Release Notes for Cisco Catalyst 9800 Series Wireless Controller, Cisco IOS XE Bengaluru 17.5.x

First Published: 2021-03-31

Release Notes for Cisco Catalyst 9800 Series Wireless Controller, Cisco IOS XE Bengaluru 17.5.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 Bengaluru 17.5.1

Table 1: New and Modified Software Features

Feature Name	Description and Documentation Link
Support for Self-Identifying Antennas	From this release, Self-Identifying Antennas (SIA) are supported on Cisco Catalyst 9800 Series Wireless Controller. **Note** If you are using an older version of the controller, we recommend that you upgrade the controller to the 17.5.x version, for smooth functioning of the antenna.
11ac Very High Throughput (VHT) MU-MIMO Support on Cisco Catalyst 9105	From this release, 11ac Very High Throughput (VHT) MU-MIMO is supported on Cisco Catalyst 9105.
11ax High Efficiency (HE) MU-MIMO Support on Cisco Catalyst 9100 Series AX APs: 9105, 9115, and 9120	From this release, 11ax High Efficiency (HE) MU-MIMO is supported on the following Cisco Catalyst 9100 Series AX APs: 9105, 9115, and 9120.
11ax OFDMA 16 Users Support	From this release, 11ax OFDMA supports up to eight users per PPDU on the uplink and 16 users per PPDU on the downlink, on the following Cisco Catalyst 9100 Series AX APs: 9105, 9115, and 9120.
Adaptive Client Load-Based EDCA	This feature dynamically changes EDCA parameters of clients based on the active client and load that significantly reduce collisions. For more information, see the Adaptive Client Load-Based EDCA chapter.

Feature Name	Description and Documentation Link
Auto-Upgrade	This feature enables the standby controller to upgrade to active controller's software image, so that both controllers can form high availability (HA). For more information, see the Auto-Upgrade chapter.
Indicator for CAC Running on AP for DFS Channels	Whenever Channel Availability Check (CAC) is run on an AP radio, # is added right next to the channel in the output of the "show ap dot11 5ghz summary" command. For more information, see the Dynamic Frequency Selection chapter.
DHCP Relay Behaviour	This feature aligns the setting of DHCP relay parameters, such as, Gateway IP address, Option 82, and DHCP server address with the Cisco AireOS behaviour. For more information, see the DHCP for WLANs chapter.
Disable Random MAC Clients	In Cisco IOS XE Release 17.5.1, the controller is equipped with a knob that denies the entry of clients with random MAC addresses into the network. When the **local-admin-mac deny** command is enabled on the controller, the association of any client joining the network with a random MAC address is rejected. By default, this feature is disabled on the controller. The following command was introduced: • **local-admin-mac deny** For more information, see the Disabling Clients with Random Access chapter.
Enable or Disable 11ax Features per SSID	From this release onwards, a 11ax configuration knob, per VAP, is introduced under the WLAN profile. When 11ax is enabled per radio, the 11ac clients can scan or connect to the SSID, if the beacon has 11ax information elements. For more information, see the 802.11ax Per Virtual Access Point chapter.
Predownloading an Image to an Access Point	This feature minimizes network outages, downloads an upgrade image to an access point from the device without resetting the access point or losing network connectivity. For more information, see the Programmability Configuration Guide, Cisco IOS XE Bengaluru 17.5.x.

Feature Name	Description and Documentation Link
Intermediate CA Support for AP Authentication	This feature is an extension support to the existing Locally Significant Certificates (LSC) feature. If your Locally Significant Certificate has been issued by an Intermediate CA, you must import the complete chain of CA certificates into the Trustpool. Otherwise, you will not be able to provision the APs without the complete chain being present on the controller. This is not required if the certificate has been issued by a Root CA. The following commands were introduced: • **crypto pki trustpoint** • **crypto pki trust pool import terminal** • **crypto pki trustpool clean** For more information, see the Locally Significant Certificates chapter.
Larger memory and NAND flash upgrade for IW6300 and ESW6300	Hardware upgrade of 2048 MB DDR4 memory and 8-bit ECC 1024MB NAND flash for Cisco Catalyst IW6300 Heavy Duty Series and 6300 Series Embedded Services Access Points is added in this release. For more information, see the Cisco Catalyst IW6300 Heavy Duty Series Access Point Hardware Installation Guide.
Multiple Cipher Support	From this release, Elliptic Curve Diffie-Hellman Ephemeral (ECDHE)/Galois Counter Mode (GCM) ciphersuite with perfect forward secrecy (PFS) capability is added in the default-list along with existing AES128-SHA. All the supported AP models, except legacy Cisco IOS APs, will prioritize this PFS ciphersuite for CAPWAP-DTLS under default configuration. For more information, see the Multiple Cipher Support chapter.
Neighbor Discovery Protocol Mode on the Cisco Catalyst 9124AX Outdoor Access Points.	In Cisco Catalyst 9124AX Outdoor Access Points, the Neighbor Discovery Protocol (NDP) packets are transmitted either ON-channel on the serving radio or OFF-channel on the RF ASIC conventional radio. The controller supports NDP mode for Cisco Catalyst 9124AX Outdoor APs, based on the deployment needs. In Cisco IOS XE Bengaluru 17.5.1 Release, Cisco Catalyst 9124AX Outdoor APs support both On-Channel and Off-Channel NDP. The following commands were introduced: • **ap dot11 {24ghz | 5ghz} rrm ndp-mode {auto | off-channel}** • **ndp-mode {auto | off-channel}** For more information, see the Neighbor Discovery Protocol Mode on Access Points chapter.

Feature Name	Description and Documentation Link
OEAP Link Test	This feature allows you to determine the DTLS upload, link latency, and jitter of the link between an AP and the controller. The following commands were introduced: • **ap name network-diagnostics** • **show flexconnect office-extend diagnostics** For more information, see the OEAP Link Test chapter.
PKI Operational Data	PKI Operational Data allows to gather current status of the device using Netconf. To view the operational data listed below, use these commands: **show crypto pki trustpoint status**, **show crypto pki certificate verbose**, and **show crypto pki counters**. • Certificate: availability, serial number, subject name, issuer name, validity start, and validity end • Associated trustpoints • Certificate: storage location, usage, and key type • Key exportability • Certificate MD5 fingerprint • PKI sessions: started, ended, and active • Validations: successful, failed, bypassed, and pending • CRLs: checked, fetch attempts, failed attempts, and rejected busy fetching • AAA authorizations

Feature Name	Description and Documentation Link
Port Channel Numbering/Label	From this release, you can change the port channel interface numbers between 1 and 64 on the following Cisco Catalyst 9800 Series Wireless Controllers: • Cisco Catalyst 9800-CL Wireless Controller for Cloud: The available range on the CLI is 1 to 64. The maximum supported port-channel interfaces are 64. • Cisco Catalyst 9800-L Wireless Controller: The available range on the CLI is 1 to 64. The maximum supported port-channel interfaces are 14. • Cisco Catalyst 9800-40 Wireless Controller: The available range on the CLI is 1 to 64. The maximum supported port-channel interfaces are 16. • Cisco Catalyst 9800-80 Wireless Controller: The available range on the CLI is 1 to 64. The maximum supported port-channel interfaces are 64. For more information, see the Link Aggregation Group chapter.
Prioritizing AWIPS over Hyperlocation for Third Radio Handling	From this release, Advanced Wireless Intrusion Prevention System (aWIPS) security gets a higher priority over Hyperlocation. For more information, see the Advanced WIPS chapter.
Standby Monitoring Enhancements	This feature monitors the standby CPU or memory information from the active controller. Also, this feature independently monitors the standby controller using SNMP for the interface MIB. The **cLHaPeerHotStandbyEvent** and **cLHaPeerHotStandbyEvent** MIB objects in **CISCO-HA-MIB** are used to monitor the standby HA status. For more information, see the High Availability chapter.
Support for both MIC and LSC APs to Join the Same Controller	From this release, the new authorization policy configuration allows MIC access points (APs) to join the LSC-deployed controller, so that the LSC and MIC APs can co-exist in the controller, at the same time. The following commands were introduced: • **ap auth-list ap-cert-policy allow-mic-ap trustpoint** • **ap auth-list ap-cert-policy** {**mac-address** *H.H.H* | **serial-number** *serial-number-ap*} **policy-type mic** For more information, see the Locally Significant Certificates chapter.

Feature Name	Description and Documentation Link
Track AP CPU Usage for AP Health	From this release, you can track the CPU utilization and the memory usage of an AP, and monitor the health of the AP by generating real-time AP statistics. The following commands were introduced: • **statistics ap-system-monitoring enable** • **statistics ap-system-monitoring sampling-interval** • **statistics ap-system-monitoring stats-interval** • **statistics ap-system-monitoring alarm-enable** • **statistics ap-system-monitoring alarm-hold-time** • **statistics ap-system-monitoring alarm-retransmit-time** • **statistics ap-system-monitoring cpu-threshold** • **statistics ap-system-monitoring mem-threshold** • **trapflags ap ap-stats** For more information, see the Access Points Real-Time Statistics chapter.
USB Support for IW6300	USB configuration is supported for Cisco Catalyst Industrial Wireless 6300 Heavy Duty series access points in this release. For more information, see the USB Support section in the Cisco Catalyst IW6300 Heavy Duty Series and 6300 Series Embedded Services Access Point Software Configuration Guide.
View AP LLDP Neighbor Information from Controller	The following Access Point Link Layer Discovery Protocol (LLDP) **show** commands are introduced: • **show ap lldp neighbors** • **show ap lldp neighbors detail** • **show ap name** *ap-name* **lldp neighbors** • **show ap name** *ap-name* **lldp neighbors detail**
WIPS Additional Signatures	In the Cisco IOS XE Amsterdam 17.3.1 and earlier releases, only 10 signatures were supported. From Cisco IOS XE Bengaluru 17.5.1, 15 signatures are supported. For more information, see the Advanced WIPS chapter.

Feature Name	Description and Documentation Link
WPA/WPA2-PSK-WebAuth on MAC Filter Failure	From this release, you can configure WLAN for Web Authentication on MAC Authentication Bypass Failure with Secure Agile Exchange (SAE), Opportunistic Wireless Encryption (OWE), and Pre-Shared Key (PSK). The following commands were introduced: • **security wpa akm owe** • **security wpa akm sae** For more information, see the Multiple Authentications for a Client and Wireless Guest Access chapters.

Table 2: New and Modified GUI Features

Feature Name	GUI Path
Adaptive Client Load-Based EDCA	• **Configuration** > **Radio Configurations** > **Parameters**
AP Real-Time Statistics	• **Configuration** > **AP Join** > **Add Window** > **AP Tab** > **AP Statistics Tab**
Enable or Disable 11ax Features per SSID	• **Configuration** > **Tags & Profiles** > **WLANs**
Fastlane+	• **Configuration** > **Tags & Profiles** > **WLANs** > **Advanced**
Intermediate CA Support for AP Authentication	• **Configuration** > **Security** > **PKI Management**
Neighbor Discovery Protocol Mode on the Cisco Catalyst 9124AX Outdoor Access Points.	• **Configuration** > **Tags & Profiles** > **RF** > **Add** • **Configuration** > **Radio Configuration** > **RRM** > **5GHz Band/2.4GHz Band** > **General** • **Monitoring** > **Wireless** > **Radio Statistics**
OEAP Link Test	• **Monitoring** > **Wireless** > **AP Statistics**
Prioritizing AWIPS over Hyperlocation for Third Radio Handling	• **Configuration** > **Tags & Profiles** > **AP Join** > **Add** > **Security**
Support for both MIC and LSC APs to Join the Same Controller	• **Configuration** >**Wireless** > **Access Points**

Behavior Changes

- Embedded Wireless on Cisco Catalyst 9000 Series Switches for Single Secure Site Deployment (Non-SDA) using GUI is not supported with this release.
- From this release, the list of ASCII characters supported for the SSID, AP name, tags, and profiles are modified as follows:
  - SSID: ASCII characters from 32 to 126, with leading and trailing spaces.
  - AP Name: ASCII characters from 33 to 126, without leading and trailing spaces.
  - Tags and Profiles: ASCII characters from 32 to 126, without leading and trailing spaces.

  To see the list of ASCII characters, see this link: ASCII Character Set and Hexadecimal Values

Note Ensure that SSID and AP names do not exceed 32 characters.

- If the RP and RMI links are down, the HA setup breaks into two active controllers. This leads to IP conflict in the network. The HA setup forms again when the RP link comes up. Depending on the state of the external switch at this time, the ARP table may or may not be updated to point to the Active controller. That is, the switch may fail to process the GARP packets from the controller. As a best practice, we recommend that you keep the ARP cache timeout to a lower value for faster recovery from multiple fault scenarios. You need to select a value that does not impact the network traffic, for instance, 30 minutes.
- Standby detects the presence of the Active over the RMI link and avoids switchover when the RP link goes down. In such a case, the standby goes to recovery mode. This mode is represented through suffix **rp-rec-mode** in the hostname. The standby in recovery mode reloads when the RP link comes up. Single faults are gracefully handled in the system.
- Rejection of Wrong WLAN ID on 802.1x SSID: If the WLAN ID attribute that is returned from the AAA server does not match the current WLAN ID, then the authentication fails. The client is deleted and added to the client exclusion list.
- Spectrum Intelligence is supported on Cisco Catalyst 9105AX Series Access Points.

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

Table 3: SNMP Traps

Trap Name	Description
trap_ap_sys_stats	Traps to be sent when statistics are past the threshold.

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 6: Supported PIDs and Ports, on page 12 for the list of supported modules.)

Table 4: 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 5: 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	• Linux KVM based on Red Hat Enterprise Linux 7.6, 7.8, and 8.2 • Ubuntu 14.04.5 LTS, Ubuntu 16.04.5 LTS

Host Environment	Software Version
AWS	AWS EC2 platform
NFVIS	ENCS 3.8.1 and 3.9.1
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 6: 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.
- The Cisco Aironet 2800 and 3800 APs do not reset an interface (to clear any Ethernet interface physical layer issues) if the Dynamic Host Configuration Protocol (DHCP) does not resolve the IP address within a certain duration.

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
- Cisco Catalyst 9124AX (I/D) Access Points

Integrated Access Points

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

Network Sensor

- Cisco Aironet 1800s Active Sensor

Supported Access Point Channels and Maximum Power Settings

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

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

Compatibility Matrix

The following table provides software compatibility information. For more information, see Cisco Wireless Solutions Software Compatibility Matrix

Table 7: Compatibility Information

Cisco Catalyst 9800 Series Wireless Controller Software	Cisco Identity Services Engine	Cisco Prime Infrastructure	Cisco AireOS-IRCM Interoperability	Cisco Catalyst Center	Cisco CMX
Bengaluru 17.5.x	3.0 2.7 2.6 2.4	3.9 3.8.1	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 8.5.176.0 8.5.176.2 8.5.164.0 8.5.164.216	See Cisco Catalyst Center Compatibility Information	10.6.3

GUI System Requirements

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

Table 8: Hardware Requirements

Processor Speed	DRAM	Number of Colors	Resolution	Font Size
233 MHz minimum[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 recommend that you increase the number of VTY lines to 50.

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

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

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

Before You Upgrade

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

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

  Workaround:

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

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

  Workaround:

  - Reboot the impacted APs through the power cycle.

  For more information, see CSCwm08044

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

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

The following Wave 1 APs are not supported from 17.4 to 17.9.2, 17.10.x, 17.11.x, 17.13.x, 17.14.x, and 17.15.x:

- **Cisco Aironet 1570 Series Access Point**
- **Cisco Aironet 1700 Series Access Point**
- **Cisco Aironet 2700 Series Access Point**
- **Cisco Aironet 3700 Series Access Point**

Note

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

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

- If APs fail to detect the backup image after running the **archive download-sw** command, perform the following steps:

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

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

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

     ```
     Device# capwap ap restart
     ```

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

- 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 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.
- From Cisco IOS XE Bengaluru 17.4.1 onwards, session timeout under the policy profile is supported.
- The GUI takes a long time to reload if a large number of files are present in the bootflash or hard disk root directory. We recommend that you remove the unnecessary files.
- When you upgrade the GUI from one release to another, we recommend that you clear browser cache for all GUI pages to reload correctly.
- Communication between Cisco Catalyst 9800 Series Wireless Controller and Cisco Prime Infrastructure uses different ports:
  - All the configurations and templates available in Cisco Prime Infrastructure are pushed through SNMP and CLI, using UDP port 161.
  - Operational data for controller is obtained over SNMP, using UDP port 162.
  - AP and client operational data leverage streaming telemetry:
    - Cisco Prime Infrastructure to controller: TCP port 830 is used by Cisco Prime Infrastructure to push the telemetry configuration to the controller (using NETCONF).

  - Controller to Cisco Prime Infrastructure: TCP port 20828 is used for Cisco IOS XE 16.10.x and 16.11.x, and TCP port 20830 is used for Cisco IOS XE 16.12.x, 17.1.x and later releases.

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

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

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

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

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

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

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

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

- 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 Bengaluru 17.5.x

Table 9: Upgrade Path to Cisco IOS XE Bengaluru 17.5.x Release

Current Software	Upgrade Path to Cisco IOS XE Bengaluru 17.5.x Release
16.10.x	Upgrade first to 16.12.5 and then to 17.5.x.
16.11.x	Upgrade first to 16.12.5 and then to 17.5.x.
16.12.x	You can upgrade directly to 17.5.x.
17.1.x	Upgrade first to 17.3 and then to 17.5.x.
17.2.x	You can upgrade directly to 17.5.x.
17.3.x	You can upgrade directly to 17.5.x.
17.4.x	You can upgrade directly to 17.5.x.

Upgrading the Controller Software

This section describes the various aspects of 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 17.5.x
- **Image Names**:
  - C9800-CL-universalk9_kvm.17.05.01.run

- C9800-CL-universalk9_esxi.17.05.01.run
- C9800-CL-universalk9_nfvis.17.05.01.run

Software Installation Commands

Cisco IOS XE, Bengaluru, 17.5.x	
To install and activate a specified file, and to commit changes to be persistent across reloads, run the following command: **device# install add file** *filename* **[activate |commit]** To separately install, activate, commit, end, or remove the installation file, run the following command: **device# install ?** **Note** We recommend that you use the GUI for installation.	
add file tftp: *filename*	Copies the install file package from a remote location to a device, and performs a compatibility check for the platform and image versions.
activateauto-abort-timer]	Activates the file and reloads the device. The **auto-abort-timer** keyword automatically rolls back image activation.
commit	Makes changes that are persistent over reloads.
rollback to committed	Rolls back the update to the last committed version.
abort	Cancels file activation, and rolls back to the version that was running before the current installation procedure started.
remove	Deletes all unused and inactive software installation files.

Licensing

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

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

Interoperability with Clients

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

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

Table 10: Test Configuration for Interoperability

Hardware or Software Parameter	Hardware or Software Type
Release	Cisco IOS XE, Bengaluru, 17.5.x
Cisco Wireless Controller	See Supported Hardware, on page 11
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 17.
Types of tests	Connectivity, traffic (ICMP), and roaming between two APs

The following table lists the client types on which the tests were conducted. Client types included laptops, hand-held devices, phones, and printers.

Table 11: Client Types

Client Type and Name	Driver or Software Version
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

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	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

Client Type and Name	Driver or Software Version
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)
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

Client Type and Name	Driver or Software Version
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
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

Client Type and Name	Driver or Software Version
Intel Dual Band Wireless AC 8260	Driver v19.50.1.6

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, Bengaluru, 17.5.1

Caveat ID	Description
CSCvv70012	No validation for access group name length.
CSCvv88988	Cisco Catalyst 9105 AP GUI: Rendering issues on switching language. Issue is observed on Firefox on MacOS.
CSCvv99767	After Flexible Radio Assignment (FRA) is disabled, XOR radios are not reverting back to default 2.4 GHz.
CSCvw07650	Cisco Catalyst 9105 AP: Data Datagram Transport Layer Security (DTLS) teardown occurs after sequence of keepalives during throughput test
CSCvw07789	Cisco Catalyst 9124 AP: Gigabit Ethernet interface link is down with AP power up by 802.3at switch with SFP unplugged.
CSCvw11049	aWIPS: Invalid-mac-oui alarm is not getting detected for certain MAC addresses.
CSCvw29362	Flex Samsung s10 client fails on dot1x with Cisco Aironet 2800 AP after disabling and enabling the WLAN.
CSCvw35023	Install rollback to ID after rolling back to base profile is not working.

Caveat ID	Description
CSCvw51196	Cisco Aironet 3800 AP: Monitoring interface is receiving packets with incorrect MAC address on MVL APs.
CSCvw52233	Workgroup Bridge fails to get Stateless Address Auto-configuration (SLACC) autoconfig IPv6 address.
CSCvw52490	AP is sending deauth when deny random MAC is enabled.
CSCvw58096	Only default AAA method list is working for netconf login.
CSCvw59541	Cisco Catalyst 9124 AP fails to do derating when AP network is unreachable.
CSCvw60372	Cisco Catalyst 9124 AP is not able to distinguish between power injector and DC power supply.
CSCvw61072	Reload required field mismatch between CLI and OPER model.
CSCvw66064	Downlink latency drop is not observed on Cisco Catalyst 9120AX for 16 users per PPDU Orthogonal Frequency Division Multiplexing (OFDMA).
CSCvw70034	Catalyst 9800 Series Wireless Controller for Cloud: Scaled Radsec scenario - wncd crash is pointing to ewlc/common/infra/src/ewlc_app_db.c:500.
CSCvw71365	Internal antenna AP slot 0 is operating at maximum txpower on 5 GHz band.
CSCvw73147	Client is not connecting when policy profile name is different from WLAN name in GA scenario (IRCM).
CSCvw76081	AP connected to fast PoE port do not negotiate power fully in alternate switch reload.
CSCvw81430	Observing MU throughput degradation when TAF is enabled.
CSCvw86864	aWIPS: RHL off channel detection is not working for Extensible Authentication Protocol (EAP) over LAN (EAPOL) start flood.
CSCvx06924	Yang/SNMP validation to be in parity with CLI for high throughput configuration.
CSCvx19683	DHCP packet is wrongly punted to IOSd when DHCP snooping is enabled on DHCP VLAN.
CSCvx24603	ClearAir statistics CLI and webpage are not showing the interference devices.
CSCvx27345	Controller is showing neighbor APs as Rogue on 2.4 Ghz band.
CSCvx51893	IPv6 address auto-config is erased from management SVI upon reload, when IPv6 RMI is enabled.

Caveat ID	Description
CSCvx54862	Unable to access OEAP GUI after modifying local DHCP.
CSCvx62279	WLAN client fails to associate on wpa3-owe security in flex: central authentication and local switching.
CSCvx62890	Following countries are missing in the global configuration: (BW, BI, GA, MU, GT, NA, UG, TZ, ZM, UZ.
CSCvx67672	Cisco DNA Center: Event view does not show any SNR information on association messages for open security WLAN.
CSCvx71565	Cisco Aironet 1815W AP: Client is not getting IP from default DHCP scope.
CSCvx72883	Cisco DNA Center: Client failed authentication EAP timeout status is not being deleted.
CSCvx73031	During image upgrade, active/standby reloaded due to stack merge.
CSCvx73273	Unwanted console log message in **show version | i Model** command for Cisco Aironet 1852/1832 AP model.
CSCvx74624	After AP reload in Flexconnect, Cisco Hyperlocation doesn't get disabled when AWIPS-FORENSIC is enabled.
CSCvx74635	AP flap is observed during SSO.
CSCvx75444	Cisco Catalyst 9124AX AP is flooding edge console with interface flaps every 1 minute.
CSCvx76428	Luajit memory consumption results in crash with monitor logging profile wireless filter.
CSCvx76675	Marlin4 AP is able to function with unsupportive versions like Cisco IOS XE Bengaluru 17.5.1.
CSCvx77143	Cisco Catalyst 9124AX AP: TPC IE is incorrectly populated in beacons for channels 116 and above.
CSCvx77815	IOSd crash is observed on new active during SSO.
CSCvx77830	Cisco Aironet 4800 AP is starting CAC and not transmitting beacons in Russia.
CSCvx78790	Reprovision of eCA is failing due to access list duplicate entry.
CSCvx84760	Cisco Catalyst 9124AX AP: On-Channel NDP is around 10 db higher than Beacon RSSI.
CSCvx85409	Cisco Aironet 3800 and 4800 APs are crashing during CAPWAPD process.

Resolved Caveats for Cisco IOS XE, Bengaluru, 17.5.1

Caveat ID	Description
CSCvu71917	Cisco Aironet 1852 and 3802 APs are crashing due to kernel panic.
CSCvu96532	AP access tunnel goes down while adding or removing an inherited VN to another embedded wireless site.
CSCvv77899	WNCD crash is observed after provisioning controller in Cisco DNA Center.
CSCvv84266	Service setting tab under Licensing page goes in loading loop.
CSCvv91755	SLE policy mode is not showing in GUI.
CSCvw07837	iPhone or iPad fails to get neighbor report when 11k is enabled.
CSCvw11113	Cisco Wave 2 and 802.11AX APs are crashing due to kernel panic.
CSCvw11880	FMAN-FP crash is observed when deleting WLAN configured with "peer-blocking allow-private-group".
CSCvw28599	Tri-radio AP sees its own 11b frames as rogue impersonation.
CSCvw33245	KVM controller cannot reach outside network.
CSCvw37272	nmspd core is observed after running **install activate** command.
CSCvw45780	The **port-channel load-balance src-dst-ip** command throws an error during bootup in 17.5
CSCvw49225	Chromebook/Linux with Intel 11ax adapter is unable to connect to 11ax APs in local mode.
CSCvw52160	table tbl_lisp_agent_client_cp entries are not deleted causing memory leak.
CSCvw53846	Cisco Catalyst 9800-80 controller is stuck in disconnecting state after upgrade from Cisco IOS XE Gibraltar 16.12.x to Cisco IOS XE Bengaluru17.4.1.
CSCvw55081	APs are unable to join the controller due to internal error
CSCvw58237	Provisioning AP with Openconfig throws an error.
CSCvw83978	WNCD memory leak is observed on epm_rcl_send_policy_apply_wireless.
CSCvw88761	Only 7 IPv6 address got assigned to client when NUM_IPV6_ADDR_PER_CLIENT is 8 in tsim.
CSCvw91795	Cisco Catalyst 9115 and 9120 Series APs are using the wrong TID when responding to block ack requests.

Caveat ID	Description
CSCvw91859	Cisco Catalyst 9120AX, 9115AX, and 9105AX APs drop upstream traffic (various types) with data DTLS enabled.
CSCvw93262	CleanAir air-quality detect time timestamp on GUI is not getting updated.
CSCvx02273	WNCD btrace log is flooded by two 802.11 FT logs at "notice" level.
CSCvx07869	Cisco DNA Center Client 360 onboarding events are missing AAA server IP for bad credentials failure.
CSCvx08499	Zero Mbps received for frame sizes 1522 and Imix on Catalyst 9800 Series Wireless Controller for Cloud.
CSCvx10352	Cisco Catalyst 9130E AP crashes continuously on wcpd process during upgrade.
CSCvx10374	Multiple kernal panic crashes were observed on Cisco Aironet 1815w AP after upgrade.
CSCvx17641	Observed WNCD traceback followed by wncd WNCD on Cisco Catalyst 9105 AP.
CSCvx24437	GUI is not refreshing entries automatically.
CSCvx30229	After aborting AP predownload, console is flooded with "Pre download handling failed..." messages.
CSCvx36012	AP disconnects post SSO with CAPWAP multiwindow feature enabled.
CSCvx38191	Cisco Catalyst 9130 AP: EWC HA setup is experiencing multiple CPU hogs, tracebacks and iosd crashes.
CSCvx39497	WNCD process reloads unexpectedly due to traffic distribution statistics.
CSCvx40044	WLAN allows special characters but not broadcast on AP because of CLI truncation.
CSCvx49446	SAE + Webauth on-macfilter-failure: Traceback on client join.
CSCvx54573	GUI need to use show wlan summary quoted in the policy tags configuration.
CSCvx71530	Tracebacks related to memory full and ChunkExpandfail is leading to iosd crash.
CSCvx74598	Error is getting generated while configuring channel more than once.

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

User Guide for Cisco User Defined Network Mobile Application

All Cisco Wireless Controller software-related documentation

Cisco Catalyst 9800 Series Wireless Controller Data Sheets

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

Cisco Embedded Wireless Controller on Catalyst Access Points

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

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

Wireless Product Comparison

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

Cisco Access Points–Statement of Volatility

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

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

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

Cisco Prime Infrastructure

Cisco Prime Infrastructure Documentation

Cisco Connected Mobile Experiences

Cisco Connected Mobile Experiences Documentation

Cisco Catalyst Center

Cisco Catalyst Center Documentation

Communications, Services, and Additional Information

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