOS XE Bengaluru 17.6.x, and Cisco IOS XE Cupertino 17.9.x.

  To avoid this behavior, the RF profiles are adjusted manually for countries supporting additional channels.
- You can allow the 5-GHz or 6-GHz XOR radio to move to 6GHz:
  - When the 6-GHz network is enabled.
  - When the **Regulatory Domain Allowed by Country** is 6GHz.

Note This does not apply when the Flexible Radio Assignment (FRA) configuration is enabled.

- The IP overlap feature supports FlexConnect VLAN-based central switching.
- The Security Group Access Control List (SGACL) logging records are generated and managed through an internal High-Speed Logging (HSL) server. These records are then sent to a Syslog server under the following conditions:
  - A packet hits a logging access control entry (ACE).
  - The Cisco TrustSec role-based policy is enabled.
- The Unscheduled Automatic Power Save Delivery (U-APSD) can now be configured to be enabled or disabled in the probe, beacon, and association response.
- From this release, it is not possible to disable the 802.11h channel switch. The channel switch announcements (CSA) remain enabled at all times because they help clients when the APs announce the change from the current channel to a new channel, thereby reducing the number of reconnections.
- The **wgb multicast-foreign-forward** command is applicable when Workgroup Bridges (WGB) roams from AireOS controller to Cisco Catalyst 9800 Wireless Controller.

Note Ensure that the mobility tunnel is correctly configured.

By configuring this command, the wired clients connected to the WGB can receive multicast traffic, ensuring seamless connectivity and data flow during the roaming process.

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 6.5, 6.7, 7.0, and 8.0 • VMware ESXi vCenter 6.5, 6.7, 7.0, and 8.0
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 Server 2019, and Windows Server 2016 (Version 1607) with Hyper-V Manager (Version 10.0.14393)
Microsoft Azure	Microsoft Azure
Oracle Cloud Infrastructure (OCI)	Oracle Cloud Infrastructure (OCI)

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	—	—	—	—	—

SFP Name	C9800-80-K9	C9800-40-K9	C9800-L-F-K9	CW9800H1	CW9800H2	CW9800M
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	—
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 Name	C9800-80-K9	C9800-40-K9	C9800-L-F-K9	CW9800H1	CW9800H2	CW9800M
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-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 Name	C9800-80-K9	C9800-40-K9	C9800-L-F-K9	CW9800H1	CW9800H2	CW9800M
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	TCP	32626	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
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 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 Industrial Wireless 9167 (I/E) Heavy Duty Access Points
- Cisco Catalyst Industrial Wireless 9165E Rugged 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 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 CMX
IOS XE 17.16.1	3.4 3.3 3.2 3.1 3.0 2.7 * all with latest patches	3.10.6 (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	11.0 10.6.3

GUI System Requirements

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

Table 8: 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 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.

-

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.

- 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 17.16.x

Table 9: Upgrade Path to Cisco IOS XE Dublin 17.16.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 17.16.x.
16.11.x	—	Upgrade first to 16.12.5 or 17.3.x and then to 17.16.x.
16.12.x	Upgrade first to 17.3.5 or later or 17.6.x or later, and then to 17.16.x.	Upgrade first to 17.3.5 or later or 17.6.x or later, and then to 17.16.x.
17.1.x	Upgrade first to 17.3.5 or later and then to 17.16.x.	Upgrade first to 17.3.5 or later and then to 17.16.x.
17.2.x	Upgrade first to 17.3.5 or later and then to 17.16.x.	Upgrade first to 17.3.5 or later and then to 17.16.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 17.16.x.	Upgrade directly to 17.16.x.
17.3.4c or later	Upgrade directly to 17.16.x.	Upgrade directly to 17.16.x.
17.4.x	Upgrade first to 17.6.x and then to 17.16.x.	Upgrade directly to 17.16.x.
17.5.x	Upgrade first to 17.6.x and then to 17.16.x.	Upgrade directly to 17.16.x.
17.6.x	Upgrade directly to 17.16.x.	Upgrade directly to 17.16.x.
17.7.x	Upgrade directly to 17.16.x.	Upgrade directly to 17.16.x.
17.8.x	Upgrade directly to 17.16.x.	Upgrade directly to 17.16.x.
17.9.x	Upgrade directly to 17.16.x	Upgrade directly to 17.16.x
17.10.x	Upgrade directly to 17.16.x	Upgrade directly to 17.16.x
17.11.x	Upgrade directly to 17.16.x	Upgrade directly to 17.16.x
17.12.x	Upgrade directly to 17.16.x	Upgrade directly to 17.16.x
17.13.x	Upgrade directly to 17.16.x	Upgrade directly to 17.16.x
17.14.x	Upgrade directly to 17.16.x	Upgrade directly to 17.16.x
17.15.x	Upgrade directly to 17.16.x	Upgrade directly to 17.16.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 17.16.x	Upgrade directly to 17.16.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 17.16.x
- **Image Names (9800-80, 9800-40, and 9800-L)**:
  - C9800-80-universalk9_wlc.17.16.x.SPA.bin
  - C9800-40-universalk9_wlc.17.16.x.SPA.bin
  - C9800-L-universalk9_wlc.17.16.x.SPA.bin
- **Image Names (9800-CL)**:
  - **Cloud**: C9800-CL-universalk9.17.16.x.SPA.bin
  - **Hyper-V/ESXi/KVM**: C9800-CL-universalk9.17.16.x.iso, C9800-CL-universalk9.17.16.x.ova
  - **KVM**: C9800-CL-universalk9.17.16.x.qcow2
  - **NFVIS**: C9800-CL-universalk9.17.16.x.tar.gz

Software Installation Commands

Cisco IOS XE 17.16.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 Smart Licensing Using Policy.

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 17.16.x

Hardware or Software Parameter	Hardware or Software Type
Cisco Wireless Controller	See Supported Hardware, on page 6.
Access Points	See Supported APs, on page 15.
Radio	• 802.11ac • 802.11a • 802.11g • 802.11n • 802.11ax in 6GHz (Wi-Fi 6E)
Security	Open, PSK (WPA2-AES), 802.1X (WPA2-AES) (EAP-FAST, EAP-TLS)
RADIUS	See Compatibility Matrix, on page 16.
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	VG3.0
Drager M300.4	VG3.0

Client Type and Name	Driver or Software Version
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
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
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 17.16.1

Identifier	Headline
CSCwn17412	FlexConnect local switching traffic gets randomly centralized on a WebAuth SSID
CSCwm58430	Cisco Catalyst 9115 AP experiences kernel unresposiveness due to: Beacon Stuck Reset Radio
CSCwm86811	Fabric APs do not take static-IP address after reload
CSCwn10606	Cisco Catalyst 9120 Wi_Fi 6 AP fails to report RFID packets to the controller

Identifier	Headline
CSCwn31021	Controller fails to represent the correct format of AP Name and VLAN ID in option 82
CSCwn33501	Controller connected to the AP does not give any output while executing the #show ap summary sort name command
CSCwn41314	Cisco Catalyst 9130 AP does not detect BLE beacons from zebra scanners
CSCwk26966	Cisco Aironet 3802 AP displays false radar detection only on UNI-II after upgrading the software
CSCwk55656	AP shadow record support in standby
CSCwm86679	Cisco Catalyst 9800-40 controllers encounter kernel unresponsiveness and reboot unexpectedly at rogue_start_containers
CSCwm99135	802.11ax client faces latency in AP
CSCwn03468	Clients encounter slow speeds while connecting to slot 2 operating in the 5-GHz band on CM66
CSCwn15048	Controller does not filter out the expansion module SN field before sending it to DNAC, causing the collection to fail
CSCwn15720	Frequent Group Key Update timeout deletes wireless clients from SSID
CSCwn18885	Cisco Catalyst 9136 series APs encounter kernel unresponsiveness with last reload reason 'unknown'
CSCwn22725	Cisco Aironet 1815 OEAP encounters repeated kernel unresponsiveness on 17.9.5 APSP 7
CSCwn27877	Cisco Catalyst 9105 AP stops responding to clients on 5GHz CS00012380774
CSCwn27951	Cisco Catalyst 9105W AP: RLAN fast switching breaks DHCP for non-native VLAN wireless
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
CSCwn16345	Cisco Catalyst 9166 AP reports an unexpected temperature reading on 17.12.4
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
CSCwn34509	Client traffic is sent to the controller inside the CAPWAP tunnel in the Flex local switching configuration
CSCwn35949	Cisco Catalyst 9120 Wi_Fi 6 AP displays memory leak
CSCwk18940	IW9167E WGB 10M speed not worked with WS-C3560CX-12PC-S switchport

Resolved Issues for Cisco IOS XE 17.16.1

Identifier	Headline
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
CSCwm07499	Cisco Catalyst 91xx AP does not rotate awipsd.log causing an upgrade issue "tar: write error: No space left on device"
CSCwm31864	Cisco Wave APs experience kernel unresponsiveness due to memory leak reason OOM
CSCwm49467	FlexConnect APs disable u-APSD in the assoc request if clients don't have it enabled
CSCwm66129	Cisco Wave 2 APs 2800, 3800, and 4800 display duplicate entries for stale clients in the Wi-Fi driver
CSCwj03060	Cisco Aironet 1815w AP encounters kernel unresponsiveness on image version 17.9.4.205
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
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
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
CSCwm65889	Cisco Catalyst 9120 Wi_Fi 6 AP's Fine Timing Measurement (FTM) is enabled by default, preventing the AP from sending HW Acks. CS0012371828
CSCwm73271	Cisco Wave 2 AP does not send syslog messages if the receiver is using an IPv6 address
CSCwn14495	Cisco Catalyst 91XX AP detects its own BSSID as rogue
CSCwm04614	WNCd logs display a CPU hog during association request processing
CSCwm12544	Controller unexpectedly reloads with cpp-ucode exception due to a rbuf out-of-handle
CSCwi04855	APs repeatedly join and disjoin controller with traceback
CSCwi16509	APs do not join the controller with invalid radio slot ID error
CSCwi78109	Controller GUI displays error messages: %CLI_AGENT-1-NVGEN_ERR while processing NVGEN command

Identifier	Headline
CSCwj08367	Cisco Catalyst 9800 Wireless Controller encounters unresponsiveness generating system report, segmentation fault - Process = IGMPSN
CSCwj13190	Inventory app shows "Internal Error" for controller that was in Catalyst Center for several releases
CSCwj36962	Controller reboots unexpectedly due to invalid QoS parameters
CSCwj79545	Controller unexpectedly reboots during WNCd process due to assertation failure with invalid BSSID
CSCwj85091	Controller unexpectedly stops working while running the show wireless client mac-address detail command
CSCwj86938	Memory leak in scale network with telemetry shared user events with Cisco Catalyst Center
CSCwj88071	Controller sends an invalid XML character (Unicode: 0x4) found in RPC response for ap-model
CSCwj93153	Controller becomes unresponsive during WNCd process
CSCwj93876	Controller unexpectedly reloads with reason "Critical process wncmgrd fault on rp_0_0 (rc=134)"
CSCwj97219	Controller experiences an unresponsive device state on DNAC when scaling APs and clients
CSCwk05030	Controller becomes unresponsive due to critical software exception
CSCwk05809	%EVENTLIB-3-CPUHOG message observed on Cisco IOS XE 17.12
CSCwk09059	Controller experiences kernel unresponsiveness due to critical process cpp_ha_top_level_server fault on fp_0_0 (rc=69)
CSCwk16780	The downstream multicast traffic is blocked for WGB wired client when WGB is associated with the controller
CSCwk17102	Client experiences unexpected disconnect due to missing M1 packet
CSCwk17667	Controller reboots due to high ODM memory consumption
CSCwk24352	Wireless clients are unable to receive the splash page and gets stuck due to webauth requirement
CSCwk27553	Controller sends unicast ARP/IPv6 NS for foreign client, causing periodic MAC flaps
CSCwk35891	Controller experiences unresponsiveness after displaying "\clear ap geolocation derivation\" message
CSCwk36229	Controller does not send M1 packet when client reconnects after an EAP_TIMEOUT
CSCwk37983	Client VLAN is retained after changing SSIDs if \"vlan-persistent\" is enabled

Identifier	Headline
CSCwk39866	Client page is stuck in loading state
CSCwk44459	Loadbalancer server holds incorrect AP IP address and stale entries
CSCwk54291	Controller voice CAC BW is not cleared
CSCwk61854	Configuration update failure when AP is in delete pending state
CSCwk70277	FRA sets slot 2 to 6 GHz in Cisco Catalyst 9166 AP even when 6-GHz network is disabled
CSCwk76746	Controller stops responding constantly when running specific UDN related commands
CSCwk84121	Local switching clients are assigned to Zone ID 0 when IP overlap is configured and FlexConnect VLAN central switching
CSCwk97948	Controller ends abnormally during an ISSU upgrade from Cisco IOS XE 17.3 to 17.12
CSCwm03016	Controller experiences kernel unresponsiveness abnormally pointing to client_orch
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
CSCwm67710	Cisco Catalyst 9800-80 controller encounters critical process WNCd failure (rc 0)
CSCwm74071	Controller encounters kernel unresponsiveness due to client being stuck in 802.11r preauth and BSSID/AP going down at the same time
CSCwn06627	Controller encounters kernel unresponsiveness with geolocation config pointing towards geo_cloudm_graph_shortest_path
CSCwj00465	Active controller becomes ActiveRecovery when the redundancy port link is down
CSCwj33979	Output for the show ap summary command takes lengthy duration to complete
CSCwj69312	Loadbalancer feature does not work when AP sends negative SNR value
CSCwj72370	Controller uses incorrect username for "show platform" command when logging in GUI
CSCwj76892	Controller configures aggregation scheduler parameter incorrectly, causing low downlink speed
CSCwj82407	Controller's Web UI enhancement shows login banner while using TACACS/RADIUS

Identifier	Headline
CSCwj83935	Controller shows tech X is empty when previous tech X term length stop didn't finish before SSH close
CSCwj85339	Controller displays no effect on disabling DCA Aggressive on startup
CSCwj94201	Controller experiences unresponsiveness CPUHOG
CSCwj96620	Syntax errors observed in CISCO-LWAPP-DOT11-CLIENT-MIB
CSCwj96666	Syntax errors observed in CISCO-LWAPP-DOT11-MIB
CSCwj97107	Standby controller does not take active role after reloading the active controller with "reload slot" command
CSCwk02633	An RSA key pair is configured in the truspoint configuration when an EC keypair is selected when creating a trustpoint on the controller
CSCwk11417	ewlc_cert_mgr, SafeC Validation: strncpy_s: does not have enough space after assigning new WebAdmin cert
CSCwk25182	Controller throws password policy alert while logging in GUI using TACACS+ credentials after upgrading to Cisco IOS XE 17.14
CSCwk28680	Controller unexpectedly reloads due to Cisco QuantumFlow Processor (QFP) ucode while updating the drop statistics
CSCwk59342	Controller using channels 1, 5, 6, 9, 11, and 13 on 2.4GHz RF profiles causes discrepancies
CSCwk74269	SNMP query with bsnAPIfTable OID fails for Cisco Catalyst 9166D APs
CSCwk74699	Controller GUI does not change AP tags displaying "System Busy! Please retry after sometime"
CSCwk77766	Cisco Catalyst 9800-80 encounters kernel unresponsiveness due to incorrect delete reason code in the AP delete mobile payload
CSCwk77862	AP does not disjoin automatically when the AP-name is changed in the Regex filter
CSCwm14401	Controller experiences an unexpected reset of WNCd
CSCwm28542	OKC roam fails after a brief WAN drop
CSCwm36501	Controller encounters kernel unresponsiveness due to TLB miss
CSCwm80472	Controller's UI and CLI fail to delete a mobility peer due to 'invalid transversal ctx for walker next rec'
CSCwm93080	IP address of the TACACS server disappears when the GUI timeout is changed
CSCwj88851	Controller reports Yang/CLI length mismatch for AP location description to Cisco Catalyst Center
CSCwk67341	IW916x WGB: wcpd crash during 802.11v neighbor list updates after multiple roams

Identifier	Headline
CSCwn08168	WGB with Dual-Radio Feature: Incorrect AP Selection Chooses Low RSSI BSSID in Mesh Topology
CSCwm38081	Terminal Flood with '8021q: adding VLAN 0 to HW filter on device' When Dual 5G is Enabled on WGB

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.

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

© 2024 Cisco Systems, Inc. All rights reserved.