Release Notes for Cisco Catalyst 9800 Series Wireless Controller, Cisco IOS XE Bengaluru 17.4.x

First Published: 2020-11-30

Last Modified: 2020-11-29

Release Notes for Cisco Catalyst 9800 Series Wireless Controller, Cisco IOS XE Bengaluru 17.4.x

Introduction to Cisco Catalyst 9800 Series Wireless Controllers

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

The Catalyst 9800 controllers are enterprise ready to power your business-critical operations and transform end-customer experiences:

- The controllers come with high availability (HA) 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 or a Cisco Catalyst access point (AP).
- The controllers can be managed using Cisco Digital Network Architecture (DNA) Center, Programmability interfaces, for example, NETCONF and YANG, or web-based GUI or CLI.
- The controllers are built on a modular operating system. Open and programmable APIs enable the automation of your day zero to day *n* network operations. Model-driven streaming telemetry provides deep insights into your network and client health.

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

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

Note All of the Cisco IOS-XE programmability-related topics on the Cisco Catalyst 9800 controllers are supported by DevNet, either through community-based support or through DevNet developer support. For more information, go to https://developer.cisco.com.

What's New in Cisco IOS XE Bengaluru 17.4.1

Table 1: Software Features Introduced in Cisco Catalyst 9800 Series Wireless Controller, Cisco IOS XE Bengaluru, 17.4.1

Feature Name	Description and Documentation Link
Access Point Memory Information	This feature allows you to view the AP memory type, the CPU type, and the memory size per AP, after the single sign-on authentication. The AP shares the memory information with the controller during the join phase. For more information, see the Access Point Memory Information chapter.
Fastlane+	This feature improves the effectiveness of estimating the uplink buffer status for Apple clients, thereby enhancing the user experience for latency-sensitive applications. The following commands were introduced: • **scheduler asr** • **show interfaces dot11Radio asr-info** For more information, see the Fastlane+ chapter.
Antenna Disconnection Detection	This feature detects the signal strength delta across the antennas on the receiver. If the delta is more than the defined limit for a specific duration, the corresponding antenna is considered to have issues. The following commands were introduced: • **antenna monitoring** • **trapflags ap broken-antenna** For more information, see the Antenna Disconnection Detection chapter.
Boot Integrity Visibility	This feature allows the Cisco platform identity and software integrity information to be visible and actionable. Platform identity provides the manufacturing installed identity of the platform. Software integrity exposes boot integrity measurements that can be used to assess whether the platform has booted a trusted code. For more information, see the Boot Integrity Visibility chapter.

Feature Name	Description and Documentation Link
Telemetry Subscriptions	For information, see the Model-Driven Telemetry chapter of the Programmability Configuration Guide, Cisco IOS XE Amsterdam 17.4.x.
Copying WebAuth Tar Bundle To Standby	From this release onwards, you can copy a WebAuth tar bundle to the standby controller, in an HA configuration. For more information, see the High Availability chapter.
DHCP Client Option 12 support for AP	The Dynamic Host Configuration Protocol (DHCP) Client Option12 feature specifies the hostname of the client. While acquiring an IP address for an interface from the DHCP server, if the AP receives the DHCP hostname option inside the response, the AP configures itself with that hostname. For more information, see the DHCP Client Option12 section.
Gateway IP Check with Native IPv6	This feature supports Redundancy Management Interface (RMI) with IPv6 addresses. Also, the IPv6 default gateway is monitored for the RMI subnet. This feature mimimizes the downtime on APs and clients when the gateway reachability is lost on the active controller. For more information, see the Gateway Reachability Detection section in Redundancy Management Interface chapter.
Equivalent of show ap bundle CLI in AireOS	The **show ap image file summary** command is modified to display two new fields: **Image File Size (in KB)** and **Supported AP models**. For more information, see the Software Maintenance Upgrade chapter.
OBSS-PD and Spatial Reuse	Overlapping BSS Packet Detect (OBSS-PD) is introduced in this release. OBSS-PD is a more aggressive Wi-Fi packet-detect threshold for inter-BSS packets, which can be higher than the typical or legacy -82 dBm. Inter-BSS packets are easily identified by comparing the BSS color in the HE PHY header of the packets received, with the BSS color of the device. The following commands were introduced: • **ap dot11** {**24ghz** | **5ghz**} **dot11ax spatial-reuse obss-pd** • **ap dot11** {**24ghz** | **5ghz**} **dot11ax spatial-reuse obss-pd non-srg-max** For more information, see the BSS Coloring chapter.

Feature Name	Description and Documentation Link
Overlapping Client IP Address in Flex Deployment	This feature offers overlapping IP address across various flex sites and provides all the functionalities that are supported in flex deployments. For more information, see the Overlapping Client IP Address in Flex Deployment chapter.
RADIUS Call Station Identifier	The called station identifier allows a RADIUS server to specify the MAC addresses or networks that a client can connect to. The following commands were modified: • **radius-server attribute wireless accounting call-station-id** • **radius-server attribute wireless authentication call-station-id** For more information, see the RADIUS Call Station Identifier chapter.
Redundancy Manangement Interface or Default Gateway Enhancements	This feature enables faster detection of gateway reachability loss. The Redundancy Manangement Interface (RMI) interface status is monitored, and all the actions associated with the gateway reachability loss are triggered when the RMI goes down. This feature is supported only on Cisco Catalyst 9800-40 and 9800-80 wireless controller platforms. For more information, see the Redundancy Management Interface chapter.
Redundant Root Access Point (RAP) Ethernet Daisy Chaining	The Root Access Point (RAP) Ethernet Daisy Chaining is a feature where RAPs are chained using wired Ethernet to avoid latency in backhaul link failure recovery. This feature proposes a redundancy in the daisy chain, wherein, two switches act as a redundant Designated Port (DP), each connected to either end of the daisy chain. In case of a link failure, the link direction is reversed using a new STP root. For more information, see the Redundant Root Access Point (RAP) Ethernet Daisy Chaining chapter.
Support for Accounting Session ID	Accounting Session ID is supported in the AAA access request while authenticating wireless client using IEEE 802.1x. Accounting ID is a unique identifier for a wireless client session. This ID helps to identify the accounting data of a client in the AAA server. An accounting session ID is generated by the corresponding AAA module. For more information, see the Support for Accounting Session ID chapter.

Feature Name	Description and Documentation Link
Support for Delimiter in DHCP Option 82 Remote ID Sub-Option	This feature supports all the valid Remote ID combinations separated with a colon (:) as the delimiter. For more information, see the DHCP Option82 chapter.
Support PROFINET Traffic Passthrough with QoS	This feature implements the ability of transparent PROFINET RT traffic over wireless on the IW6300 and ESW6300 access points. The PROFINET frame with ether-type 0x8892 is encoded in an 802.1q trunk and Traffic is prioritized as high priority by setting the priority bits in the 802.1q header to 6 on Cisco switches. For more information, see PROFINET Traffic Passthrough With QoS guide.
Support to Configure Multiple Ethernet LAN Ports of IW6300 and ESW6300	From this release onwards, you can enable or disable the LAN ports and configure the PoE status of the LAN ports on IW6300 and ESW6300 access points, using the following commands: • **ap name** *cisco_ap_name* **lan port-id** *lan-port-id* {**enable**|**disable**} • **ap name** *cisco_ap_name* **lan port-id** *lan-port-id* **poe** {**enable**|**disable**} For more information, see the Configuring Ethernet LAN Ports section in the Cisco Catalyst IW6300 Heavy Duty Series and 6300 Series Embedded Services Access Point Software Configuration Guide.
Support to Print RFID at AP Level on IW6300 and ESW6300	From this release onwards, you can print radio frequency identification (RFID) on IW6300 and ESW6300 access points. The following command was introduced: • **debug client dump rfid** For more information, see the Printing RFID at AP Level section of the Cisco Catalyst IW6300 Heavy Duty Series and 6300 Series Embedded Services Access Point Software Configuration Guide.
WIPS: Configurable Threshold for Alarms	From this release onwards, you can use the Cisco DNA Center to change threshold values and push new signature file to the APs.
WIPS: Forensics Capture Support	From this release onwards, you can enable forensics for aWIPS alarms. For more information, see the Advanced WIPS chapter.
USB Support for Cisco Catalyst Industrial Wireless 6300 Heavy Duty Series Access Points	USB support is added for Cisco Catalyst Industrial Wireless 6300 Heavy Duty series access points in this release.

Feature Name	Description and Documentation Link
Wireless Enabled Cisco Setup Command Facility	This feature introduces a Day 0 CLI wizard for Cisco Catalyst 9800 Series Wireless Controller platforms. For more information, see the Using the Cisco IOS-XE CLI - Cisco Setup Command Facility section in the following guides: • Cisco Catalyst 9800-40 Wireless Controller Hardware Installation Guide • Cisco Catalyst 9800-80 Wireless Controller Hardware Installation Guide • Cisco Catalyst 9800-CL Cloud Wireless Controller Installation Guide • Cisco Catalyst 9800-L Wireless Controller Hardware Installation Guide
Wireless Telemetry Scale Improvements	From this release onwards, the following set of OpenConfig XPath expressions are supported on the controller. • /access-points/access-point/radios/radio/state • /access-points/access-point/radios/radio/neighbors/neighbor • /access-points/access-point/radios/radio/neighbors/neighbor/state • /access-points/access-point/ssids/ssid/bssids/bssid/state/counters • /access-points/access-point/ssids/ssid/clients/client/state/counters • /access-points/access-point/ssids/ssid/clients/client/client-rf/state • /access-points/access-point/ssids/ssid/clients/client/client-connection/state • /access-points/access-point/system/aaa/server-groups/server-group/servers/server/radius/state • /joined-aps/joined-ap/state/opstate For more information, see the Model-Driven Telemetry chapter of the Programmability Configuration Guide, Cisco IOS XE Amsterdam 17.4.x.

Table 2: GUI Features Introduced or Modified on Cisco Catalyst 9800 Series Wireless Controllers

Feature Name	GUI Path
Advanced Scheduling Request	• **Configuration > Tags & Profiles > WLANs** • **Monitoring >Wireless > Clients**
Antenna Disconnection Detection	• **Configuration > Tags & Profiles > AP Join** • **Administration > Management > SNMP** • **Monitoring > Wireless > AP Statistics**
AP Reboot	• **Configuration > Wireless Setup > AP Provisioning**
BLE Management	• **Configuration > Wireless > Wireless Global** • **Monitoring > Wireless > AP Statistics**
BSS Coloring Support	• **Configuration > Radio Configurations > Parameters** • **Configuration > Tags & Profiles > RF**
Clean Air: Persistent Device Avoidance	• **Configurations > Radio Configurations > RRM** • **Monitoring > Wireless > Radio Statistics**
Copy Webauth Tar Bundle to Standby Bootflash	• **Administration > Management > Backup & Restore**
Define Syslog Hosts on Controller by Hostname	• **Troubleshooting > Logs**
Dynamic Protocol Pack Upgrade	• **Configuration > Services > Application Visibility**
Ethernet VLAN Tag on AP	• **Configuration > Wireless > Access Points**
Gateway IP Check with Native IPv6	• **Administration > Device**
Multi- LAG and Load Balancing Based on VLAN and SSO	• **Configuration > Services > Multicast**
OKC Disabling	• **Configuration > Tags & Profiles > WLANs > Add**
OpenDNS Integration	• **Configuration > Security > Threat Defense > Cisco DNS Layer Security Integration**

Feature Name	GUI Path
Overlapping Client IP Address in Flex Deployment	• **Configuration > Tags & Profiles > Flex** • **Monitoring > Wireless > Clients**
Persistent Device Avoidance	• **Configurations > Radio Configurations > RRM** • **Monitoring > Wireless > Radio Statistics**
Reboot APs by Groups	• **Configuration > Tags & Profiles > Tags > Site**
RFID Tag Support	• **Configuration > Wireless > Advanced > RFID** • **Monitoring > RFID**
RMI/Def Gateway Enhancements	• **Administration > Device**
Web UI for Golden Monitor for Packet Drops	• **Monitoring > General > System > CPU Utilization** • **Monitor > General > Ports**
WGB Support	• **Monitoring > Wireless > Clients**
WIPS: Forensics Capture Support	• **Configuration > Tags & Profiles > AP Join**
Wireless SNMP Traps	• **Administration > Management > SNMP**
MLD Snooping Per VLAN	• **Configuration > Services > Multicast**

Behavior Changes

- From Cisco IOS XE Bengaluru Release 17.4.1 onwards, routing protocols and HSRP are not supported.
- Embedded Wireless on Cisco Catalyst 9000 Series Switches for Single Secure Site Deployment (Non-SDA) using WebUI is not supported with this release.
- The following APs are not supported from this release:
  - Cisco Aironet 800 Series Access Point
  - Cisco Aironet 1570 Series Access Point
  - Cisco Aironet 1700 Series Access Point
  - Cisco Aironet 2700 Series Access Point
  - Cisco Aironet 3700 Series Access Point
- The Rogue Location Discovery Protocol (RLDP) feature is not supported from this release, and the following configuration, Privileged EXEC, and show commands are removed.

RLDP Configuration Commands

- **wireless wps rogue ap rldp alarm-only**
- **wireless wps rogue ap rldp alarm-only monitor-ap-only**
- **wireless wps rogue ap rldp auto-contain**
- **wireless wps rogue ap rldp auto-contain monitor-ap-only**
- **wireless wps rogue ap rldp retries**
- **wireless wps rogue ap rldp schedule**
- **wireless wps rogue ap rldp schedule day**

RLDP Privileged EXEC Command

- **wireless wps rogue ap mac-address rldp initiate**

RLDP show Commands

- **show wireless wps rogue ap rldp detailed**
- **show wireless wps rogue ap rldp in-progress**
- **show wireless wps rogue ap rldp summary**

- Disk space has been increased to 16 GB for QCOW2.
- From this release, you can reset all the APs associated to a site tag, in one click.
- You can use **show awips wlc-alarm** command to get information about the alarms detected by AWIPS, such as KRACK (WPA2 key reinstallation attack).
- You can disable 802.11ax Overlapping BSS Packet Detect (OBSS-PD) spatial reuse globally on a specific band and RF profile.
- If you configure 802.1x with session timeout between 0 and 299, Pairwise Master Key (PMK) cache is created with a timer of 1 day 84600 seconds.
- You can use the **parameter-map type umbrella** *custom_pmap* command to configure a customized Umbrella Parameter Map.
- The controller acts as a remote member when Cisco DNA Center is configured as the remote leader.
- Support is added for the syslog server configuration using the Fully Qualified Domain Name (FQDN).
- The request for converting an EWC noncapable device to EWC mode is rejected if the access point cannot be converted.
- Information about Wi-Fi Protected Access 3 (WPA3) Opportunistic Wireless Encryption (OWE) and WPA3 Simultaneous Authentication of Equals (SAE) is included in the rogue encryption description and in the **show wireless wps rogue ap detailed** command output, if WPA3 rogue is detected.
- Support is added for the Cisco Persistent Device Avoidance feature in the GUI.
- ACLs that are longer than 32 characters under the WLAN and policy profile may cause issues when you upgrade to Cisco IOS XE Bengaluru 17.4.x or later using ISSU. To avoid this, you should explicitly

unconfigure ACLs that are longer than 32 characters from the corresponding WLAN and the policy profile before the upgrade.

- We recommend that you use CLIs to upgrade embedded wireless on a Catalyst 9000 switch because wireless upgrade through GUI is not supported.
- From Cisco IOS XE Bengaluru Release 17.4.1 onwards, the AP name will be appended to the AP Cisco Discovery Protocol neighbor information for an upstream switch.
- Gateway monitoring is disabled when the Redundancy Management Interface (RMI) is administratively shut down. If the underlying Layer 2 or port channel interfaces are administratively shutdown while the RMI is still up, gateway monitoring continues. In such a scenario, all the actions associated with gateway reachability loss are triggered.
- In releases prior to Cisco IOS XE Bengaluru Release 17.4.1, when the **factory reset** command was executed on the controller in install mode resulted in controller booting up in ROMMON prompt, as backup of the current image was not taken. From Cisco IOS XE Bengaluru Release 17.4.1 onwards, the **factory reset** command on the controller takes the backup of the current image (in install as well as bundle mode) if the image is stored locally. If the image is not stored locally (booted through tftpboot/netboot) then the administrator needs to take the backup of the image before executing the **factory reset** command.
- From Cisco IOS XE Bengaluru Release 17.4.1 onwards, adaptive fast transition is supported only with WPA2 or WPA3 SSID. If you have an open SSID, ensure that you disable adaptive fast transition before the upgrade.

  In case, adaptive fast transition is not disabled before the upgrade, you can enable open SSID by performing the following steps:

  1. Disable adaptive fast transition (**no security ft adaptive**)
  2. Disable WPA (**no security wpa**)
  3. Disable WPA2 (**no security wpa wpa2**)
  4. Disable WPA3 (**no security wpa wpa3**)
  5. Enable the SSID (**no shutdown**)

- The following commands are used for antenna configuration in the Privileged EXEC mode, for Cisco Catalyst IW6300 Heavy Duty Series Access Points and Cisco Aironet 1562 Outdoor Access Points:
  - Device# **ap name Cisco-AP dot11 5ghz dot11n antenna A**
  - Device# **ap name Cisco-AP dot11 5ghz dot11n antenna B**

  An error message is displayed when you attempt to disable Antenna A. Only Antenna B can be disabled, since, at least one antenna must be in the **Enabled** state for AP operations.

MIBs

The following MIBs are modified:

- CISCO-LWAPP-AP-MIB.my
- CISCO-LWAPP-RF-MIB.my

- CISCO-LWAPP-RRM-MIB.my
- CISCO-LWAPP-DOT11-CLIENT-MIB.my
- CISCO-LWAPP-DOT11-MIB.my
- CISCO-WIRELESS-HOTSPOT-MIB.my
- CISCO-LWAPP-REAP-MIB.my
- CISCO-LWAPP-MOBILITY-EXT-MIB.my
- CISCO-LWAPP-MOBILITY-MIB.my
- CISCO-LWAPP-HA-MIB.my

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 5: Supported PIDs and Ports, on page 13 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 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 1-rack unit space and provides four 1-GE or 10-GE uplink ports.
Cisco Catalyst 9800 Wireless Controller for Cloud	A virtual form factor of the Catalyst 9800 Wireless Controller that can be deployed in a private cloud (supports ESXi, KVM, Microsoft Hyper-V, and NFVIS on ENCS hypervisors), or in the public cloud as Infrastructure as a Service (IaaS) in Amazon Web Services (AWS) and Google Cloud Platform (GCP) marketplace.
Cisco Catalyst 9800 Embedded Wireless Controller for Switch	The Catalyst 9800 Wireless Controller software for the Cisco Catalyst 9000 switches bring the wired and wireless infrastructure together with consistent policy and management. This deployment model supports only SD Access, which is a highly secure solution for small campuses and distributed branches.
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.

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, 6.7, and 7.0 • VMware ESXi vCenter 6.0, 6.5, 6.7 and 7.0
KVM	• Ubuntu 14.04.5 LTS, Ubuntu 16.04.5 LTS
AWS	AWS EC2 platform
NFVIS	ENCS 3.8.1 and 3.9.1

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

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 RP port 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. The following SFPs are supported: • GLC-BX-D • GLC-BX-U • GLC-EX-SMD • GLC-LH-SMD • GLC-SX-MMD • GLC-ZX-SMD • GLC-TE

Controller Model	Description
	The following enhanced SFPs are supported: • SFP-10G-AOC1M • SFP-10G-AOC2M • SFP-10G-AOC3M • SFP-10G-AOC5M • SFP-10G-AOC7M • SFP-10G-AOC10M • SFP-10G-SR • SFP-10G-SR-S • SFP-10G-SR-X • SFP-10G-ER • SFP-10G-ZR • SFP-H10GB-ACU7M • SFP-H10GB-ACU10M • DWDM-SFP10G-30.33 • DWDM-SFP10G-61.41
	The following QSFP+s are supported: • QSFP-40G-SR4 • QSFP-40G-LR4 • QSFP-40GE-LR4 • QSFP-40G-ER4 • QSFP-40G-SR4-S • QSFP-40G-LR4-S • QSFP-40G-SR-BD • QSFP-40G-BD-RX • QSFP-100G-SR4-S • QSFP-100G-LR4-S

Controller Model	Description
C9800-40-K9	Four 1/10-Gigabit Ethernet SFP or SFP+ ports and two power supply slots The following SFPs are supported: • GLC-BX-D • GLC-BX-U • GLC-LH-SMD • GLC-SX-MMD • GLC-EX-SMD • GLC-ZX-SMD • GLC-TE
	The following enhanced SFPs are supported: • SFP-10G-AOC1M • SFP-10G-AOC2M • SFP-10G-AOC3M • SFP-10G-AOC5M • SFP-10G-AOC7M • SFP-10G-AOC10M • SFP-10G-SR • SFP-10G-SR-S • SFP-10G-SR-X • SFP-10G-ER • SFP-10G-ZR • SFP-H10GB-ACU7M • SFP-H10GB-ACU10M • DWDM-SFP10G-30.33 - DWDM-SFP10G-61.41

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

Optics Modules

Cisco Catalyst 9800 Series Wireless Controller supports a wide range of optics. The list of supported optics is updated on a regular basis. See the tables at the following location for the latest transceiver module compatibility information:

https://www.cisco.com/en/US/products/hw/modules/ps5455/products_device_support_tables_list.html

Important Notes

- 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 carry forward.

Supported APs

The following Cisco APs are supported in this release.

Indoor Access Points

- Cisco Catalyst 9105AX (I) Access Points
  - VID 03 or earlier
- Cisco Catalyst 9105AX (W) Access Points
  - VID 01 or earlier
- Cisco Catalyst 9115AX (I/E) Access Points
- Cisco Catalyst 9117AX (I) Access Points
- Cisco Catalyst 9120AX (I/E) Access Points
  - VID 06 or earlier
- Cisco Catalyst 9120AX (P) Access Points
- Cisco Catalyst 9130AX (I/E) Access Points
  - VID 02 or earlier

  (For information about Cisco Catalyst 9105, 9120, or 9130 Access Points version support, see the Field Notice 72424.)
- Cisco Aironet 1815 (I/W), 1830 (I), 1840 (I), and 1852 (I/E) Access Points
- Cisco Aironet 2800 (I/E) Series Access Points
- Cisco Aironet 3800 (I/E/P) Series Access Points
- Cisco Aironet 4800 Series Access Points

Outdoor Access Points

- Cisco Aironet 1540 Series Access Points
- Cisco Aironet 1560 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

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

Supported Access Point Channels and Maximum Power Settings

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

For information about Cisco Wireless software releases that support specific Cisco AP modules, see the "Software Release Support for Specific Access Point Modules" section in the *Cisco Wireless Solutions Software Compatibility Matrix* document.

Compatibility Matrix

The following table provides software compatibility information.

Table 6: Compatibility Information

Cisco Catalyst 9800 Series Wireless Controller Software	Cisco Identity Services Engine	Cisco Prime Infrastructure	Cisco AireOS-IRCM Interoperability	Cisco DNA Center	Cisco DNA Spaces - Connector	Cisco DNA Spaces - On Premise
Bengaluru 17.4.x	3.0 2.7 2.6 2.4	3.9	8.10.171.0 8.10.162.0 8.10.151.0 8.10.142.0 8.10.130.0 8.8.130.0 8.5.182.104 8.5.176.2 8.5.164.216 8.5.152.103	See Cisco DNA Center Compatibility Information	2.3 2.2	10.6.3

GUI System Requirements

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

Table 7: Hardware Requirements

Processor Speed	DRAM	Number of Colors	Resolution	Font Size
233 MHz minimum[1]	512 MB[2]	256	1280 x 800 or higher	Small

[1] We recommend 1 GHz.
[2] 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 recommendthat you increase the number of VTY lines to 50.

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

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

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

Before You Upgrade

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

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

- 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.
- Rolling AP upgrade, which is a part of the ISSU feature, is not supported for mesh APs.

The following Wave 1 APs are not supported from 17.4 to 17.9.2, 17.10.x and 17.11.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 were 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.
- Feature support is on parity with 17.3.x release. Features introduced in 17.4.1 or later are not supported on these APs in 17.9.3 release.
- You can migrate directly to 17.9.3 from 17.3.x, where x=4c or above.

- 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
```

Note 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.

- You might observe a high Confd CPU when full synchronization occurs between NETCONF datastore and Cisco IOS configuration. This behavior is normal and is triggered by the **line vty** command.
- From Cisco IOS XE Amsterdam 17.3.1 onwards, the Cisco Catalyst 9800-CL Wireless Controller requires 16 GB of disk space for new deployments.

  If you are upgrading to Cisco IOS XE Amsterdam 17.3.x from a previous release, resizing of disk space is not supported. If the current disk space is lesser than 16 GB, you need to redeploy the VM to meet the new disk space requirements.
- Fragmentation lower than 1500 is not supported for RADIUS packets generated by wireless clients in 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 following order:

  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, as given in the following order, 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 DNA 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 DNA Centre.
- From Cisco IOS XE Bengaluru 17.4.1 onwards, session timeout under the policy profile is supported.
- Clicking on the **Clear** button does not clear the entries on the **Monitor > RFID** page of the GUI. We recommend that you refresh the page to see the cleared entries.
- 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 carry forward.
- When you encounter the SNMP error "SNMP_ERRORSTATUS_NOACCESS 6", it means that the specified SNMP variable is not accessible.

Upgrade Path to Cisco IOS XE Bengaluru 17.4.x

Table 8: Upgrade Path to Cisco IOS XE Bengaluru 17.4.x Release

Current Software	Upgrade Path to Cisco IOS XE Bengaluru 17.4.x Release
16.10.x	Upgrade first to 16.12.5 and then to 17.4.x.
16.11.x	Upgrade first to 16.12.5 and then to 17.4.x.
16.12.x	You can upgrade directly to 17.4.x.
17.1.x	Upgrade first to 17.3 and then to 17.4.x.
17.2.x	You can upgrade directly to 17.4.x.
17.3.x	You can upgrade directly to 17.4.x.

Upgrading the Controller Software

For information on the upgrade process and the methods to upgrade the Cisco Catalyst 9800 Series Wireless Controller software, see the "Upgrading the Cisco Catalyst 9800 Wireless Controller Software" chapter of the Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide.

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 Bengaluru 17.4.x
- **Image Names**:
  - C9800-CL-universalk9_kvm.17.04.01.run
  - C9800-CL-universalk9_esxi.17.04.01.run
  - C9800-CL-universalk9_nfvis.17.04.01.run

Software Installation Commands

Cisco IOS XE, Bengaluru, 17.4.x	
To install and activate a specified file, and to commit changes to be persistent across reloads, run the following command: **device# install add file** *filename* **[activate |commit]** To separately install, activate, commit, end, or remove the installation file, run the following command: **device# install ?** **Note** We recommend that you use the GUI for installation.	
add file tftp: *filename*	Copies the install file package from a remote location to a device, and performs a compatibility check for the platform and image versions.
activateauto-abort-timer]	Activates the file and reloads the device. The **auto-abort-timer** keyword automatically rolls back image activation.
commit	Makes changes that are persistent over reloads.
rollback to committed	Rolls back the update to the last committed version.
abort	Cancels file activation, and rolls back to the version that was running before the current installation procedure started.
remove	Deletes all unused and inactive software installation files.

Licensing

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

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

Interoperability with Clients

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

The following table lists the configurations used for testing client devices.

Table 9: Test Configuration for Interoperability

Hardware or Software Parameter	Hardware or Software Type
Release	Cisco IOS XE, Bengaluru, 17.4.x

Hardware or Software Parameter	Hardware or Software Type
Cisco Wireless Controller	See Supported Hardware, on page 12.
Access Points	See Supported APs.
Radio	• 802.11ax • 802.11ac • 802.11a • 802.11g • 802.11n
Security	Open, PSK (WPA2-AES), 802.1X (WPA2-AES) (EAP-FAST, EAP-TLS) 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 10: Client Types

Client Type and Name	Driver or Software Version
Wi-Fi 6 Devices (Mobile Phone and Laptop)	
Apple iPhone 11	iOS 14.1
Apple iPhone SE 2020	iOS 14.1
Dell Intel AX1650w	Windows 10 (21.90.2.1)
Dell Latitude 5491 (Intel AX200)	Windows 10 Pro (21.40.2)
Samsung S20	Android 10
Samsung S10 (SM-G973U1)	Android 9.0 (One UI 1.1)
Samsung S10e (SM-G970U1)	Android 9.0 (One UI 1.1)
Samsung Galaxy S10+	Android 9.0
Samsung Galaxy Fold 2	Android 10
Samsung Galaxy Flip Z	Android 10
Samsung Note 20	Android 10
Laptops	
Acer Aspire E 15 E5-573-3870 (Qualcomm Atheros QCA9377)	Windows 10 Pro (12.0.0.832)

Client Type and Name	Driver or Software Version
Apple Macbook Air 11 inch	OS Sierra 10.12.6
Apple Macbook Air 13 inch	OS Catalina 10.15.4
Apple Macbook Air 13 inch	OS High Sierra 10.13.4
Macbook Pro Retina	OS Mojave 10.14.3
Macbook Pro Retina 13 inch early 2015	OS Mojave 10.14.3
Dell Inspiron 2020 Chromebook	Chrome OS 75.0.3770.129
Google Pixelbook Go	Chrome OS 84.0.4147.136
HP chromebook 11a	Chrome OS 76.0.3809.136
Samsung Chromebook 4+	Chrome OS 77.0.3865.105
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 (18.32.0.5)
Dell Latitude E5540 (Intel Dual Band Wireless AC7260)	Windows 7 Professional (21.10.1)
Dell XPS 12 v9250 (Intel Dual Band Wireless AC 8260)	Windows 10 (19.50.1.6)
Dell Latitude 5491 (Intel AX200)	Windows 10 Pro (21.40.2)
Dell XPS Latitude12 9250 (Intel Dual Band Wireless AC 8260)	Windows 10 Home (21.40.0)
Lenovo Yoga C630 Snapdragon 850 (Qualcomm AC 2x2 Svc)	Windows 10 (1.0.10440.0)
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	iOS 13.5
Apple iPad Air2 MGLW2LL/A	iOS 12.4.1
Apple iPad Mini 4 9.0.1 MK872LL/A	iOS 11.4.1
Apple iPad Mini 2 ME279LL/A	iOS 12.0
Microsoft Surface Pro 3 – 11ac	Qualcomm Atheros QCA61x4A
Microsoft Surface Pro 3 – 11ax	Intel AX201 chipset. Driver v21.40.1.3
Microsoft Surface Pro 7 – 11ax	Intel Wi-Fi chip (HarrisonPeak AX201) (11ax, WPA3)

Client Type and Name	Driver or Software Version
Microsoft Surface Pro X – 11ac & WPA3	WCN3998 Wi-Fi Chip (11ac, WPA3)
Mobile Phones	
Apple iPhone 5	iOS 12.4.1
Apple iPhone 6s	iOS 13.5
Apple iPhone 8	iOS 13.5
Apple iPhone X MQA52LL/A	iOS 13.5
Apple iPhone 11	iOS 14.1
Apple iPhone SE MLY12LL/A	iOS 11.3
ASCOM SH1 Myco2	Build 2.1
ASCOM SH1 Myco2	Build 4.5
ASCOM Myco 3 v1.2.3	Android 8.1
Drager Delta	VG9.0.2
Drager M300.3	VG2.4
Drager M300.4	VG2.4
Drager M540	DG6.0.2 (1.2.6)
Google Pixel 2	Android 10
Google Pixel 3	Android 11
Google Pixel 3a	Android 11
Google Pixel 4	Android 11
Huawei Mate 20 pro	Android 9.0
Huawei P20 Pro	Android 9.0
Huawei P40	Android 10
LG v40 ThinQ	Android 9.0
One Plus 8	Android 10
Oppo Find X2	Android 10
Redmi K20 Pro	Android 10
Samsung Galaxy S7	Andriod 6.0.1
Samsung Galaxy S7 SM - G930F	Android 8.0
Samsung Galaxy S8	Android 8.0
Samsung Galaxy S9+ - G965U1	Android 9.0
Samsung Galaxy SM - G950U	Android 7.0

Client Type and Name	Driver or Software Version
Sony Experia 1 ii	Android 10
Sony Experia xz3	Android 9.0
Xiaomi Mi10	Android 10
Spectralink 8744	Android 5.1.1
Spectralink Versity Phones 9540	Android 8.1
Vocera Badges B3000n	4.3.2.5
Vocera Smart Badges V5000	5.0.4.30
Zebra MC40	Android 5.0
Zebra MC40N0	Android 4.1.1
Zebra MC92N0	Android 4.4.4
Zebra TC51	Android 7.1.2
Zebra TC52	Android 8.1.0
Zebra TC55	Android 8.1.0
Zebra TC57	Android 8.1.0
Zebra TC70	Android 6.1
Zebra TC75	Android 6.1.1
Printers	
Zebra QLn320 Printer	LINK OS 6.3
Zebra ZT230 Printer	LINK OS 6.3
Zebra ZQ310 Printer	LINK OS 6.3
Zebra ZD410 Printer	LINK OS 6.3
Zebra ZT410 Printer	LINK OS 6.3
Zebra ZQ610 Printer	LINK OS 6.3
Zebra ZQ620 Printer	LINK OS 6.3
Wireless Module	
Intel 11ax 200	Driver v22.20.0
Intel AC 9260	Driver v21.40.0
Intel Dual Band Wireless AC 8260	Driver v19.50.1.6

Caveats

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

Note All incremental releases 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 a caveat, click the corresponding identifier.

Open Caveats for Cisco IOS XE, Bengaluru, 17.4.1

Caveat ID	Description
CSCvr16233	Cisco Aironet 2802 AP beacon loss issue.
CSCvs77557	Cisco Aironet 3802 AP fails to acknowledge EAP frames.
CSCvv40240	AP is sending large invalid field_count and template id that causes memory leak in the controller.
CSCvv52618	Cisco Aironet 2800 and 3800 APs exhibit choppiness during the multicast voice call.
CSCvv78264	MESH: Cisco Aironet 1542 Outdoor AP does not converge to Cisco Aironet 1572 Outdoor AP.
CSCvv78719	Certain APs (2800/3800/4800/1560/6300) fails to transmit data frame to the client from the radio interface.
CSCvv79700	Fault tolerance is broken in FlexConnect APs due to vendor_set_ccx_elements.
CSCvv81814	Cisco Aironet 1852 and 1832 APs are facing firmware assert with 0x00942D74/0x00942D79 on 2.4 or 5-Ghz radio.
CSCvv95733	Some commands are not applied while using iosxe_config.txt to load configuration to Cisco Catalyst 9800-CL Wireless Controller using Kernel-Based Virtual Machine (KVM).
CSCvv97156	Cisco Catalyst 9130AX Series APs are dropping some uplink packets from macbooks.

Caveat ID	Description
CSCvv99213	Cisco Catalyst 9130AXE AP is not taking RF tag power settings on slot 2.
CSCvv99765	Cisco Catalyst 9120 AP stops forwarding client traffic after random roam events.
CSCvw00891	FlexConnect APs are experiencing radio reset during fault tolerance scenario.
CSCvw01612	Cisco Catalyst 9130AX Series AP is not sending M1 over the air.
CSCvw02981	Cisco Aironet 2802 AP shows sudden drop in TX power level.
CSCvw08044	Cisco Aironet 2802 and 3802 APs are crashing due to watchdog reset.
CSCvw15298	Cisco Embedded Wireless Controller for an AP is not forwarding downstream traffic after active AP failover.
CSCvw16307	Cisco OfficeExtend access point (OEAP) crashes after running network diagnostics.
CSCvw19820	Controller is unable to push SSIDs while doing a configuration change on policy profile.
CSCvw20363	Cisco Aironet 2800 and 3800 APs: Workgroup bridge (WGB) fails to connect through Protected Extensible Authentication Protocol (PEAP) if client certificate is not installed.
CSCvw21621	Controller ignores DHCP offer for client.
CSCvw25812	AP is not sending ADD Traffic Stream (ADDTS) response frame when Protected Management Frame (PMF) is enabled.
CSCvw27910	Cisco Aironet 2800 AP shows slowness while downloading image from the controller.
CSCvw30043	Cisco Aironet 3800 AP is randomly not sending traffic to client queue 0 after dot1x session-timeout.
CSCvw30197	Cisco Aironet 2802 AP radio is crashing due to firmware exception.
CSCvw31938	WNCD_DB is stuck with tbl_bssid_dms when 11v Directed Multicast Service (DMS) is enabled.
CSCvw32098	Cisco switches connected to Wave2 APs generate CDP-4-DUPLEX_MISMATCH.
CSCvw32970	Wave 2 AP crash due to FIQ/NMI reset.
CSCvw33498	Cisco Catalyst 9800-CL Wireless Controller: High Availability is suddenly broken and the secondary controller fails to come up.

Caveat ID	Description
CSCvw33504	Cisco Catalyst 9117 AP: Kernel Panic NSS firmware crash is observed.
CSCvw35589	Controller displays incorrect antenna gain.
CSCvw35611	Cisco Catalyst 9800-L-C Wireless Controller is crashing due to IntelResetRequest.
CSCvw35698	Cisco Aironet 3700 series APs fail to join controller.
CSCvw36167	Implement legitimate debugs to troubleshoot multi-user, multiple-input, multiple-output (MU-MIMO) transmission failures.
CSCvw37503	Cisco Catalyst 9120 and 9115 APs are not processing protected Neighbor Discovery Protocol (NDP) from other AP models except for NDP tx by Cisco Catalyst 9115 AP.
CSCvw39267	Cisco Aironet 2800 AP is crashing due to FIQ/NMI reset.
CSCvw40346	AP is not responding to probe requests.
CSCvw44971	Cisco Aironet 1832 AP unexpectedly reloads due to kernel panic.
CSCvw47518	SNMP OID gives incorrect client count.
CSCvw48334	Cisco Aironet 3802 AP: "Object read info failed status = TAM_LIB_ERR_READ_FAILURE" causing DTLS failures.
CSCvw67128	Smart Liensing Policy: Purchase information should be protected and shouldn't be able to erase.

Resolved Caveats for Cisco IOS XE, Bengaluru, 17.4.1

Caveat ID	Description
CSCvr03516	Need **show mac address-table tree** command.
CSCvs03712	Data rates should be updated when the client moves from one AP to another.
CSCvs48567	Unable to delete a client using SNMP OID bsnMobileStationDeleteAction.
CSCvs65189	AP Ethernet PHY interop issue when using IEEE Fast Retrain when connected at mGig speeds.
CSCvt19736	IEEE 802.11ax feature is enabled automatically after upgrading from 16.12.2s to 17.1.1s.
CSCvt55572	Client 360 Assurance: Client RX packets reported on Cisco DNA-C is wrong.

Caveat ID	Description
CSCvt63940	Authentication fails for some clients, when local authentication is configured in the policy profile..
CSCvt75852	Brand new AP joins the anchor controller with a different mobility group name.
CSCvt79712	Client is deleted due to the reason code: "CO_CLIENT_DELETE_REASON_NOOP".
CSCvt83553	Cisco Catalyst 9800-40 Wireless Controller: Stale FMAP-FP/CPP tunnel issue is observed.
CSCvt83796	APs do not apply client QoS policy in FlexConnect local-switching and local-auth.
CSCvt96686	Controller is showing the following message during client join or re-association: "SWPORT-4-MAC_CONFLICT: Dynamic mac conflict with WlClient:.
CSCvt96968	The default run-time constraint leads to abort or crash of processes.
CSCvu03389	Controller is remarking client Differentiated Services Code Point (DSCP) packets to zero when voice Call Admission Control (CAC) is configured.
CSCvu03863	RF profile max clients configuration is not working.
CSCvu06366	The **show ap name tag detail** command output is not displaying WLAN profile name.
CSCvu12784	The output of the **show ap location details** command does not show AP MAC addresses in a contiguous manner.
CSCvu14009	CAPWAPv6 APMGR is not sending AP name and updates the load balancer with default-policy-tag.
CSCvu14381	Controller reloads unexpectedly.
CSCvu15936	FlexConnect local-sw client is not assigned to VLAN1 when VLAN assigment is done through AAA.
CSCvu16348	Flexconnect RLAN-VLAN tag is not working when used with a named VLAN.
CSCvu17521	Interface speed for the AP is showing as *None* in Cisco Prime.
CSCvu17670	In an HA RP based pairing, configuring RMI (IPv4) on the primary or active controller crashes the standby controller.
CSCvu19000	Cisco Catalyst 9800-L Wireless Controller goes administratively down after running **reload** command following a factory reset.

Caveat ID	Description
CSCvu19379	Do not present "host mode" configuration options when the RLAN profile is set to open.
CSCvu19436	CWA + Dot1x is not working.
CSCvu19988	Disabilng High Availability is not erasing the configuration on the standby controller, which results in network conflict.
CSCvu20686	EWC Day0: Internal AP doesn't accept address from IOSd DHCP server, when powered from switch.
CSCvu22410	The dot11n and dot11ac are disabled and configuration is saved. When the controller reloads, they are enabled again.
CSCvu23655	Traffic drop is observed when Address Resolution Protocol (ARP) response is sent from wired client to wireless client.
CSCvu23990	Show command output displays that 802.11ac is not supported on XOR radios of APs.
CSCvu25924	When vlan-id1 is applied to policy profile, FlexConnect profile has native X VLAN clients assigned to X.
CSCvu29653	Web UI is not updating the correct TX power of AP while configuring custom RF profile.
CSCvu30088	WNCD kernel process memory leak.
CSCvu31306	Central Web Authentication (CWA) access control lists (ACLs) is removed from the existing FlexConnect AP, when a new FlexConnect profile is created with the same ACL.
CSCvu34813	AP operating in EG and BH country code allows to configure incorrect channels.
CSCvu37330	Client is getting deleted due to DOT11_STATUS_DENIED_RATES.
CSCvu37389	When AP's interface operational status goes down, an SNMP trap is sent, and the device reloads.
CSCvu38894	AP power is changing even when it is configured as static; the value of Tx power is not changing.
CSCvu38986	Memory leak is observed under wncd_x due to CAPWAP messaging.
CSCvu42093	Controller tag assigment using filters is working correctly up to 102 filters, new filters are causing the previous ones to fail.
CSCvu44330	Memory leak is observed under process SACRcvWQWrk2 when Smart Licensing feature is enabled.

Caveat ID	Description
CSCvu47560	The client goes into exclusionlist even if client exclusion is disabled.
CSCvu47855	DHCP Behaviour change feature.
CSCvu50579	AP coverage hole with 0 clients.
CSCvu53318	Controller is not sending off channel scan defer attributes.
CSCvu53459	Controller reboots unexpectedly in WNCD process.
CSCvu54413	AIRESPACE-WIRELESS-MIB RFID OID support is required.
CSCvu54641	Cisco Catalyst 9800-80 Wireless Controller: High Availability is not working after upgrading to 17.x from 16.2.3
CSCvu57730	Controller reboots unexpectedly in CPP (data path).
CSCvu58564	AP is using non-allowed channel on dual radio when the setting is changed to 5-Ghz.
CSCvu58782	License level doesn't show up in prompt level.
CSCvu60464	Deletion and creation of second control plane IP fails due to RPC ordering.
CSCvu60723	Several pp-qos errors are observed in cpp logs, which is bloating the tracelogs space.
CSCvu64805	Stale entries are shown in the **show wireless device-tracking database ip** command output.
CSCvu64811	AP disjoins over public IP during upgrade and downgrade.
CSCvu65380	Cisco Aironet 2700 AP is unable to join the controller, as max radio is reported as zero.
CSCvu66388	WNCD crash is observed in WTP event LED brightness payload processing.
CSCvu71187	AID leak is observed with RLANs.
CSCvu71871	Cisco Catalyst 9800-80 Wireless Controller crashes with SIGSEGV while removing timer RB tree color.
CSCvu71908	The *ledflash indefinite* configuration under the ap-profile should not be enabled by default.
CSCvu73277	WNCD crash is observed after AP join.
CSCvu73873	Cisco Catalyst 9800-80 Wireless Controller is sending client traffic out of AP manager interface.
CSCvu74722	APs are getting mapped to default site tag after stateful switchover (SSO).

Caveat ID	Description
CSCvu78070	Controller crash is observed on WNCD process.
CSCvu78124	Client join SNMP notifications are showing incorrect and missing values.
CSCvu78679	Cisco Aironet 2800 is dropping off from the controller due to malformed inactive_client_payload.
CSCvu92898	Cisco Catalyst 9800-L Wireless Controller: WNCD crash due to process rrm_client_chd assertion failed.
CSCvu95504	Controller reloads unexpectedly while doing MAC comparison.
CSCvv00474	MESH: Changing BH bandwidth requires reboot of AP in order to get good throughput for ethernet client.
CSCvv02670	Controller is showing incorrect AP CDP information.
CSCvv22536	Client moves to RUN state without Extensible Authentication Protocol (EAP).
CSCvv34749	Controller sends its private IP in discovery response even when it is not supposed to.
CSCvv39859	The site tag name is not sent in the remote id, instead AP MAC is sent.

Troubleshooting

For the most up-to-date, detailed troubleshooting information, visit the Cisco TAC website at:

https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/213949-wireless-debugging-and-log-collection-on.html

Go to **Product Support** and select your product from the list or enter the name of your product. Look under **Troubleshoot and Alerts** to find information about the problem that you are experiencing.

Related Documentation

Information about Cisco IOS XE is available at:

https://www.cisco.com/c/en/us/products/ios-nx-os-software/ios-xe/index.html

Cisco Validated Designs documents are available at:

https://www.cisco.com/go/designzone

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use the Cisco MIB Locator found at:

http://www.cisco.com/go/mibs

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

The installation guide for your controller is available at:

- Hardware Installation Guides

The user guide for Cisco User Defined Network Mobile Application is available at: https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/config-guide/b_wl_udn_mobile_app_user_guide.html

For all Cisco Wireless Controller software-related documentation, see:

https://www.cisco.com/c/en/us/support/wireless/catalyst-9800-series-wireless-controllers/tsd-products-support-series-home.html

Cisco Catalyst 9800 Wireless Controller Data Sheets

- Cisco Catalyst 9800-CL Wireless Controller: https://www.cisco.com/c/en/us/products/collateral/wireless/catalyst-9800-cl-wireless-controller-cloud/nb-06-cat9800-cl-cloud-wirel-data-sheet-ctp-en.html
- Cisco Catalyst 9800-80 Wireless Controller: https://www.cisco.com/c/en/us/products/collateral/wireless/catalyst-9800-series-wireless-controllers/nb-06-cat9800-80-wirel-mod-data-sheet-ctp-en.html
- Cisco Catalyst 9800-40 Wireless Controller: https://www.cisco.com/c/en/us/products/collateral/wireless/catalyst-9800-series-wireless-controllers/nb-06-cat9800-wirel-cont-data-sheet-ctp-en.html
- Cisco Catalyst 9800-L Wireless Controller: https://www.cisco.com/c/en/us/products/collateral/wireless/catalyst-9800-series-wireless-controllers/datasheet-c78-742434.html

Cisco Embedded Wireless Controller on Catalyst Access Points

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

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

Wireless Products Comparison

- Use this tool to compare the specifications of Cisco wireless APs and controllers:

  https://www.cisco.com/c/en/us/products/wireless/wireless-lan-controller/product-comparison.html

- Wireless LAN Compliance Lookup:

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

- Cisco AireOS to Cisco Catalyst 9800 Wireless Controller Feature Comparison Matrix:

  https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-8/AireOS_Cat_9800_Feature_Comparison_Matrix.html

Cisco Prime Infrastructure

Cisco Prime Infrastructure Documentation

Cisco Connected Mobile Experiences

Cisco Connected Mobile Experiences Documentation

Cisco DNA Center

Cisco DNA Center Documentation

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.