Release Notes for Cisco Catalyst 9800 Series Wireless Controller, Cisco IOS XE Release 17.13.x

First Published: 2023-12-08

Last Modified: 2023-12-08

Release Notes for Cisco Catalyst 9800 Series Wireless Controller, Cisco IOS XE 17.13.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 17.13.1

Table 1: New and Modified Software Features

Feature Name	Description and Documentation Link
802.11h support on IW9167E	802.11h is intended to resolve interference issues introduced by the use of 802.11a in some locations, particularly with radar systems and medical devices. Dynamic Frequency Selection (DFS) and Transmit Power Control (TPC) are two main features of 802.11h. The following are supported from this release: • Associating STAs with an AP in a BSS based on the STAs' supported channels • Smoothly switching to a new channel when receiving CSA • Selection of a transmit power for each transmission in a channel within constraints imposed by regulatory and local requirements. The following command is introduced: • **show wgb dot11h dot11Radio** <*radio_slot_id*> **info**

Feature Name	Description and Documentation Link
Access Point Auto Location Support	The improvized Access Point Auto Location Support feature helps wireless clients to leverage Fine Timing Measurement (FTM) and AP GNSS for indoor navigation. The following commands are introduced: • **geolocation ftm-responder advertise-ap-location** • **clear ap geolocation ranging** • **ap sensor air-pressure** • **show ap name geolocation ranging status** For more information, see the chapter AP Management.
Access Point Client ACL Counter Support	From this release, the AP Client ACL Counter feature provides a statistical count for client ACL rules. This feature allows you to count the number of packets that hit a specific rule in the client ACL. For more information, see the chapter Security.
Amazon S3 Support	The Amazon S3 or Amazon Simple Storage Service is a service offered by Amazon Web Services (AWS) that provides scalable storage infrastructure through a web service interface. Using Amazon S3, you can seamlessly supplement built-in persistent storage with cloud-based storage The following commands are introduced: • **bucket** • **cloud-services aws s3 profile** • **permissions** • **show cloud-services aws s3 summary** • **show cloud-services aws s3 profile** For more information, see the Chapter Amazon S3 Support.

Feature Name	Description and Documentation Link
Amazon Web Services CloudWatch	The AWS CloudWatch facilitates the monitoring and observability of server system logs, metrics, and events. The following commands are introduced: • **access-key** • **cloud-services aws cloudwatch profile** • **log** • **proxy** • **region** • **vrf** • **show cloud-services aws cloudwatch summary** • **show cloud-services aws cloudwatch profile** For more information, see the Chapter Amazon Web Services CloudWatch.
AP Deployment Mode	This feature configures the Cisco Catalyst 9124AX Series Outdoor Access Points to operate in Indoor mode (in -E regulatory domain only) to increase the available channel list. The following commands are introduced: • **dual-mode-ap-deployment-mode** • **show ap name config general** • **show rrm receive configuration** • **show capwap client configuration** For more information, see the Chapter AP Deployment Mode.
AP DHCP Option82 Support on FlexConnect Local Switching Mode	The AP DHCP Option82 Support on FlexConnect Local Switching Mode feature enables the AP to act as a DHCP relay agent to prevent DHCP client requests from unreliable sources. For more information, see the Chapter DHCP Option 82.
AP Power Distribution Support in Cisco Catalyst 9124 Series Access Points.	From this release, AP power distribution is supported in Cisco Catalyst 9124 Series APs. The PoE-out interface is introduced in Cisco Catalyst 9124 Series APs, in addition to the USB, Ethernet, and LAN interfaces. The following command is introduced: • *sequence-number* **ethernet LAN1 poe-out disable** For more information, see the chapter AP Management.

Feature Name	Description and Documentation Link
Cisco Aironet Wave 2 and Catalyst Access Point Image Management	A new command is introduced to display brief information about the AP image details: • **show ap image details** The **show ap config general** command has been enhanced to view the general configuration information of all Cisco APs.
Cisco Catalyst 9163E Access Point	Cisco Catalyst 9163E Access Point is a Wi-Fi 6E technology-based 2x2 tri-band outdoor enterprise-class 802.11ax access point. The AP is designed to cater to low and medium-density environment applications. This outdoor AP can work with external antenna models based on use case requirements. The AP features 2x2 tri-band radios, a 1x1 tri-band scanning radio, a 2.4 GHz IoT radio and a GNSS receiver for 6 GHz AFC compliance.
Cisco Work Group Bridge (WGB) Concurrent Radio Support on Cisco Catalyst 9130 Series Access Points and Cisco Catalyst 9124 Series Access Points.	From this release, Cisco WGB concurrent radio is supported on Cisco Catalyst 9130 Series Access Points and Cisco Catalyst 9124 Series Access Points.
DHCP Option 82 for Guest Foreign and Anchor Scenario	From this release, DHCP Option 82 is supported on Guest - Anchor scenarios. If the client roams to a different AP from the guest controller, the new AP information will not be propagated to the anchor controller. For more information, see the Chapter DHCP Option 82.
ED-RRM Support for 6-GHz Band Radio	From this release, the Event-Driven Radio Resource Management (EDRRM) is enabled in the 6-GHz band radio of AP. For more information, see the Chapter Cisco CleanAir.
Increase Rogue AP Scale Limitation from 625	The rogue AP manual classification and the rogue client manual classification limit have been enhanced from 625 to 10,000 configurations at a time.

Feature Name	Description and Documentation Link
Layer 3 Access	This feature allows the Cisco Catalyst 9800 Series Wireless Controller platforms to be deployed as Layer 3 network devices and perform forwarding functions. The following commands are introduced: • **l3-access** • **router ospf** • **ip ospf authentication message-digest** • **ip ospf area** • **ip ospf bfd** • **ip multicast-routing distributed** • **ip pim rp-address** • **ip pim sparse-mode** • **ip nat outside** • **ip nat inside** For more information, see the Chapter Layer 3 Access.
Low Latency Profile	IEEE 802.11 networks have a great role to play in supporting and deploying the Internet of Things (IoT) for the low latency and QoS requirement by applying the Enhanced Distributed Channel Access (EDCA), aggregated MAC protocol data unit (AMPDU), aggregated/non-aggregated packet retry. A new EDCA profile is added to the wireless controller to support IoT Wi-Fi network with low latency requirements. A new policy based AMPDU Length is introduced to configure profiled based A-MPDU under 2.4G, 5G and 6G radio. Two predefined low-latency profiles are introduced on WGB to configure EDCA parameters and A-MPDU length. Meanwhile, users are able to customize their own profiles to meet different requirements. For more information, see the section *Low Latency Profile* of the Cisco Catalyst IW9165E Rugged Access Point and Wireless Client Configuration Guide.
Quad Radio Support in Cisco Catalyst 9136 Series Access Points.	From this release, the Quad Radio feature is supported in Cisco Catalyst 9136 Series Access Points. The Tri-radio settings are enabled by default, and cannot be disabled. For more information, see the chapter Cisco Access Points with Tri-Radio.

Feature Name	Description and Documentation Link
Roaming Enhancement with 802.11v Support	This feature enables WGB to periodically query for latest neighbor APs and associate to the optimal AP on next roam. The scan handoff mode with dual 5G radio is supported from this release. For more information, see the section *802.11v Support* of the Cisco Catalyst IW9165E Rugged Access Point and Wireless Client Configuration Guide.
Roaming Enhancement with Aux Scan-handoff Mode Support	This feature enables WGB to use the second 5G radio to periodically scan the neighbor Aps. This Aux 5G radio will associate to the optimal AP based on next roam handoff decision. For more information, see the section *Configuring Aux-Scan Handoff Mode* of the Cisco Catalyst IW9165E Rugged Access Point and Wireless Client Configuration Guide.
SD-Access Wireless Mesh Inter Fabric Edge Switch Roaming Protection	The Mesh AP roam is restricted to Mesh and Root APs connected to the same fabric edge switch. For more information, see the Chapter Software-Defined Access Wireless.
Support to Configure 802.11n Speed Rates	Support to configure WGB radio in HT (802.11n) mode and customize MCS rates. For more information, see the section *Configuring HT Speed Limit* of the Cisco Catalyst IW9165E Rugged Access Point and Wireless Client Configuration Guide.
WGB 1:1 NAT Functionality in Client Mode	One-to-one (1:1) Layer 2 NAT is a service that allows the assignment of a unique public IP address to an existing private IP address (end device), so that the end device can communicate with public network. This feature solves the problem of multiple end devices with the same duplicated IP addresses in the industrial network communicating with the public network. For more information, see the section *Configuring Layer 2 NAT* of the Cisco Catalyst IW9165E Rugged Access Point and Wireless Client Configuration Guide.
WGB mode and uWGB mode support on IW9165E	From this release, WGB mode and Universal Workgroup Bridge (uWGB) mode are supported on the Cisco Catalyst IW9165E Rugged Access Point and Wireless Client. For more information, see Cisco Catalyst IW9165E Rugged Access Point and Wireless Client Configuration Guide.

Feature Name	Description and Documentation Link
WGB Serviceability Enhancement	WGB serviceability enhancement provides support to configure device, monitor device status, and collect statistics or logs easily for troubleshooting. The following enhancements are supported from this release: • Standalone with static IP • Syslog service • Radio statistics CLIs • Event logging For more information, see Cisco Catalyst IW9165E Rugged Access Point and Wireless Client Configuration Guide.

Table 2: New and Modified GUI Features

Feature Name	GUI Path
Access Point Auto Location Support	• **Configuration > Tags & Profiles > WLANs**
AP Power Distribution Support in Cisco Catalyst 9124 Series Access Points.	• **Configuration > Tags & Profiles > Power Profile**

MIBs

The following MIBs are newly added or modified:

- AIRESPACE-WIRELESS-MIB
- CISCO-LWAPP-QOS-MIB
- CISCO-LWAPP-SI-MIB
- CISCO-LWAPP-TUNNEL-MIB
- CISCO-LWAPP-WLAN-POLICY-MIB

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

- From Cisco IOS XE Dublin 17.13.1, the **show ap master list** command is modified. The **master** keyword is replaced with **primary**.
- The rogue AP manual classification limit has been enhanced from 625 to 10,000 configurations at a time. The rogue client manual classification limit has been enhanced from 625 to 10,000 configurations at a time.
- From this release, the ap geolocation ranging time has been changed from 10 minutes to 15 minutes.
- The CSV file import fails if the static AP mapping table already contains a few entries. You must delete those entries manually and then add the CSV files.
- If you have configured CISCO_IDEVID_SUDI trustpoint in your configuration, you will need to replace it with CISCO_IDEVID_CMCA3_SUDI to avoid client connection and AP join issues. The reason for this change being the CISCO_IDEVID_SUDI changed from SW-SUDI certificate in previous releases to HW-SUDI certificate. The processing of HW-SUDI certificate is much slower than the SW-SUDI. Here, CISCO_IDEVID_CMCA3_SUDI is the new SW-SUDI certificate.

Interactive help

Interactive help is a user interface feature that

- provides step-by-step guidance within the application
- adapts instructions and walk-throughs to the user's context, and
- assists users in completing complex configurations or navigating the system.

Modes of starting the interactive Help

You can start the interactive help in the these ways.

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

  For example, **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.

Additional troubleshooting information

If the WalkMe launcher is unavailable on Safari, modify the browser settings.

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 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	• VMware ESXi vSphere 6.0, 6.5, 6.7, and 7.0 • VMware ESXi vCenter 6.0, 6.5, 6.7, and 7.0 • 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
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
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
FINISAR- FTL4C1QL2L	Supported	—	—
FINISAR- FTL4C1QE1C	Supported	—	—
GLC-BX-D	Supported	Supported	Supported
GLC-BX-U	Supported	Supported	Supported
GLC-EX-SMD	Supported	Supported	—

SFP Name	C9800-80-K9	C9800-40-K9	C9800-L-F-K9
GLC-LH-SMD	Supported	Supported	—
GLC-SX-MMD	Supported	Supported	Supported
GLC-T	Supported	—	—
GLC-TE	Supported	Supported	Supported
GLC-ZX-SMD	Supported	Supported	Supported
QSFP-100G-LR4-S	Supported	—	—
QSFP-100G-SR4-S	Supported	—	—
QSFP-40G-BD-RX	Supported	—	—
QSFP-40G-CSR-S	Supported	—	—
QSFP-40G-ER4	Supported	—	—
QSFP-40G-LR4	Supported	—	—
QSFP-40G-LR4-S	Supported	—	—
QSFP-40G-SR-BD	Supported	—	—
QSFP-40G-SR4	Supported	—	—
QSFP-40G-SR4-S	Supported	—	—
QSFP-40GE-LR4	Supported	—	—
QSFP-H40G-ACU7M	Supported	—	—
SFP-10G-AOC10M	Supported	Supported	—
SFP-10G-AOC1M	Supported	Supported	—
SFP-10G-AOC2M	Supported	Supported	—
SFP-10G-AOC3M	Supported	Supported	—
SFP-10G-AOC5M	Supported	Supported	—
SFP-10G-AOC7M	Supported	Supported	—
SFP-10G-ER	Supported	Supported	—
SFP-10G-LR	Supported	Supported	Supported
SFP-10G-LR-S	Supported	Supported	Supported
SFP-10G-LR-X	Supported	Supported	Supported
SFP-10G-LRM	Supported	Supported	Supported

SFP Name	C9800-80-K9	C9800-40-K9	C9800-L-F-K9
SFP-10G-SR	Supported	Supported	Supported
SFP-10G-SR-S	Supported	Supported	Supported
SFP-10G-SR-X	Supported	Supported	Supported
SFP-10G-ZR	Supported	Supported	—
SFP-H10GB- ACU10M	Supported	Supported	Supported
SFP-H10GB- ACU7M	Supported	Supported	Supported
SFP-H10GB- CU1.5M	Supported	Supported	Supported
SFP-H10GB-CU1M	Supported	Supported	Supported
SFP-H10GB-CU2.5M	Supported	Supported	Supported
SFP-H10GB-CU2M	Supported	Supported	Supported
SFP-H10GB-CU3M	Supported	Supported	Supported
SFP-H10GB-CU5M	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

Source	Destination	Protocol	Destination Port	Source Port	Description
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.
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

Source	Destination	Protocol	Destination Port	Source Port	Description
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
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

Source	Destination	Protocol	Destination Port	Source Port	Description
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 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

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 Informaton

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 26.1.2	3.4 3.3 3.2 3.1 3.0 2.7 * all with latest patches	Not Available	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	11.1.1 11.1.0 11.0.1 11.0.0 10.6.3
IOS XE 26.1.1	3.4 3.3 3.2 3.1 3.0 2.7 * all with latest patches	Not Available	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	11.1.1 11.1.0 11.0.1 11.0.0 10.6.3

Table 9: 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 17.13.1	3.2 3.1 3.0 2.7 * all with latest patches	3.10.6 Security Update 03 3.10.6 Security Update 02 3.10.6 Security Update 01 3.10.6 3.10.5 3.10.4 Update 03 (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 11.0.0 10.6.3

GUI System Requirements

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

Table 10: 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

To ensure a smooth upgrade and prevent potential boot loop issues with APs, review these **Field Notice** and **technical documentation**. It is critical to complete these actions prior to initiating your upgrade.

1. FN74383: Field Notice
2. Validate and Recover Catalyst APs on 17.12

Other guidelines before you upgrade

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

- ERSPAN is not supported on the Cisco Catalyst 9800 Series Wireless Controller platform. Although the CLI allows you to enter **monitor session** commands for ERSPAN configuration, do not configure monitor

session for ERSPAN on the controller. If an ERSPAN monitor session is configured, the configuration cannot be deleted from the controller.

- 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.

- 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 and 6E 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.

- ISSU feature is supported only within and between major releases, for example, 17.3.x (within a release) and 17.3.x to 17.6.x (among major releases).
- Controller upgrade from Cisco IOS XE Bengaluru 17.3.x to Cisco IOS XE Bengaluru 17.6.x or Cisco IOS XE Cupertino 17.9.x or later using ISSU may fail if the **domain** command is configured. Ensure that you run the **no domain** command before starting an ISSU upgrade because the **domain** command has been removed from Cisco IOS XE Bengaluru 17.6.x.
- Controller upgrade from Cisco IOS XE Bengaluru 17.3.x to any release using ISSU may fail if the **snmp-server enable traps hsrp** command is configured. Ensure that you remove the **snmp-server enable traps hsrp** command from the configuration before starting an ISSU upgrade because the **snmp-server enable traps hsrp** command has been removed from Cisco IOS XE Bengaluru 17.4.x.
- Controller upgrade to Cisco IOS XE Dublin 17.12.x from any prior release using ISSU may fail if the **snmp-server enable traps license** command is configured. Ensure that you remove the **snmp-server enable traps license** command from the configuration before starting an ISSU upgrade because the **snmp-server enable traps license** command has been removed from Cisco IOS XE Dublin 17.12.x.
- Rolling AP upgrade, which is a part of the ISSU feature, is not supported for mesh APs.
- Ensure that you add Authentication and Key Management (AKM) setting when you configure WPA3. In older releases, this scenario was not mandatory which resulted in an invalid configuration. However, from 17.9 and higher releases, this invalid scenario is detected and prevented.

Cisco Catalyst APs may enter a boot loop if you upgrade software versions earlier than 17.9.4 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.

- When you downgrade an AP from a higher version to Cisco IOS XE Amsterdam 17.3.x, the AP will not be accessible through SSH or the console due to the denial of the **enable** password, when the AP has not yet joined a controller. If the AP joins a controller, then the AP becomes accessible without any password denial.

Upgrade Path to Cisco IOS XE 17.13.x

Table 11: Upgrade Path to Cisco IOS XE Dublin 17.13.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 17.13.x.
16.11.x	—	Upgrade first to 16.12.5 or 17.3.x and then to 17.13.x.
16.12.x	Upgrade first to 17.3.5 or later or 17.6.x or later, and then to 17.13.x.	Upgrade first to 17.3.5 or later or 17.6.x or later, and then to 17.13.x.
17.1.x	Upgrade first to 17.3.5 or later and then to 17.13.x.	Upgrade first to 17.3.5 or later and then to 17.13.x.
17.2.x	Upgrade first to 17.3.5 or later and then to 17.13.x.	Upgrade first to 17.3.5 or later and then to 17.13.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 17.13.x.	Upgrade directly to 17.13.x.
17.3.4c or later	Upgrade directly to 17.13.x.	Upgrade directly to 17.13.x.
17.4.x	Upgrade first to 17.6.x and then to 17.13.x.	Upgrade directly to 17.13.x.
17.5.x	Upgrade first to 17.6.x and then to 17.13.x.	Upgrade directly to 17.13.x.
17.6.x	Upgrade directly to 17.13.x.	Upgrade directly to 17.13.x.
17.7.x	Upgrade directly to 17.13.x.	Upgrade directly to 17.13.x.
17.8.x	Upgrade directly to 17.13.x.	Upgrade directly to 17.13.x.
17.9.x	Upgrade directly to 17.13.x	Upgrade directly to 17.13.x
17.10.x	Upgrade directly to 17.13.x	Upgrade directly to 17.13.x
17.11.x	Upgrade directly to 17.13.x	Upgrade directly to 17.13.x

Current Software	Upgrade Path for Deployments with 9130 or 9124	Upgrade Path for Deployments Without 9130 or 9124
17.12.x	Upgrade directly to 17.13.x	Upgrade directly to 17.13.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 17.13.x	Upgrade directly to 17.13.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 17.13.x
- **Image Names (9800-80, 9800-40, and 9800-L)**:
  - C9800-80-universalk9_wlc.17.13.x.SPA.bin
  - C9800-40-universalk9_wlc.17.13.x.SPA.bin
  - C9800-L-universalk9_wlc.17.13.x.SPA.bin
- **Image Names (9800-CL)**:
  - **Cloud**: C9800-CL-universalk9.17.13.x.SPA.bin
  - **Hyper-V/ESXi/KVM**: C9800-CL-universalk9.17.13.x.iso, C9800-CL-universalk9.17.13.x.ova
  - **KVM**: C9800-CL-universalk9.17.13.x.qcow2
  - **NFVIS**: C9800-CL-universalk9.17.13.x.tar.gz

Software Installation Commands

Cisco IOS XE 17.13.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 12: Test Configuration for Interoperability

Hardware or Software Parameter	Hardware or Software Type
Release	Cisco IOS XE 17.13.x

Hardware or Software Parameter	Hardware or Software Type
Cisco Wireless Controller	See Supported Hardware, on page 10.
Access Points	See Supported APs, on page 17.
Radio	• 802.11ax • 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) WPA3 AKM 802.11ax
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 13: 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

Client Type and Name	Driver or Software Version
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)
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

Client Type and Name	Driver or Software Version
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
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

Client Type and Name	Driver or Software Version
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
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

Client Type and Name	Driver or Software Version
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
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

Client Type and Name	Driver or Software Version
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 Caveats for Cisco IOS XE 17.13.1

Identifier	Headline
CSCwd71613	AP detects its own Basic Service Set Identifier (BSSID) as malicious after a channel reset.
CSCwe81775	Apple devices are not deleted after sending Extensible Authentication Protocol (EAP) logoff messages.
CSCwf90946	Cisco Catalyst 9130 AP doesn't forward 802.1x "Identity Request" with wireless phones.
CSCwh57076	The controller is not forwarding broadcast address resolution protocol (ARP) request to the wireless client.
CSCwh63050	The controller is sending Internet Group Management Protocol (IGMP) queries using the client VLAN gateway ip address that is not present in the controller and with the controller mac-address.
CSCwh66453	Run state client (after successful webauth) is not able to pass traffic.
CSCwh68219	Cisco Catalyst 9100 Series AP is not processing the Extensible Authentication Protocol (EAP)-Transport Layer Security (TLS) server Hello.
CSCwh74415	Per client rate limit with FlexConnect local switching APs is not working.
CSCwh88246	A URL filter is not applied after an invalid configuration.
CSCwh92425	Cisco Catalyst 9130 and 9136 APs are not considering power save mode.
CSCwi06785	The controller is not sending IPv4 Gratuitous ARP (GARP) or IPv6 NA for wireless clients in RUN state after switchover.
CSCwi07094	Apple client is not able to connect to flex Wi-Fi Protected Access (WPA) 2 + WPA3 SSID with Simultaneous Authentication of Equals (SAE) enabled and Opportunistic Key Caching (OKC) disabled.
CSCwi16104	A dbm crash is observed at VLAN list retrieval.
CSCwi18057	4-way handshake failure, missing M3 packet.
CSCwi22847	Cisco Catalyst 9800-80 Controller crashes after receiving analytics from AP.
CSCwi38210	After a factory reset, Cisco Catalyst IW9167 WGB reboots automatically during uplink.
CSCwh92173	Cisco Catalyst IW916x WGB: Per chain RSSI reading is always 0.
CSCwi46923	Incorrect Fine Timing Measurement (FTM) responder capable beacon misleads clients.
CSCwm95849	Cisco Catalyst 9136 AP does not receive the 6e SSID

Resolved Caveats for Cisco IOS XE 17.13.1

Identifier	Headline
CSCwe11213	Cisco Catalyst 9130 AP crashes due to radio recovery failure.
CSCwe24263	Cisco Catalyst 9130 AP: Inconsistent TX power levels are advertised in beacons.
CSCwf07384	The wired client behind Cisco Catalyst 9105 RLAN is not able to pass traffic.
CSCwf10839	Bursts of Virtual Router Redundancy Protocol (VRRP) traffic sent from the Cisco Embedded Wireless Controller on Cisco Catalyst Access Points and Switch port get down due to storm-control action.
CSCwf12301	WCPD tx retry count is always 0.
CSCwf13107	Cisco Catalyst 9105 AP: Radio crash is observed.
CSCwf13804	Cisco Catalyst 9120 APs are randomly failing to onboard new client associations.
CSCwf21390	Duplicate Access-Request messages with CTS client username are seen when multiple RADIUS servers are configured.
CSCwf29742	Cisco Catalyst 9120 AP: Firmware crash is observed while running multicast and longevity with more than 80 clients.
CSCwf36752	Terminal Access Controller Access-Control System (TACACS) failed to encrypt the secret key if we used a fully qualified domain name (FQDN) as a TACACS+ address when configured for the first time.
CSCwf52815	Cisco Wave 2 AP: Improve Path Maximum Transmission Unit (PMTU) discovery mechanism to be able to honor the Internet Control Message Protocol (ICMP) unreachable maximum transmission unit (MTU) value.
CSCwf53520	Cisco Aironet 1815 AP: Kernel panic crash is observed.
CSCwf59348	Cisco Catalyst 9105/9115/9120 AP: The beacon is set to a maximum transmit power level of 128 dBm for Ireland.
CSCwf60151	Memory leak with pubd on controller due to telemetry connection flap.
CSCwf61881	Cisco Catalyst 9166D1 AP changes the country code to the UX domain and prevents setting it to standard power.
CSCwf62051	Cisco Aironet 1815W AP crashes due to kernel panic.
CSCwf63818	Cisco Aironet 1832 AP: Kernal panic crash is observed.
CSCwf64009	Cisco Aironet 1815 AP is leaking Remote LAN (RLAN)-VLAN traffic with a looped port.
CSCwf65794	Cisco Aironet 1852 AP reloads unexpectedly due to radio failure (radio recovery failed).
CSCwf66661	The sm_device_count_list takes too long to populate leading to websocket termination.

Identifier	Headline
CSCwf68131	Cisco Catalyst 9105AXW AP: A large number of bad blocks are detected.
CSCwf68612	The controller reloads unexpectedly due to a segmentation fault in the WNCD process.
CSCwf78066	Cisco DNA Center 2.3.3.7: "No radios in the selected band" message on the floor map.
CSCwf81866	Radio 0 WGB configuration is not backed up correctly when doing a TFTP backup of the configuration.
CSCwf83278	Client traffic fails with N+1 when AP sends CLIENT_DEL_STOP_REASSOC.
CSCwf83292	Cisco Catalyst 9130 AP is not sending DHCP offers and ACK over the air to clients.
CSCwf86242	The controller reloads unexpectedly with CAPWAP window size set to 0.
CSCwf91445	Controller pushes accounting information for preshared key (PSK) local authentication WLANs.
CSCwf93992	Cisco Aironet 2800 APs in FlexConnect mode are not processing Extensible Authentication Protocol (EAP)-Transport Layer Security (TLS) fragmented packets if the delay is more than 50 ms.
CSCwf94863	Cisco Catalyst 9115 AP: Kernel panic crash is observed (at drop_pagecache_sb+0x78/0x110).
CSCwf95868	The Tx power of single-band BCM workgroup bridge (WGB) radio 0 is decreased by nearly 20 dBm after configuring antenna number.
CSCwf99906	Network time protocol (NTP) authentication that is removed after a reload is using more than 16 bytes.
CSCwf99932	Cisco Catalyst 9120 AP: Radio1 is crashing.
CSCwh06834	Using special characters in the password while generating trust point generates an invalid trust point.
CSCwh08625	AP kernel panic crash is observed (at _raw_spin_unlock).
CSCwh09879	Cisco Wave 2 APs in FlexConnect mode are sending assoc-resp failure with status code 12 and AID 0 after changing country code.
CSCwh11858	Cisco Switch running IOS-XE software crashes when removing the Fully Qualified Domain Name (FQDN) Access Control List (ACL).
CSCwh18613	Encrypted mesh pre-shared key changes each time "password encryption aes" is applied.
CSCwh20306	Cisco Wave 2 AP: The Cisco Hyperlocation feature is broken when the Advanced Wireless Intrusion Prevention System (aWIPS) is enabled.
CSCwh20934	CiscoWave 2 APs are reloading due to a Systemd critical process crash.
CSCwh27366	AP radio firmware crashes with reset code 2.

Identifier	Headline
CSCwh27425	Cisco Catalyst 9115AX AP is not forwarding a part of CAPWAP data packets to the uplink direction.
CSCwh29924	Cisco Catalyst 9105/9115/9120 AP WGB: Antenna-a couldn't function properly if configuration is ab-antenna.
CSCwh33190	Cisco Catalyst 9115 AP (Local Mode) crashes due to kernel panic.
CSCwh35072	Cisco Aironet 3800 AP reloads unexpectedly due to Fast Interrupt Request (FIQ)/Non-Maskable Interrupt (NMI) reset.
CSCwh42002	Controller crashes with wireless network control deamons (WNCD) core while processing CAPWAP data.
CSCwh49810	Audit session ID changes after inter-WNCD roam.
CSCwh50681	New SSID arp0v0 is being broadcasted after an upgrade.
CSCwh54762	A kernel panic occurs as a result of failure to synchronize (assert:"0" failed: file "wlc_fifo.c:960").
CSCwh56147	SNMP OID for AP location tag is missing on the controller.
CSCwh58099	After client deletion and Change of Authorization (CoA) terminate, the controller allows the client to reconnect.
CSCwh59420	Cisco Catalyst 9136 AP is crashing.
CSCwh61007	The controller is crashing constantly whenever it provisions multiple APs.
CSCwh61011	Cisco Catalyst 9120 and 9115 APs unexpectedly disjoin from the controller and are not able to establish Datagram Transport Layer Security (DTLS) again.
CSCwh74663	Cisco Aironet 3800 AP is not sending Quality of Service (QoS) data frames downstream due to the RadarDetected flag as TRUE.
CSCwh76420	Controller crashes while performing In-Service Software Upgrade (ISSU) upgrade.
CSCwh87343	Cisco IOS XE Software Web UI privilege escalation vulnerability.
CSCwh89539	CAPWAP messages are queued for longer than x seconds when client throttling is turned on.
CSCwh92459	The controller reloads unexpectedly with a WNCD fault on rp_0_0.
CSCwf95676	WIFI module went out of service upon reloading the device.
CSCwh95315	Cisco Catalyst IW9167E AP is changing its backhaul upon reload.
CSCwh58663	WGB: Incorrect RSSI value is shown when there is a broken antenna or physically not present.
CSCwi06055	Cisco Industrial Wireless 3702 AP radios are reset and stays down when the board temperature is less than -20 C.

Identifier	Headline
CSCwf26991	The **show controller dot11Radio 1** command output always shows 20 MHz wide regardless of the channel width being used.
CSCwh94965	Cisco Catalyst IW916x WGB: The wired infra client fails to ping the WGB wired client.

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 Wireless Access Points Detailed Channels and Maximum Power Settings

For detailed channels and maximum power settings for Cisco Wireless indoor and outdoor APs, and country support per release, see:

Detailed Channels and Maximum Power Settings Document for Supported Access Points

Feature Matrix for Cisco Wireless Access Points

Feature Matrix for Cisco Wireless Access Points

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)

© 2023 Cisco Systems, Inc. All rights reserved.