Release Notes for Cisco Catalyst 9800 Series Wireless Controller, Cisco IOS XE 17.15.x

First Published: 2024-08-14

Last Modified: 2025-08-07

Release Notes for Cisco Catalyst 9800 Series Wireless Controller, Cisco IOS XE 17.15.x

Introduction to Cisco Catalyst 9800 Series Wireless Controllers

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

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

- The controllers come with high availability and seamless software updates that are enabled by hot and cold patching. This keeps your clients and services up and running always, both during planned and unplanned events.

- The controllers come with built-in security, including secure boot, run-time defenses, image signing, integrity verification, and hardware authenticity.

- The controllers can be deployed anywhere to enable wireless connectivity, for example, on an on-premise device, on cloud (public or private), or embedded on a Cisco Catalyst switch (for SDA deployments) or a Cisco Catalyst access point (AP).

- The controllers can be managed using Cisco Catalyst Center, programmability interfaces, for example, NETCONF and YANG,or web-based GUI or CLI.

- The controllers are built on a modular operating system. Open and programmable APIs enable the automation of your day zero to day *n* network operations. Model-driven streaming telemetry provides deep insights into your network and client health.

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

- Catalyst 9800 Series Wireless Controller Appliance
  - Cisco Catalyst 9800-80, Catalyst 9800-40, and Catalyst 9800-L Wireless Controllers
  - Cisco Catalyst CW9800H1 and CW9800H2 Wireless Controllers
  - Cisco Catalyst CW9800M Wireless Controller

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

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

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

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

Revision History

Modification Date	Modification Details
July 15, 2025	Cisco IOS XE 17.15.4 release
April 01, 2025	Cisco IOS XE 17.15.3 release
February 19, 2025	Cisco IOS XE 17.15.2b release
November 27, 2024	Cisco IOS XE 17.15.2 release
November 14, 2024	Added bug ID CSCwi39486 to the Resolved Issues list.
September 26, 2024	Updated: **Compatibility Matrix** section—Added version 3.3 to the **Cisco Identity Services Engine** information in the **Compatibility Information** table.
September 17, 2024	Updated: **What's New in Cisco IOS XE 17.15.1** section—Changed "Tier B/C/D Country Support for Cisco Catalyst 9124 Outdoor Access Points" to "Tier B/C/D Country Support for Cisco Catalyst 9163E Outdoor Access Points".

What's New in Cisco IOS XE 17.15.4

Table 1: New and Modified Software Features

Feature Name	Description and Documentation Link
Wired Proximity-Based Resolution	APs having adjacency via Cisco Discovery Protocol (CDP) or Link Layer Discovery Protocol (LLDP) on the same switch, are included in the neighborhood graph and treated as neighbors. If an AP has a neighbor on the wired side that is just a hop away, it will not be considered as an adjacency because the controller lacks information about the network topology and the CDP neighbors of the switch, the AP is connected to.

What's New in Cisco IOS XE 17.15.3

Table 2: New and Modified Software Features

Feature Name	Description and Documentation Link
Support for Dual-Band (XOR) Radio in Cisco Wireless 9176 Series Wi-Fi 7 Access Points (CW9176I/D)	From this release, dual-band (XOR) radio is supported when operating in 2.4-GHz or 5-GHz low band mode (UNII 1-2A), on Cisco Wireless 9176 Series Wi-Fi 7 APs.
Multi-Link Operation (MLO) Support in Cisco Wireless 9178 Series Wi-Fi 7 Access Points (CW9178I)	From this release, MLO is supported on Cisco Wireless 9178 Series Wi-Fi 7 Access Points, in the AT mode.
Cisco Sensor Connect for IoT Services	Cisco Sensor Connect for IoT Services solution enables delivery of advanced BLE capabilities over Cisco Catalyst Wireless infrastructure. The key component of this solution is the IoT Orchestrator component which is a Cisco IOx application that can be deployed on existing Cisco Catalyst 9800 Wireless Controller platforms. With the Cisco Sensor Connect for IoT Services, you have capabilities to securely onboard and control BLE devices, and consume data telemetry using the Message Queuing Telemetry Transport (MQTT). For information, see the configuration guide: https://www.cisco.com/c/en/us/td/docs/wireless/spaces/iot-orchestrator/config-guide/b-spaces-connect-iot-config-guide.html **Note** For scale numbers, see the Scale Summary section in the configuration guide.

What's New in Cisco IOS XE 17.15.2b

Table 3: New and Modified Software Features

Feature Name	Description and Documentation Link
Support for Cisco Wireless 9172I Series Wi-Fi 7 Access Points (CW9172I)	The Cisco Wireless 9172I Wi-Fi 7 Access Point is an enterprise-class tri-band (2.4 GHz, 5 GHz, 6 GHz) access point. The AP supports full interoperability with leading 802.11ax and 802.11ac clients and a hybrid deployment with other APs and controllers. Note: For more information about all the supported countries for the APs, see https://www.cisco.com/c/dam/assets/prod/wireless/wireless-compliance-tool/index.html.
Split-PHY Mode Support in Cisco Wireless 9172I Series Wi-Fi 7 Access Points (CW9172I) Radio	The radio on Cisco Wireless 9172i AP operates in the following modes: • 5-GHz 4x4 (single-PHY) • 5-GHz 2x2 + 6-GHz 2x2 (split-PHY) The default mode is 5-GHz 2x2 or 6-GHz 2x2. If the AP operates in a regulatory domain where 6-GHz is not supported, then it will operate in the 5-GHz 4x4 mode.

What's New in Cisco IOS XE 17.15.2

Attention If you have deployments that use web authentication with FlexConnect local switching, we recommend that you do not use Cisco IOS XE 17.15.2 release because FlexConnect local switching traffic on web authentication SSID is randomly centralized and clients lose connectivity (see CSCwn17412). Therefore, we recommend that you wait until a fix is available in an APSP or a subsequent release.

Table 4: New and Modified Software Features

Feature Name	Description and Documentation Link
Cisco Network Subscription	Cisco Wireless licenses, a part of the Cisco Networking Subscription licensing model, is a software license that helps you to deploy your Wi-Fi 7 Access Points in an on-premise, hybrid, or a cloud managed network. From Cisco IOS XE 17.15.2, Cisco Wireless licenses are supported on Wi-Fi 7 Access Points (APs) and later models of APs. The Cisco Wireless licenses consist of the following tiers: • **Cisco Wireless Essentials (LIC-CW-E)**: The tier that provides fundamental features and functionalities that are essential to manage a network. • **Cisco Wireless Advantage (LIC-CW-A)**: The tier that supports additional features and capabilities, and includes all the essential capabilities in addition to the advanced capabilities to manage a network. For more information, see Cisco Wireless Licensing.
Support for the following Wi-Fi 7 APs: • Cisco Wireless 9178I Series Wi-Fi 7 Access Points (CW9178I) • Cisco Wireless 9176I Series Wi-Fi 7 Access Points (CW9176I) • Cisco Wireless 9176D1 Series Wi-Fi 7 Access Points (CW9176D)	The CW9178I APs, CW9176I APs, and CW9176D APs, are enterprise-class tri-band (2.4 GHz, 5 GHz, 6 GHz) APs. The APs support full interoperability with leading 802.11be, 802.11ax, and legacy clients, and a hybrid deployment with other APs and controllers. For a full listing of the APs' features and specifications, see: • Cisco Wireless 9178I Series Wi-Fi 7 Access Point Data Sheet • Cisco Wireless 9176 Series Wi-Fi 7 Access Point Data Sheet **Note** Support for Wi-Fi 7 APs (CW9176, CW9176I, and CW9178D) in availabe for Singapore Thailand, and Hong Kong. For more information about all the supported countries for the APs, see https://www.cisco.com/c/dam/assets/prod/wireless/wireless-compliance-tool/index.htm
AP AnyLocate	In this release, Ultra Wide Band Ranging technology is introduced, which provides superior location accuracy and enhanced network reliability in high-density and multipath-prone environments, resulting in precise and improved wireless performance. UWB radio is used by APs to perform AP-to-AP ranging that improves the accuracy of AP AnyLocate. The following commands are introduced: • **geolocation uwb initiator burst-size** • **geolocation uwb initiator burst-duration** For more information, see AP Management.

Feature Name	Description and Documentation Link
Third-Party Antenna Support for Cisco Catalyst 9163E Outdoor Access Point (CW9163E-x).	From this release, third-party antennas are supported on the CW9163E-x APs .
Dynamic Band Switching in Cisco Catalyst 9166 Series APs (CW9166)	The CW9166I and CW9166D APs include dynamic XOR 5-GHz or 6-GHz radio band switching that optimizes performance and ensuring regulatory compliance. The APs actively adjust and communicate channel power settings, offering full 5-GHz channels when configured for 6-GHz and restricted channels when in 5-GHz mode. The following commands are introduced: • **ap name dot11 dual-band slot radio role manual client-serving** • **ap name dot11 dual-band slot shutdown** • **ap name dot11 dual-band slot band 6ghz** For more information, see Countries and Regulations.
Enhanced Security Group Access Control List (SG-ACL) Logging	The Enhanced SG-ACL Logging feature uses High-Speed Logging (HSL) to forward the SG-ACL IPv4 and IPv6 **permit** or **deny** logging messages in HSL v9 format to the syslog server.
Fast Switching on RLAN Ports in Cisco Catalyst 9105 Series APs	Fast switching for RLAN client traffic is supported on Cisco Catalyst 9105 Series APs. The following command is introduced: **rlan fast-switching** **Note** If you enable RLAN fast switching for FlexConnect AP using local switching or local DHCP WLAN, which is assigned a non-native VLAN, it is not possible to get a DHCP address from the local DHCP server. As a workaround, add the wireless client VLAN to the RLAN profile. For more information, see Remote LANs.

Feature Name	Description and Documentation Link
Global Use APs	With the new Wi-Fi 7 APs, Cisco now has one AP portfolio that can be used either with the Meraki cloud native network or Catalyst on-premise controller-based deployments. With the introduction of the one AP portfolio, it is essential to have a single product ID (PID) at manufacturing, to simplify logistics or operations. The Global Use AP simplifies the Cisco Wireless AP portfolio, by • Decoupling the AP PID/SKU from the regulatory domain (geography) that they can be used. • Decoupling the AP PID/SKU from the boot mode, that is, Catalyst controller-based or Meraki based. The two key aspects that are addressed by Global Use AP for Catalyst and Meraki Cloud deployments are — AP Mode of Operation and Cisco Regulatory Domain. The following commands are introduced: • **ap regulatory activation apply** • **ap regulatory activation clear** • **ap regulatory activation file** • **show ap regulatory activation** For more information, see Global Use APs.
Global Navigation Satellite System (GNSS) Raw Data Streaming from Cisco AP to Cisco Spaces Connector	In this release, the Global Navigation Satellite System (GNSS) raw data streaming through Google Remote Procedure Call (gRPC) feature allows data to be streamed from the APs directly to Cisco Spaces Connector using the gRPC protocol. For more information, see AP Management.
Support for Cisco Catalyst 9124AX Series Outdoor Access Points in Morocco	Morocco allows indoor channels and power for units attached outside buildings. In this release, the Catalyst 9124AXI and 9124AXD Outdoor APs are supported in Morocco. The outdoor designation is 2.4 GHz. For more information, 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.

Feature Name	Description and Documentation Link
Support for Multi-link Statistics Table	The multilink statistics table tracks performance for multilink clients, keyed by their MAC address. It stores both per-link and aggregated statistics. For Multicast Listener Discovery (MLD) stations, the system generates and updates these statistics automatically as new links are added. Non-MLD stations initially record only aggregated stats, which are later transferred to the per-link stats table if they connect to an MLD access point. The following commands are introduced: • **show wireless client mac-address mobility history** • **show wireless client mac-address** • **show wireless client summary** • **show wireless summary** For more information, see Wi-Fi 7 Operations.
Support for Multi-link Operation (MLO) in Wi-Fi 7 APs	In this release, Wi-Fi 7 APs allow client devices to operate multiple links with APs as part of the 802.11be standard. The system automatically enables Multi-link Operation (MLO) with 802.11be, requiring no separate configuration. The following AP commands are introduced: • **copy logs driver radio** • **debug aid** • **debug client** • **debug dot11 dot11Radio** • **show controller dot11Radio <radio-id> aid-list** • **show dot11 clients** • **show dot11 ml-clients** • **show dot11 mlo configuration** • **show dot11 mlo driver** • **show dot11 mlo status** • **show flash logs driver radio** • **test crash radiofw recovery-mode**

Feature Name	Description and Documentation Link
Wi-Fi 7 WPA3 Security Constraints	In this release, the Wi-Fi 7 standard dictates the following security constraints, which are applicable for Wi-Fi 7 compliant APs: The security standards mentioned below are beaconed as Wi-Fi 7 clients. This is a deviation from the actual security constraint. • Open authentication as Wi-Fi 7 is not permitted to associate. • WPA1 as Wi-Fi 7 is not permitted to associate. • WPA2 as Wi-Fi 7 is not permitted to associate. • WPA3 is permitted with certain restrictions: • SAE(24/25) is permitted with GCMP-256. • SAE(8/9) is permitted. (This is a deviation from the actual security constraint.) • WPA2 PSK/802.1x with PMF is permitted. (This is a deviation from the actual security constraint.) • 802.1x-SHA256 with PMF is permitted. • Suite-B-192 with PMF is permitted. For more information, see WPA3 Security Enhancements for Access Points

Table 5: New and Modified GUI Features

Feature Name	GUI Path
Unified Licensing	• **Monitoring** > **Wireless** > **AP Statistics** • **Licensing** > **General** > **Change Wireless License Level** • **Licensing** > **Service Settings**
AP AnyLocate	• **Configuration** > **Tags & Profiles** > **AP Join**
Global Use APs	• **Administration** > **Regulatory Activation**

Feature Name	GUI Path
Support for the following Wi-Fi 7 APs: - Cisco Wireless 9178I Series Wi-Fi 7 Access Points - Cisco Wireless 9176I Series Wi-Fi 7 Access Points - Cisco Wireless 9176D1 Series Wi-Fi 7 Access Points	- **Configuration** > **Tags & Profiles** > **AP Join** - **Configuration** > **Radio Configuration** > **Network** - **Configuration** > **Tags & Profiles** > **RF/Radio** - **Configuration** > **Wireless** > **Access Point** - **Configuration** > **Radio Configuration** > **High Throughput** - **Configuration** > **Tags & Profiles** > **Multi BSSID** - **Configuration** > **Tags & Profiles** > **802.11be** - **Configuration** > **Wireless** > **Radio Statistics** - **Configuration** > **Wireless** > **AP Statistics**

MIBs

The following MIBs are newly added or modified:

- CISCO-LWAPP-DOT11-MIB.my
- CISCO-LWAPP-DOT11-MIB.my

What's New in Cisco IOS XE 17.15.1

Table 6: New and Modified Software Features

Feature Name	Description and Documentation Link
Packet Capture: TCP Dump on WGB	This feature captures packets from a WGB terminal using a default or customized filter through a WGB wired port and uploads them to an external server for further analysis. The feature is supported on the following APs: - Cisco Catalyst IW9167E Heavy Duty Series Access Points - Cisco Catalyst IW9165E Rugged Access Point For more information, see Packet Capture: TCP Dump on WGB on Cisco Catalyst IW9167E Heavy Duty Access Point Configuration Guide and Cisco Catalyst IW9165E Rugged Access Point and Wireless Client Configuration Guide.

Feature Name	Description and Documentation Link
Cisco IW9167IH AP Mesh Support	This feature enables Bridge and Flex+Bridge mode on the Cisco IW9167IH AP allowing you to extend the wireless network coverage through mesh backhaul using the 2.4 GHz and 5 GHz frequencies. The following command is introduced: • **ap name** *ap-name* **mode bridge** For more information, see Mesh Support.
AAA User Authentication Support for WGB	The AAA User Authentication Support for WGB feature provides information about how to use AAA to control network resource usage and define permissible actions. The feature is supported on the following APs: • Cisco Catalyst IW9167E Heavy Duty Series Access Points • Cisco Catalyst IW9165E Rugged Access Points For more information, see AAA User Authentication Support on Cisco Catalyst IW9167E Heavy Duty Access Point Configuration Guide and Cisco Catalyst IW9165E Rugged Access Point and Wireless Client Configuration Guide.
Radio 4 in Scanning Only Mode	This feature enhances the WGB auxiliary scanning and roaming capabilities, allowing you to configure radio 4 to operate in scanning mode only. Radio 4 supports both 2.4 GHz and 5 GHz frequencies. The feature is supported on Cisco Catalyst IW9167E Heavy Duty Series Access Points. For more information, see Configure Aux Scanning.
Optimized Roaming with Dual-Radio WGB	This feature reduces service downtime and ensures a smoother and reliable network experience. When roaming is triggered by a beacon miss-count or maximum packet retries, the second radio enables the WGB to bypass the scanning phase and check the scanning table for potential APs. The feature is supported on the following APs: • Cisco Catalyst IW9167E Heavy Duty Series Access Points • Cisco Catalyst IW9165E Rugged Access Points For more information, see Configure Aux Scanning on Cisco Catalyst IW9167E Heavy Duty Access Point Configuration Guide and Cisco Catalyst IW9165E Rugged Access Point and Wireless Client Configuration Guide.

Feature Name	Description and Documentation Link
Cisco Catalyst 9800-CL Cloud Wireless Controller Oracle Cloud Infrastructure (OCI) Support	The Cisco Catalyst Wireless Controller for Cloud (C9800-CL) sets the standard for Infrastructure as a Service (IaaS) secure wireless network services with Oracle Cloud Infrastructure (OCI). C9800-CL combines the advantages and flexibility of an OCI public cloud with the customization and feature-richness that customers usually experience on-prem deployments. For more information, see Cisco Catalyst 9800-CL Cloud Wireless Controller Installation Guide.
Cloud Monitoring for Cisco Catalyst 9800 Hardware Wireless Controllers	The Cloud Monitoring for Cisco Catalyst 9800 Hardware Wireless Controllers feature helps to monitor controllers using the Meraki dashboard. The following command is introduced: • **service meraki connect** For more information, see Using Cloud Monitoring as a Solution for Network Monitoring.
Cisco Spaces Connect for IoT Services: Support for On-Premise in Cisco Catalyst Wireless Infrastructure	Cisco Spaces Connect for IoT Services solution enables delivery of advanced BLE capabilities over Cisco Catalyst Wireless infrastructure. The key component of this solution is the IoT Orchestrator which is a Cisco IOx application that can be deployed on existing Cisco Catalyst 9800 Wireless Controller platforms. With the Spaces Connect for IoT Services solution, you have capabilities to securely onboard and control BLE devices, and consume data telemetry using the Message Queuing Telemetry Transport (MQTT). **Note** The **Spaces Connect for IoT Services** is now in **Public Beta**. For more information about this feature, see the following documentation: • Cisco Spaces Connect for IoT Services Configuration Guide • Cisco Spaces Connect for IoT Services Quick Start Guide • Cisco Spaces Connect for IoT Services Programmability Guide • Cisco Spaces Connect for IoT Services Online Help • Cisco Spaces Connect for IoT Services Release Notes For further help, you can reach out to Cisco TAC or write to: c9800-spaces-connect-for-iot-services@external.cisco.com

Feature Name	Description and Documentation Link
New Channel Support for United Arab Emirates and Qatar	In this release, the following channels are supported for indoor APs in the United Arab Emirates and Qatar: 149, 153, 157, 161, and 165. The following channels are supported for outdoor APs in the United Arab Emirates: 36, 40, 44, 52, 56, 60, 64. Also, the outdoor power table value for the 5-GHz band is updated for the United Arab Emirates in this release. For more information, see Countries and Regulations.
New Countries for 6-GHz Support	From this release, Taiwan (TW) and Guatemala (GT) are added to the list of countries that support the 6-GHz radio band. For more information, see Countries and Regulations.
Software-Defined Access (SDA) Updates	The following are the SDA updates for Cisco IOS XE 17.15.1: • IPv6 Underlay Support for FIAB (Fabric in a Box) • Flex OTT (Meraki Access Points) support in SDA • Dual Ethernet support for Cisco Catalyst 9136 Series APs in SDA (Non-authenticated ports and single switch stack homed deployment)
SuiteB-1X and SuiteB-192-1X Support in FlexConnect Mode for WPA2 and WPA3	From Cisco IOS XE 17.15.1 onwards, Cisco WLAN FlexConnect mode supports enterprise authentication key management (AKM) — SuiteB-192-1X (AKM 12) and SuiteB-1X (AKM 11). This feature supports the configuration of SuiteB-192-1X and SuiteB-1X in FlexConnect mode, and also supports Galois Counter Mode Protocol 128 (GCMP-128), GCMP-256, and Counter Cipher Mode with Block Chaining Message Authentication Code Protocol 256 (CCMP-256) ciphers for pairwise transport keys (PTK) and group temporal key (GTK) derivation in FlexConnect Local Authentication mode and FlexConnect Central Authentication mode. For more information, see SuiteB-1X and SuiteB-192-1X Support in FlexConnect Mode for WPA2 and WPA3.
Support for Security-Enhanced Linux	In this release, the controller is supported with Security-Enhanced Linux (SELinux) MAC operating in enforcing mode, to improve the overall security profile. SELinux is a solution composed of Linux kernel security module and system utilities to incorporate a strong, flexible Mandatory Access Control (MAC) architecture into the controller. The following commands are introduced: • **set platform software selinux** • **platform security selinux** For more information, see Security-Enhanced Linux.

Feature Name	Description and Documentation Link
Wi-Fi Protected Access (WPA3) Security Enhancements for Access Points	The following are the security enhancements developed in Cisco IOS XE 17.15.1, for APs: • GCMP-256 Cipher and SuiteB-192-1X AKM • SAE-EXT-KEY Support • AP Beacon Protection • Multiple Cipher Support per WLAN • Opportunistic Wireless Encryption (OWE) Support with GCMP-256 Cipher The following commands are introduced: • **security wpa akm sae ext-key** • **security wpa akm ft sae ext-key** • **security wpa akm suiteb-192** • **security wpa akm suiteb** • **security wpa wpa2 ciphers** • **security wpa wpa3 beacon-protection** For more information, see Wi-Fi Protected Access (WPA3) Security Enhancements for Access Points.
Tier B/C/D Country Support for Cisco Catalyst 9163E Outdoor Access Points	From this release, Cisco Catalyst 9163E Outdoor APs are supported in the following countries: Bosnia, Hong Kong, India, Indonesia, Israel, Jordan, Kuwait, Puerto Rico, Qatar, Saudi Arabia, Singapore, South Africa, Taiwan, Turkey, and United Arab Emirates. For more information, see Countries and Regulations.

Table 7: New and Modified GUI Features

Feature Name	GUI Path
Cloud Monitoring for Cisco Catalyst 9800 Hardware Controllers	**Configuration** > **Services** > **Cloud Services** > **Meraki**
Cisco Spaces Connect for IoT Services: Support for On-Premise in Cisco Catalyst Wireless Infrastructure	**Configuration** > **Services** > **IoT Services** ***Currently, this feature is in a limited customer public beta phase and supported by Cisco TAC.*** ***For more information about this feature, contact the following mailer:*** *c9800-spaces-connect-for-iot-services@external.cisco.com*

Feature Name	GUI Path
SuiteB-1X and SuiteB-192-1X Support in FlexConnect Mode for WPA2 and WPA3	**Configuration** > **Tags & Profiles** > **WLANs**
Wi-Fi Protected Access (WPA3) Security Enhancements for Access Points	**Configuration** > **Tags & Profiles** > **WLANs**

MIBs

The following MIBs are newly added or modified:

- AIRESPACE-WIRELESS-MIB.my
- CISCO-LWAPP-AP-MIB.my
- CISCO-LWAPP-DOT11-MIB.my
- CISCO-LWAPP-DOT11-CLIENT-MIB.my
- CISCO-LWAPP-REAP-MIB.my
- CISCO-LWAPP-RF-MIB.my
- CISCO-LWAPP-TAGS-MIB.my
- CISCO-LWAPP-TC-MIB.my
- CISCO-LWAPP-WLAN-SECURITY-MIB.my

Product Analytics

This feature allows for the collection of non-personal usage device systems information for Cisco products, which helps in continuous product improvements. This feature is supported on the Cisco Catalyst 9800 Series Wireless Controllers (9800-80, 9800-40, 9800-L, 9800-CL, CW9800M, and CW9800H1/H2). You can use the the **pae** command to enable or disable this feature.

The following commands are introduced as part of this feature:

- **pae**
- **show product-analytics kpi**
- **show product-analytics report**
- **show product-analytics stats**

Note Turning off Smart Licensing Device Systems Information does not impact other Systems Information collection including from Cisco Catalyst Center or vManage.

Important: We are constantly striving to advance our products and services. Knowing how you use our products is key to accomplishing this goal. To that end, Cisco will collect device and licensing Systems Information through Cisco Smart Software Manager (CSSM) and other channels for product and customer experience improvement, analytics, and adoption. Cisco processes your data in accordance with the General Terms and Conditions, the Cisco Privacy Statement and any other applicable agreement with Cisco. To modify your organization's preferences for device and licensing systems information, use the **pae** command. For more information, see *Cisco Catalyst 9800 Series Wireless Controller Command Reference*.

For additional information on this feature, see *Wireless Product Analytics FAQ*.

Behavior Change

Behavior Change for Cisco IOS XE 17.15.4

- The Cisco Catalyst 9124 mesh APs (MAP) powered with 30W, when joined to a Cisco Catalyst 9124 EWC root AP, tri-radio was not supported with 30W. It was only possible to enable it if MAP was powered with 60W. With the change in behavior, you can enable tri-radio with 30W.
- Controller displayed out-of-order packet issue with fragmented packets when Auto QoS was enabled. When a client tries to connect to an EAP-TLS-based SSID, during the certificate exchange, the client sends its device certificate. If the certificate is fragmented because it exceeds the MTU (1500), the fragments are observed to be sent out-of-order from the controller when Auto QoS is enabled.

  With the change in behavior, the fragments are classified and applied with default action. For workarounds, refer to CSCwo97886.
- The Cisco Catalyst 9130AXI-C APs in Bangladesh (BD) regulatory domain do not announce High Efficiency capabilities (802.11ax) on 5-GHz radio (Slot 1) but the same AP advertises on 2.4-GHz radio (Slot 0). Therefore, clients to connect to 2.4-GHz or on 5-GHz by using 802.11a data rates.

  With the change in behavior, the APs advertise High Efficiency on 5-GHz radio and clients connect to 802.11ax(5-GHz). For workarounds, refer to CSCwp17376
- The **ip proxy-arp** configuration is disabled by default under VLAN interfaces for the controller.
- Remove redundant counters from **show wireless stats ap name** *ap-name* **dot11 5GHz** output.

  The output of **show wireless stats ap name** *ap-name* **dot11 5GHz**, displays two counters: **FailedCount** and **AckFailureCount**. Confirm if both counters are identical and remove one of them (preferably **AckFailureCount**, since it is not incremental).
- For Cisco Aironet 1815T Series AP, from Cisco IOS XE 17.12.x, `.../storage/config.oeap` was created beforehand as long as the AP is in OEAP mode.

  With the change in behavior, once the AP boots in FlexConnect OEAP mode, it switches on the default OEAP DHCP server (dhcp0) as day 1 configuration.
- In the Mobility Data DTLS tunnel, DTLS encryption was enabled on Peer1 and disabled on Peer2, causing the mobility tunnel to be up. However, with the change in behavior, DTLS encryption is enabled on Peer1 and disabled on Peer2, causing the mobility tunnel to go down.
- The maximum supported RFIDs per WNCD for any platform has been increased to greater than 9601 RFIDs. The new value of the maximum RFID is platform dependent.

- When source-interface was configured under mDNS globally, this source-interface was chosen to send out mDNS packets. When the source-interface was not configured, then, the controller used wireless management interface WMI) to send out the mDNS packets.

  With the change in behavior, when source-interface is configured, the controller uses this configured source-interface to send out mDNS packets. When the source-interface is not configured,

  - Option 1: Use SVI as the source-interface (if SVI of the intended VLAN is configured).
  - Option 2: If option 1 fails, use the default Wireless Management Interface (WMI).

- Authentication for AP with EAP fails if the password is more than 31 characters. With the change in behavior, password with more than 31 characters works successfully.

- Thermal throttle configuration between 40C and 50C for CW9172I AP:

  Split-phy: 2/5/6 GHz 1SS, Scan Radio, BLE, USB, and 2.5 Gbps Ethernet

  Single-phy: 2ghz 1SS, 5 GHz 2SS, Scan Radio, BLE, USB, and 2.5Gbps Ethernet

  Thermal throttle configuration between 40C and 50C for CW9172H AP: 2/5/6 GHz 1SS, Scan Radio, BLE, PoE-out and 2.5Gbps Ethernet

- Thermal degradation for CW9172I and CW9172H APs start before reaching 40C. With the change in behavior, the thermal degradation for CW9172I and CW9172H APs start at 40C.

- In the early development phase, radio profiles were not mapped by default. Later, the behavior changed to automatically link the default radio profile under an RF tag whenever a new RF tag was created.

  However, due to code limitations, a default radio profile cannot be created under the RF tag when the RF tag is created using NETCONF or WebUI. The radio profile has to be linked manually while creating an RF tag using NETCONF or WebUI interfaces.

Behavior Change for Cisco IOS XE 17.15.3

- RADIUS packets were getting fragmented with the default value of 1396. With the change in behavior, RADIUS packets are fragmented based on the source interface IP MTU.

  This behaviour change is applicable only when the RADIUS source interface is attached under the RADIUS group. If there is no source interface attached under the RADIUS group, this change is not applicable.

- The default **platform punt-policer** commands have been modified. We recommend that you check if you have modified the default **platform punt-policer** commands for any of the releases. In such a case, delete the commands before upgrading, and reapply them after upgrading to 17.15 or later, using the corresponding keywords.

Note The following command has changed in-between releases:

platform punt-policer wls_sisf_pkt 5000 high (17.9) > **platform punt-policer wls_sisf_arp_v6nd_pkt 5000 high** (17.12) > **platform punt-policer wls-sisf-arp-v6nd-pkt 5000 high** (17.15)

The following are the default commands in Cisco IOS XE 17.12 and Cisco IOS XE 17.15:

17.12

```
Device# show run all | i platform punt-policer wls
platform punt-policer wls_dot11_pkt 14000
platform punt-policer wls_dot11_pkt 2700 high
platform punt-policer wls_capwap_pkt 437
platform punt-policer wls_capwap_pkt 90000 high
platform punt-policer wls_mobility_pkt 437
platform punt-policer wls_mobility_pkt 45000 high
platform punt-policer wls_sisf_pkt 437
platform punt-policer wls_sisf_pkt 8000 high
platform punt-policer wls_sisf_arp_v6nd_pkt 437
platform punt-policer wls_sisf_arp_v6nd_pkt 8000 high
platform punt-policer wls_ap_https 40000
platform punt-policer wls_ap_https 437 high
```

17.15

```
Device# show run all | i platform punt-policer wls
platform punt-policer wls-mgmt-pkt 14000
platform punt-policer wls-mgmt-pkt 2700 high
platform punt-policer wls-tunnel-pkt 437
platform punt-policer wls-tunnel-pkt 90000 high
platform punt-policer wls-mobility-pkt 437
platform punt-policer wls-mobility-pkt 45000 high
platform punt-policer wls-sisf-pkt 437
platform punt-policer wls-sisf-pkt 8000 high
platform punt-policer wls-sisf-arp-v6nd-pkt 437
platform punt-policer wls-sisf-arp-v6nd-pkt 8000 high
platform punt-policer wls-https-dnld 40000
platform punt-policer wls-https-dnld 437 high
platform punt-policer wls-cfg-pkt 4000
platform punt-policer wls-cfg-pkt 437 high
```

- When the controller receives an ARP request with the source IP matching another client IP address that is present in the device tracking database, whose preference level is higher than ARP [DHCP], the baseline behavior is to exclude the incoming client.

  With the behavior change, the controller drops the ARP packet and does not exclude the client.

- If you have enabled 802.11be and Wi-Fi clients connect to an SSID, the SSID must be compatible with Wi-Fi 7 requirements (WPA3; if using SAE, it must be SAE-EXT or SAE/SAE-EXT). This functionality was optional in Cisco IOS XE 17.15.2, but in Cisco IOS XE 17.15.3, it is enforced.

Behavior Change for Cisco IOS XE 17.15.2

- When Wi-Fi 7 APs are converted from Meraki to Cisco Catalyst with a valid country code stored in the shared environment, the **Country Code Resolution Method** is displayed as **Installed via Meraki Dashboard**.

- XOR 5-GHz or 6-GHz slot 2 will be put in the 5-GHz band if the country code set on Cisco Catalyst Wireless 9166I Series AP does not support the 6-GHz band.

- Fast Transition Adaptive is not supported for WPA3 SAE.

- In Cisco IOS XE 17.15.2, the lack of support for link re-configuration in Multi-Link Operation (MLO) may lead to client disruptions. This issue arises when clients are connected to 802.11be radios, especially if 802.11be is enabled across all radio bands. To notify of potential disruptions, users will be notified through pop-up notifcations. These messages appear across all radio bands of the AP whenever configuration changes to radio parameters result in a radio reset, or enable or disable the workflow.

- The output for **show ap config slots** and **show ap config general** commands are duplicate. To reduce the duplicate output, perform the following:
    - Leave the detailed information for each radio slot remains unchanged.
    - Retain only the key AP general information.
- When a country using channels 1, 5, 9, and 13 is added to the controller, the 2.4-GHz RF profiles automatically update to include these channels, leading to inconsistencies. The behaviour is observed in Cisco IOS XE Amsterdam 17.3.x, Cisco IOS XE Bengaluru 17.6.x, and Cisco IOS XE Cupertino 17.9.x, and it should be avoided. RF profiles should remain unchanged initially, with manual adjustments made only if necessary for countries supporting additional channels.
- When a country from the European Telecommunications Standards Institute (ETSI) or Rest of World (ROW) domain is set up in the controller and AP join profile, Dual 5G is enabled. If the country code is then changed to another within the same domain, it causes the AP to continuously reboot.
- Global Use APs: APs are not able to migrate to Meraki in Catalyst mode via Option 17 in external DHCPv6 server. Set the Fast Offline migration bit to `01` in external DHCP server, for the APs to migrate to Meraki mode.
- Global Use APs: The output of the **show ap regulatory activation all** command displays the regulatory activation file metadata.
- You can allow the 5-GHz or 6-GHz XOR radio to move to 6GHz:
    - When the 6-GHz network is enabled.
    - When the **Regulatory Domain Allowed by Country** is 6GHz.

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

- The IP overlap feature supports FlexConnect VLAN-based central switching.
- The Security Group Access Control List (SGACL) logging records are generated and managed through an internal High-Speed Logging (HSL) server. These records are then sent to a Syslog server under the following conditions:
    - A packet hits a logging access control entry (ACE).
    - The Cisco TrustSec role-based policy is enabled.
- The Unscheduled Automatic Power Save Delivery (U-APSD) can now be configured to be enabled or disabled in the probe, beacon, and association response.

Behavior Change for Cisco IOS XE 17.15.1

- From this release, the Mobility Tunnel UP/DOWN messages will be marked for severity level ALERT.
- From this release, it is not possible to disable the 802.11h channel switch. The channel switch announcements (CSA) remain enabled at all times because they help clients when the APs announce the change from the current channel to a new channel, thereby reducing the number of reconnections.

- The minimum memory requirement of the Cisco Catalyst 9800 Wireless Controller for Cloud - Ultra-Low Profile variant is increased from 4 GB to 6 GB.
- From this release, the SuiteB and SuiteB-192 authentication and key management (AKMs) are decoupled from the GCMP128, GCMP256/CCMP256 and must be configured separately. When the controller is upgraded from a lower version to 17.15, WLANs configured with suiteb AKMs will be affected. If the controller downgrades from version 17.15 to a lower one, the WLANs enabled with only suiteb AKMs will remain operational, while the WLANs with multiple AKMs enabled will be operational without the suiteb-related AKMs.
- From this release, the default air pressure sample interval is changed from 30 seconds to 60 seconds. For example, if the duration is set to 10 minutes, the APs send 10 samples that are spaced at 60 seconds each.

Interactive Help

The Cisco Catalyst 9800 Series Wireless Controller GUI features an interactive help that walks you through the GUI and guides you through complex configurations.

You can start the interactive help in the following ways:

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

  For instance, **Show me How** in **Configure** > **AAA** walks you through the various steps for configuring a RADIUS server. Choose **Configuration**> **Wireless Setup** > **Advanced** and click **Show me How** to trigger the interactive help that walks you through the steps relating to various kinds of authentication.

The following features have an associated interactive help:

- Configuring AAA
- Configuring FlexConnect Authentication
- Configuring 802.1X Authentication
- Configuring Local Web Authentication
- Configuring OpenRoaming
- Configuring Mesh APs

Note If the WalkMe launcher is unavailable on Safari, modify the settings as follows:

1. Choose **Preferences > Privacy**.
2. In the **Website tracking** section, uncheck the **Prevent cross-site tracking** check box to disable this action.
3. In the **Cookies and website data** section, uncheck the **Block all cookies** check box to disable this action.

Important Notes

- Upgrading the controller software on Cisco Catalyst CW9800M, CW9800H2, or CW9800H1 hardware platforms from 17.14.1, 17.15.1, or 17.15.2 release to any later release:
    - Causes SNMP user authentication failure.
    - After the upgrade, the mobility tunnels go down and do not re-establish.

  Conditions:

  Regarding the SNMP issue:

    - The controller is hosted on Cisco Catalyst CW9800M, CW9800H2, or CW9800H1, with the 17.14.1, 17.15.1. or 17.15.2 image loaded on the controller.
    - SNMP users are configured on the controller and static SNMP engine ID is not configured.
    - An upgrade is made to a later release, such as 17.15.3.

  Regarding the mobility issue:

    - The controller is hosted on Cisco Catalyst CW9800M, CW9800H2, or CW9800H1, with 17.14.1, 17.15.1. or 17.15.2 image loaded on the controller.
    - Mobility tunnels are already established and mobility MAC is not configured.

  Note If High Availability is configured, the mobility MAC is already configured for it to work.

    - An upgrade is made to a later release, such as 17.15.3.

  Workaround:

    - For the SNMP issue, before you upgrade, follow these steps:
      1. Remove all the configured SNMP users.

         For example,

         ```
         Device(config)# no snmp-server user user-name grp v3
         ```

      2. Configure static engine ID.

         For example,

         ```
         Device(config)# snmp-server engineID local 800000090300F8E94F0077FF
         ```

      3. Configure the SNMP users that were removed earlier.

         For example,
         ```
         Device(config)# snmp-server user user-name grp v3 auth sha cisco1234
         priv aes 128 cisco1234
         ```

      4. Verify that the engine ID has been updated for all users.

         For example,

```
        Device# show snmp user
        User name: user-name
        Engine ID: 800000090300F8E94F0077FF <<<<<<<<<
        storage-type: nonvolatile active
        Authentication Protocol: SHA
        Privacy Protocol: AES128
        Group-name: grp
        ```

    5. Perform the upgrade.

  - For mobility tunnel issue, follow these steps:

    1. Configure mobility MAC address on the controller being upgraded.

        ```
        Device# config terminal
        Device(config)# wireless mobility mac-address mac-address
        ```

    2. Update the peer mobility MAC addresses accordingly on each peer controller.

        ```
        Device# config terminal
        Device(config)# wireless mobility group member mac-address mac-address
        ```

        Momentarily, the mobility tunnel will go down.

    3. Perform the upgrade.

- On Cisco Wireless 9176 AP, you can change the XOR band for slot 0 during runtime to switch between 5-GHz dual-band (Slot 0 and Slot 1) and 5-GHz full band on Slot 1.

  With cyclic toggling of the XOR band on CW9176 AP, Slot 0 from 5-GHz to 2.4-GHz, Slot 1 fails to obtain the 5-GHz full band channels (especially the lower 5-GHz channels). As a result, the channel switch to lower 5-GHz channel fails.

  This is because, the dynamic mode switch was performed only by

  1. updating the `.ini`,
  2. followed by FW recovery, with which, mode switch was not reflected on the device.

  During the XOR band change on CW9176 AP, WLAN firmware reload takes place on Slot 1, for updating the XOR band on Slot 0 and Slot 1. The cyclic toggling of XOR band on CW9176 AP, 5-GHz (Slot 0) to 2.4-GHz, Slot 1 obtains the 5-GHz full band channels (especially the lower 5-GHz channels). Therefore, the channel switch to lower 5G channel works correctly.

- Due to CSCwn80984 (where the management port and the fiber port have the same MAC address), you must configure a mobility MAC address when Cisco Catalyst CW9800H1, CW9800H2, or CW9800M wireless controllers operate in standalone mode (not in HA mode) and handle mobility roaming (with mobility peers).

  To configure the mobility MAC address, use the following command:

  ```
  Device(config)# wireless mobility mac-address H.H.H
  ```

- To prevent controller discovery by Meraki APs (unicast, multicast, or broadcast discovery) during the CAPWAP discovery mode, configure the following:

  ```
  Device(config)# ap profile cisco-ap-profile
  Device(config-ap-profile)# capwap-discovery onboarding {all | unicast}
  ```

- When multi-ciphers (GCMP-128 + GCMP-256) and multi-AKMs (SuiteB + SuiteB-192) are enabled on a WLAN, clients that are compatible with WPA3 security will not support GCMP-128 encryption. Clients supporting GCMP-128 encryption will not be able to join the GCMP-128 + GCMP-256 cipher with SuiteB and SuiteB-192 AKMs.

Supported Hardware

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

Table 8: Supported Virtual and Hardware Platforms

Platform	Description
Cisco Catalyst 9800-80 Wireless Controller	A modular wireless controller with up to 100-GE modular uplinks and seamless software updates. The controller occupies a 2-rack unit space and supports multiple module uplinks.
Cisco Catalyst 9800-40 Wireless Controller	A fixed wireless controller with seamless software updates for mid-size to large enterprises. The controller occupies a 1-rack unit space and provides four 1-GE or 10-GE uplink ports.
Cisco Catalyst 9800-L Wireless Controller	The Cisco Catalyst 9800-L Wireless Controller is the first low-end controller that provides a significant boost in performance and features.
Cisco Catalyst 9800 Wireless Controller for Cloud	A virtual form factor of the Catalyst 9800 Wireless Controller that can be deployed in a private cloud (supports VMware ESXi, Kernel-based Virtual Machine [KVM], Microsoft Hyper-V, and Cisco Enterprise NFV Infrastructure Software [NFVIS] on Enterprise Network Compute System [ENCS] hypervisors), or in the public cloud as Infrastructure as a Service (IaaS) in Amazon Web Services (AWS), Google Cloud Platform (GCP) marketplace, Microsoft Azure, and Oracle Cloud Infrastructure (OCI).
Cisco Catalyst 9800 Embedded Wireless Controller for Switch	The Catalyst 9800 Wireless Controller software for the Cisco Catalyst 9000 switches brings the wired and wireless infrastructure together with consistent policy and management. This deployment model supports only Software Defined-Access (SDA), which is a highly secure solution for small campuses and distributed branches.

Platform	Description
Cisco Catalyst CW9800M Wireless Controller	The Cisco Catalyst CW9800M Wireless Controller is the next generation Cisco Catalyst CW9800 Series Wireless LAN Controller built to deliver a 53% performance improvement while consuming 18% less power when compared to the previous generation models. Additionally, the Cisco Catalyst CW9800M Wireless Controller supports 3000 APs and 32000 clients to ensure better performance and scale for business-critical networks and provides up to 40 Gbps of forwarding throughput for both normal packet and encrypted packets while remaining a single RU designed to save you space and provide greater flexibility in your datacenters.
Cisco Catalyst CW9800H1 and CW9800H2 Wireless Controllers	The Cisco Catalyst CW9800H1 and CW9800H2 Wireless Controllers are the next-generation Cisco Catalyst CW9800 Series Wireless LAN Controllers that boast up to a 36% increase in performance and consume up to 40% less power compared to their predecessors. Additionally, the CW9800H1 and CW9800H2 models are built with a space-saving single RU design and support up to 6000 APs and 64,000 clients with 100 Gbps of maximum throughput. They also offer a choice of uplinks with either 4 x 25 Gbps (CW9800H1) or 2 x 40 Gbps (CW9800H2) configurations to meet high throughput demands of next-generation wireless requirements.

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

Table 9: Supported Host Environments for Public and Private Cloud

Host Environment	Software Version
VMware ESXi	• VMware ESXi vSphere 6.5, 6.7, 7.0, and 8.0 • VMware ESXi vCenter 6.5, 6.7, 7.0, and 8.0
KVM	• Linux KVM-based on Red Hat Enterprise Linux 7.6, 7.8, and 8.2 • Ubuntu 16.04.5 LTS, Ubuntu 18.04.5 LTS, Ubuntu 20.04.5 LTS
AWS	AWS EC2 platform
NFVIS	ENCS 3.8.1 and 3.9.1
GCP	GCP marketplace
Microsoft Hyper-V	Windows Server 2022, Windows Server 2019, and Windows Server 2016 (Version 1607) with Hyper-V Manager (Version 10.0.14393)
Microsoft Azure	Microsoft Azure

Host Environment	Software Version
Oracle Cloud Infrastructure (OCI)	Oracle Cloud Infrastructure (OCI)

The following table lists the supported Cisco Catalyst 9800 Series Wireless Controller hardware models.

The base PIDs are the model numbers of the controller.

The bundled PIDs indicate the orderable part numbers for the base PIDs that are bundled with a particular network module. Running the **show version**, **show module**, or **show inventory** command on such a controller (bundled PID) displays its base PID.

Note that unsupported SFPs will bring down a port. Only Cisco-supported SFPs (GLC-LH-SMD and GLC-SX-MMD) should be used on the route processor (RP) ports of C9800-80-K9 and C9800-40-K9.

Table 10: Supported PIDs and Ports

Controller Model	Description
C9800-CL-K9	Cisco Catalyst Wireless Controller as an infrastructure for cloud.
C9800-80-K9	Eight 1/10-Gigabit Ethernet SFP or SFP+ ports and two power supply slots.
C9800-40-K9	Four 1/10-Gigabit Ethernet SFP or SFP+ ports and two power supply slots.
C9800-L-C-K9	• 4x2.5/1-Gigabit ports • 2x10/5/2.5/1-Gigabit ports
C9800-L-F-K9	• 4x2.5/1-Gigabit ports • 2x10/1-Gigabit ports
CW9800H1	• 8x1 GE/10 GE SFP ports • 4x25 GE SFP interfaces
CW9800H2	• 8x1 GE/10 GE SFP Ports • 2X 40 GE QSFP interfaces
CW9800M	• Four built-in 1 GE /10 GE SFP ports • Two built-in 25 GE SFP ports

The following table lists the supported SFP models.

Table 11: Supported SFPs

SFP Name	C9800-80-K9	C9800-40-K9	C9800-L-F-K9	CW9800H1	CW9800H2	CW9800M
COLORCHIP-C040-Q020-CWDM4-03B	Supported	—	—	—	—	—
DWDM-SFP10G-30.33	Supported	Supported	—	—	—	—
DWDM-SFP10G-61.41	Supported	Supported	—	—	—	—
FINISAR-LR – FTLX1471D3BCL [1]	Supported	Supported	Supported	—	—	—
FINISAR-SR – FTLX8574D3BCL	Supported	Supported	Supported	—	—	—
GLC-BX-D	Supported	Supported	Supported	Supported	Supported	Supported
GLC-BX-U	Supported	Supported	Supported	Supported	Supported	Supported
GLC-EX-SMD	Supported	Supported	—	Supported	Supported	Supported
GLC-LH-SMD	Supported	Supported	—	Supported	Supported	Supported
GLC-SX-MMD	Supported	Supported	Supported	Supported	Supported	Supported
GLC-T	Supported	—	—	—	—	—
GLC-TE	Supported	Supported	Supported	Supported	Supported	Supported
GLC-ZX-SMD	Supported	Supported	Supported	Supported	Supported	Supported
QSFP-100G-LR4-S	Supported	—	—	—	—	—
QSFP-100G-SR4-S	Supported	—	—	—	—	—
QSFP-40G-BD-RX	Supported	—	—	—	—	—
QSFP-40G-ER4	Supported	—	—	—	Supported	—
QSFP-40G-LR4	Supported	—	—	—	Supported	—
QSFP-40G-LR4-S	Supported	—	—	—	Supported	—
QSFP-40G-CSR4	—	—	—	—	Supported	—
QSFP-40G-SR4	Supported	—	—	—	Supported	—
QSFP-40G-SR4-S	Supported	—	—	—	Supported	—
QSFP-40GE-LR4	Supported	—	—	—	—	—
QSFP-H40G-ACU10M	—	—	—	—	Supported	—

SFP Name	C9800-80-K9	C9800-40-K9	C9800-L-F-K9	CW9800H1	CW9800H2	CW9800M
QSFP-H40G-CU1M	—	—	—	—	Supported	—
QSFP-H40G-CU2M	—	—	—	—	Supported	—
QSFP-H40G-CU3M	—	—	—	—	Supported	—
QSFP-H40G-CU4M	—	—	—	—	Supported	—
QSFP-H40G-CU5M	—	—	—	—	Supported	—
QSFP-H40G-CUO-5M	—	—	—	—	Supported	—
QSFP-H40G-AOC1M	—	—	—	—	Supported	—
QSFP-H40G-AOC2M	—	—	—	—	Supported	—
QSFP-H40G-AOC3M	—	—	—	—	Supported	—
QSFP-H40G-AOC5M	—	—	—	—	Supported	—
QSFP-H40G-AOC7M	—	—	—	—	Supported	—
QSFP-H40G-AOC10M	—	—	—	—	Supported	—
QSFP-H40G-AOC15M	—	—	—	—	Supported	—
QSFP-H40G-AOC20M	—	—	—	—	Supported	—
QSFP-H40G-AOC25M	—	—	—	—	Supported	—
QSFP-H40G-AOC30M	—	—	—	—	Supported	—
SFP-10G-AOC10M	Supported	Supported	—	—	—	—
SFP-10G-AOC1M	Supported	Supported	—	Supported	Supported	Supported
SFP-10G-AOC2M	Supported	Supported	—	Supported	Supported	Supported
SFP-10G-AOC3M	Supported	Supported	—	Supported	Supported	Supported
SFP-10G-AOC5M	Supported	Supported	—	Supported	Supported	Supported
SFP-10G-AOC7M	Supported	Supported	—	Supported	Supported	Supported
SFP-10G-ER	Supported	Supported	—	Supported	Supported	Supported
SFP-10G-LR	Supported	Supported	Supported	Supported	Supported	Supported
SFP-10G-LR-S	Supported	Supported	Supported	—	—	—
SFP-10G-LR-X	Supported	Supported	Supported	Supported	Supported	Supported
SFP-10G-LRM	Supported	Supported	Supported	—	—	—
SFP-10G-SR	Supported	Supported	Supported	Supported	Supported	Supported

SFP Name	C9800-80-K9	C9800-40-K9	C9800-L-F-K9	CW9800H1	CW9800H2	CW9800M
SFP-10G-SR-S	Supported	Supported	Supported	Supported	Supported	Supported
SFP-10G-SR-I	—	—	—	Supported	Supported	Supported
SFP-10G-SR-X	Supported	Supported	Supported	—	—	—
SFP-10G-ZR	Supported	Supported	—	—	—	—
SFP-10G-ZR-I	—	—	—	Supported	Supported	Supported
SFP-10G-T-X	—	—	—	Supported	Supported	Supported
SFP-25G-SR-S	—	—	—	Supported	—	Supported
SFP-25G-ER-I	—	—	—	Supported	—	Supported
SFP-10/25G-LR-I	—	—	—	Supported	—	Supported
SFP-10/25G-LR-S	—	—	—	Supported	—	Supported
SFP-10/25G-CSR-S	—	—	—	Supported	—	Supported
SFP-10/25G-BXD-I	—	—	—	Supported	—	Supported
SFP-10/25G-BXU-I	—	—	—	Supported	—	Supported
SFP-H25G-CU1M	—	—	—	Supported	—	Supported
SFP-H25G-CU5M	—	—	—	Supported	—	Supported
SFP-25G-AOC1M	—	—	—	Supported	—	Supported
SFP-25G-AOC2M	—	—	—	Supported	—	Supported
SFP-25G-AOC3M	—	—	—	Supported	—	Supported
SFP-25G-AOC5M	—	—	—	Supported	—	Supported
SFP-25G-AOC7M	—	—	—	Supported	—	Supported
SFP-25G-AOC10M	—	—	—	Supported	—	Supported
SFP-H10GB-ACU10M	Supported	Supported	Supported	Supported	Supported	Supported
SFP-H10GB-ACU7M	Supported	Supported	Supported	Supported	Supported	Supported
SFP-H10GB- CU1.5M	Supported	Supported	Supported	—	—	—
SFP-H10GB-CU1M	Supported	Supported	Supported	Supported	Supported	Supported
SFP-H10GB-CU2.5M	Supported	Supported	Supported	—	—	—
SFP-H10GB-CU2M	Supported	Supported	Supported	Supported	Supported	Supported
SFP-H10GB-CU3M	Supported	Supported	Supported	Supported	Supported	Supported

SFP Name	C9800-80-K9	C9800-40-K9	C9800-L-F-K9	CW9800H1	CW9800H2	CW9800M
SFP-H10GB-CU5M	Supported	Supported	Supported	Supported	Supported	Supported
SFP-H10GB-CU1-5M	Supported	Supported	—	Supported	Supported	Supported
Finisar-LR (FTLX1471D3BCL)	—	—	Supported	Supported	Supported	Supported
Finisar-SR (FTLX8574D3BC)	—	—	—	Supported	Supported	Supported

[1] The FINISAR SFPs are not Cisco specific and some of the features, such as DOM, may not work properly.

Optics Modules

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

https://www.cisco.com/c/en/us/support/interfaces-modules/transceiver-modules/products-device-support-tables-list.html

Network Protocols and Port Matrix

Table 12: Cisco Catalyst 9800 Series Wireless Controller - Network Protocols and Port Matrix

Source	Destination	Protocol	Destination Port	Source Port	Description
Any	Cisco Catalyst 9800 Series Wireless Controller	TCP	22	Any	SSH
Any	Cisco Catalyst 9800 Series Wireless Controller	TCP	23	Any	Telnet
Any	Cisco Catalyst 9800 Series Wireless Controller	TCP	80	Any	HTTP
Any	Cisco Catalyst 9800 Series Wireless Controller	TCP	443	Any	HTTPS

Source	Destination	Protocol	Destination Port	Source Port	Description
Any	Cisco Catalyst 9800 Series Wireless Controller	UDP	161	Any	SNMP Agent
Any	Any	UDP	5353	5353	mDNS
Any	Cisco Catalyst 9800 Series Wireless Controller	UDP	69	69	TFTP
Any	DNS Server	UDP	53	Any	DNS
Any	Cisco Catalyst 9800 Series Wireless Controller	TCP	830	Any	NetConf
Any	Cisco Catalyst 9800 Series Wireless Controller	TCP	443	Any	REST API
Any	WLC Protocol	UDP	1700	Any	Receive CoA packets.
AP	Cisco Catalyst 9800 Series Wireless Controller	UDP	5246	Any	CAPWAP Control
AP	Cisco Catalyst 9800 Series Wireless Controller	UDP	5247	Any	CAPWAP Data
AP	Cisco Catalyst 9800 Series Wireless Controller	UDP	5248	Any	CAPWAP MCAST
AP	Cisco Catalyst Center	TCP	32626	Any	Intelligent capture and RF telemetry
AP	AP	UDP	16670	Any	Client Policies (AP-AP)

Source	Destination	Protocol	Destination Port	Source Port	Description
Cisco Catalyst 9800 Series Wireless Controller	Cisco Catalyst 9800 Series Wireless Controller	UDP	16666	16666	Mobility Control
Cisco Catalyst 9800 Series Wireless Controller	SNMP	UDP	162	Any	SNMP Trap
Cisco Catalyst 9800 Series Wireless Controller	RADIUS	UDP	1812/1645	Any	RADIUS Auth
Cisco Catalyst 9800 Series Wireless Controller	RADIUS	UDP	1813/1646	Any	RADIUS ACCT
Cisco Catalyst 9800 Series Wireless Controller	TACACS+	TCP	49	Any	TACACS+
Cisco Catalyst 9800 Series Wireless Controller	Cisco Catalyst 9800 Series Wireless Controller	UDP	16667	16667	Mobility
Cisco Catalyst 9800 Series Wireless Controller	NTP Server	UDP	123	Any	NTP
Cisco Catalyst 9800 Series Wireless Controller	Syslog Server	UDP	514	Any	SYSLOG
AP	Cisco Catalyst 9800 Series Wireless Controller	HTTPS	8443	Any	Out of Band AP Image Download Cisco CleanAir Spectral Capture
Cisco Catalyst 9800 Series Wireless Controller	NetFlow Server	UDP	9996	Any	NetFlow

Source	Destination	Protocol	Destination Port	Source Port	Description
Cisco Catalyst 9800 Series Wireless Controller	Cisco Connected Mobile Experiences (CMX)	UDP	16113	Any	NMSP
Cisco Catalyst Center	Cisco Catalyst 9800 Series Wireless Controller	TCP	32222	Any	Device Discovery
Cisco Catalyst Center	Cisco Catalyst 9800 Series Wireless Controller	TCP	25103	Any	Telemetry Subscriptions

Supported APs

The following Cisco APs are supported in this release.

Indoor Access Points

- Cisco Catalyst 9105AX (I/W) Access Points
- Cisco Catalyst 9115AX (I/E) Access Points
- Cisco Catalyst 9117AX (I) Access Points
- Cisco Catalyst 9120AX (I/E/P) Access Points
- Cisco Catalyst 9130AX (I/E) Access Points
- Cisco Catalyst 9136AX Access Points
- Cisco Catalyst 9162 (I) Series Access Points
- Cisco Catalyst 9164 (I) Series Access Points
- Cisco Catalyst 9166 (I/D1) Series Access Points
- Cisco Wireless 9172 (I) Series Wi-Fi 7 Access Points
- Cisco Wireless 9176 (I/D1) Series Wi-Fi 7 Access Points
- Cisco Wireless 9178 (I) Series Wi-Fi 7 Access Points
- Cisco Aironet 1815 (I/W/M/T), 1830 (I), 1840 (I), and 1852 (I/E) Access Points
- Cisco Aironet 1800i Access Point
- Cisco Aironet 2800 (I/E) Series Access Points
- Cisco Aironet 3800 (I/E/P) Series Access Points
- Cisco Aironet 4800 (I) Series Access Points

Outdoor Access Points

- Cisco Aironet 1540 (I/D) Series Access Points
- Cisco Aironet 1560 (I/D/E) Series Access Points
- Cisco Aironet 1570 (I/D/E) Series Access Points
- Cisco Aironet 1570 (IC/EC/EAC) Series Access Points
- Cisco Catalyst Industrial Wireless 6300 Heavy Duty Series Access Point
- Cisco 6300 Series Embedded Services Access Point
- Cisco Catalyst 9124AX (I/D/E) Access Points
- Cisco Catalyst 9163 (E) Series Access Points
- Cisco Catalyst Industrial Wireless 9167 (I/E) Heavy Duty Access Points
- Cisco Catalyst Industrial Wireless 9165E Rugged Access Point
- Cisco Catalyst Industrial Wireless 9165D Heavy Duty Access Point

Integrated Access Points

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

Network Sensor

- Cisco Aironet 1800s Active Sensor

Pluggable Modules

- Cisco Wi-Fi Interface Module (WIM)

Supported Access Point Channels and Maximum Power Settings

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

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

Compatibility Matrix

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

Table 13: Compatibility Information

Cisco Catalyst 9800 Series Wireless Controller Software	Cisco Identity Services Engine	Cisco Prime Infrastructure	Cisco AireOS-IRCM Interoperability	Cisco Catalyst Center	Cisco CMX
IOS XE 17.15.4	3.4 3.3 3.2 3.1 3.0 2.7 * all with latest patches	3.10.6 (base version) **Note** Base release of Cisco Prime Infrastructure that supports corresponding Cisco Catalyst 9800 Series Wireless Controller platform release and its features.	8.10.196.0 8.10.190.0 8.10.185.0 8.10.183.0 8.10.182.0 8.10.181.0 8.10.171.0 8.10.162.0 8.10.151.0 8.10.142.0 8.10.130.0 8.5.176.2 8.5.182.104	See Cisco Catalyst Center Compatibility Information	11.0.0 10.6.3
IOS XE 17.15.3	3.4 3.3 3.2 3.1 3.0 2.7 * all with latest patches	3.10.6 (base version) **Note** Base release of Cisco Prime Infrastructure that supports corresponding Cisco Catalyst 9800 Series Wireless Controller platform release and its features.	8.10.196.0 8.10.190.0 8.10.185.0 8.10.183.0 8.10.182.0 8.10.181.0 8.10.171.0 8.10.162.0 8.10.151.0 8.10.142.0 8.10.130.0 8.5.176.2 8.5.182.104	See Cisco Catalyst Center Compatibility Information	11.0.0 10.6.3

Cisco Catalyst 9800 Series Wireless Controller Software	Cisco Identity Services Engine	Cisco Prime Infrastructure	Cisco AireOS-IRCM Interoperability	Cisco Catalyst Center	Cisco CMX
IOS XE 17.15.2b	3.4 3.3 3.2 3.1 3.0 2.7 * all with latest patches	3.10.6 (base version) **Note** Base release of Cisco Prime Infrastructure that supports corresponding Cisco Catalyst 9800 Series Wireless Controller platform release and its features.	8.10.196.0 8.10.190.0 8.10.185.0 8.10.183.0 8.10.182.0 8.10.181.0 8.10.171.0 8.10.162.0 8.10.151.0 8.10.142.0 8.10.130.0 8.5.176.2 8.5.182.104	See Cisco Catalyst Center Compatibility Information	11.0.0 10.6.3
IOS XE 17.15.2	3.4 3.3 3.2 3.1 3.0 2.7 * all with latest patches	3.10.6 (base version) **Note** Base release of Cisco Prime Infrastructure that supports corresponding Cisco Catalyst 9800 Series Wireless Controller platform release and its features.	8.10.196.0 8.10.190.0 8.10.185.0 8.10.183.0 8.10.182.0 8.10.181.0 8.10.171.0 8.10.162.0 8.10.151.0 8.10.142.0 8.10.130.0 8.5.176.2 8.5.182.104	See Cisco Catalyst Center Compatibility Information	11.0.0 10.6.3

Cisco Catalyst 9800 Series Wireless Controller Software	Cisco Identity Services Engine	Cisco Prime Infrastructure	Cisco AireOS-IRCM Interoperability	Cisco Catalyst Center	Cisco CMX
IOS XE 17.15.1	3.4 3.3 3.2 3.1 3.0 2.7 * all with latest patches	3.10.6 (base version) **Note** Base release of Cisco Prime Infrastructure that supports corresponding Cisco Catalyst 9800 Series Wireless Controller platform release and its features.	8.10.196.0 8.10.190.0 8.10.185.0 8.10.183.0 8.10.182.0 8.10.181.0 8.10.171.0 8.10.162.0 8.10.151.0 8.10.142.0 8.10.130.0 8.5.176.2 8.5.182.104	See Cisco Catalyst Center Compatibility Information	11.0.0 10.6.3

GUI System Requirements

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

Table 14: Hardware Requirements

Processor Speed	DRAM	Number of Colors	Resolution	Font Size
233 MHz minimum[2]	512 MB[3]	256	1280 x 800 or higher	Small

[2] We recommend 1 GHz.
[3] We recommend 1-GB DRAM.

Software Requirements

Operating Systems:

- Windows 7 or later
- Mac OS X 10.11 or later

Browsers:

- Google Chrome: Version 59 or later (on Windows and Mac)
- Microsoft Edge: Version 40 or later (on Windows)
- Safari: Version 10 or later (on Mac)
- Mozilla Firefox: Version 60 or later (on Windows and Mac)

Note Firefox Version 63.x is not supported.

The controller GUI uses Virtual Terminal (VTY) lines for processing HTTP requests. At times, when multiple connections are open, the default number of VTY lines of 15 set by the device might get exhausted. Therefore, we recommend that you increase the number of VTY lines to 50.

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

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

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

Before You Upgrade

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

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

  Workaround:

  - Upgrade using the CLI commands, or,
  - Upgrade to a fixed release first, and then upgrade to 17.15.x.
- Kernel panic is observed in CW9176 while disabling few of the associated clients.
- Kernel panic is observed in CW9176 and CW9178 during configuration change, after the initial bootup.

  After upgrading the controller image, the AP joins the controller and reboots. Kernel panic is observed when the policy tag is changed for the first time. This is seen only the first time after build upgrade.
- When you upgrade from Cisco IOS XE Dublin 17.12.3 to 17.12.4 or Cisco IOS XE 17.15.1, the Cisco Catalyst Wi-Fi 6 APs fail to upgrade the AP image.

  Workaround:

  - Reboot the impacted APs through the power cycle.

For more information, see CSCwm08044

Important The Cisco Catalyst 9800 Series Wireless Controller may experience an unexpected reload when CLI **accounting** is enabled and the wireless configuration is changed using the WebUI with an IPv6 address. The issue affects only wireless platforms.

Workaround:

- Disable the CLI accounting command when accessing the WebUI with an IPv6 address, or,
- Access the WebUI with an IPv4 address when the CLI accounting command is enabled.

- The Air Quality Sensor feature is disabled in Cisco IOS XE 17.15.1. Although, you may be able to view the **Config-State** (as Enabled), **Admin-State** (as Enabled), and **Oper-Status** (as Up), there will be no values sent from the Air Quality Sensor.

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

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

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

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

Note

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

- From Cisco IOS XE Dublin 17.10.x, Key Exchange and MAC algorithms like diffie-hellman-group14-sha1, hmac-sha1, hmac-sha2-256, and hmac-sha2-512 are not supported by default and it may impact some SSH clients that only support these algorithms. If required, you can add them manually. For information on manually adding these algorithms, see the **SSH Algorithms for**

Common Criteria Certification document available at:
https://www.cisco.com/c/en/us/td/docs/routers/ios/config/17-x/sec-vpn/b-security-vpn/m_sec-secure-shell-algorithm-ccc.html

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

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

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

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

     ```
     Device# capwap ap restart
     ```

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

- Fragmentation lower than 1500 is not supported for the RADIUS packets generated by wireless clients in the Gi0 (OOB) interface.

- Cisco IOS XE allows you to encrypt all the passwords used on the device. This includes user passwords and SSID passwords (PSK). For more information, see the "Password Encryption" section of the Cisco Catalyst 9800 Series Configuration Best Practices document.

- While upgrading to Cisco IOS XE 17.3.x and later releases, if the **ip http active-session-modules none** command is enabled, you will not be able to access the controller GUI using HTTPS. To access the GUI using HTTPS, run the following commands in the order specified below:

  1. **ip http session-module-list pkilist OPENRESTY_PKI**

  2. **ip http active-session-modules pkilist**

- Cisco Aironet 1815T OfficeExtend Access Point will be in local mode when connected to the controller. However, when it functions as a standalone AP, it gets converted to FlexConnect mode.

- The Cisco Catalyst 9800-L Wireless Controller may fail to respond to the BREAK signals received on its console port during boot time, preventing users from getting to the ROMMON. This problem is observed on the controllers manufactured until November 2019, with the default config-register setting of 0x2102. This problem can be avoided if you set config-register to 0x2002. This problem is fixed in the 16.12(3r) ROMMON for Cisco Catalyst 9800-L Wireless Controller. For information about how to upgrade the ROMMON, see the Upgrading ROMMON for Cisco Catalyst 9800-L Wireless Controllers section of the Upgrading Field Programmable Hardware Devices for Cisco Catalyst 9800 Series Wireless Controllers document.

- By default, the controller uses a TFTP block size value of 512, which is the lowest possible value. This default setting is used to ensure interoperability with legacy TFTP servers. If required, you can change the block size value to 8192 to speed up the transfer process, using the **ip tftp blocksize** command in global configuration mode.

- We recommend that you configure the **password encryption aes** and the **key config-key password-encrypt** *key* commands to encrypt your password.

- If the following error message is displayed after a reboot or system crash, we recommend that you regenerate the trustpoint certificate:

  ```
  ERR_SSL_VERSION_OR_CIPHER_MISMATCH
  ```

  Use the following commands in the order specified below to generate a new self-signed trustpoint certificate:

  1. device# **configure terminal**
  2. device(config)# **no crypto pki trustpoint** *trustpoint_name*
  3. device(config)# **no ip http server**
  4. device(config)# **no ip http secure-server**
  5. device(config)# **ip http server**
  6. device(config)# **ip http secure-server**
  7. device(config)# **ip http authentication** *local/aaa*

- Do not deploy OVA files directly to VMware ESXi 6.5. We recommend that you use an OVF tool to deploy the OVA files.
- Ensure that you remove the controller from Cisco Prime Infrastructure before disabling or enabling Netconf-YANG. Otherwise, the system may reload unexpectedly.
- Unidirectional Link Detection (UDLD) protocol is not supported.
- SIP media session snooping is not supported on FlexConnect local switching deployments.
- The Cisco Catalyst 9800 Series Wireless Controllers (C9800-CL, C9800-L, C9800-40, and C9800-80) support a maximum of 14,000 leases with internal DHCP scope.
- Configuring the mobility MAC address using the **wireless mobility mac-address** command is mandatory for both HA and 802.11r.
- If you have Cisco Catalyst 9120 (E/I/P) and Cisco Catalyst 9130 (E) APs in your network and you want to downgrade, use only Cisco IOS XE Gibraltar 16.12.1t. Do not downgrade to Cisco IOS XE Gibraltar 16.12.1s.
- The following SNMP variables are not supported:
  - CISCO-LWAPP-WLAN-MIB: cLWlanMdnsMode
  - CISCO-LWAPP-AP-MIB.my: cLApDot11IfRptncPresent, cLApDot11IfDartPresent
- If you are upgrading from Cisco IOS XE Gibraltar 16.11.x or an earlier release, ensure that you unconfigure the *advipservices* boot-level licenses on both the active and standby controllers using the **no license boot level advipservices** command before the upgrade. Note that the **license boot level advipservices** command is not available in Cisco IOS XE Gibraltar 16.12.1s and 16.12.2s.
- The Cisco Catalyst 9800 Series Wireless Controller has a service port that is referred to as *GigabitEthernet 0* port.

  The following protocols and features are supported through this port:

  - Cisco Catalyst Center

  - Cisco Smart Software Manager
  - Cisco Prime Infrastructure
  - Telnet
  - Controller GUI
  - HTTP
  - HTTPS
  - Licensing for Smart Licensing feature to communicate with CSSM
  - SSH

- During device upgrade using GUI, if a switchover occurs, the session expires and the upgrade process gets terminated. As a result, the GUI cannot display the upgrade state or status.

- From Cisco IOS XE Bengaluru 17.4.1 onwards, the telemetry solution provides a name for the receiver address instead of the IP address for telemetry data. This is an additional option. During the controller downgrade and subsequent upgrade, there is likely to be an issue—the upgrade version uses the newly named receivers, and these are not recognized in the downgrade. The new configuration gets rejected and fails in the subsequent upgrade. Configuration loss can be avoided when the upgrade or downgrade is performed from Cisco Catalyst Center.

- Communication between Cisco Catalyst 9800 Series Wireless Controller and Cisco Prime Infrastructure uses different ports:
  - All the configurations and templates available in Cisco Prime Infrastructure are pushed through SNMP and CLI, using UDP port 161.
  - Operational data for controller is obtained over SNMP, using UDP port 162.
  - AP and client operational data leverage streaming telemetry:
    - Cisco Prime Infrastructure to controller: TCP port 830 is used by Cisco Prime Infrastructure to push the telemetry configuration to the controller (using NETCONF).
    - Controller to Cisco Prime Infrastructure: TCP port 20828 is used for Cisco IOS XE 16.10.x and 16.11.x, and TCP port 20830 is used for Cisco IOS XE 16.12.x, 17.1.x and later releases.

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

- To migrate public IP address from 16.12.x to 17.x. ensure that you configure the **service internal** command. If you do not configure the **service internal** command, the IP address does not get carried forward.

- RLAN support with Virtual Routing and Forwarding (VRF) is not available.

- When you encounter the SNMP error *SNMP_ERRORSTATUS_NOACCESS 6*, it means that the specified SNMP variable is not accessible.

- We recommend that you perform a controller reload whenever there is a change in the controller's clock time to reflect an earlier time.

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

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

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

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

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

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

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

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

Upgrade Path to Cisco IOS XE 17.15.x

Table 15: Upgrade Path to Cisco IOS XE Dublin 17.15.x (where x > 1)

Current Software	Upgrade Path for Deployments with 9130 or 9124	Upgrade Path for Deployments Without 9130 or 9124
16.10.x	—[4]	Upgrade first to 16.12.5 or 17.3.x and then to 17.15.x.
16.11.x	—	Upgrade first to 16.12.5 or 17.3.x and then to 17.15.x.
16.12.x	Upgrade first to 17.3.5 or later or 17.6.x or later, then to 17.9.6 or later or 17.12.x or later, and then to 17.15.x.	Upgrade first to 17.3.5 or later or 17.6.x or later, and then to 17.15.x.

Current Software	Upgrade Path for Deployments with 9130 or 9124	Upgrade Path for Deployments Without 9130 or 9124
17.1.x	Upgrade first to 17.3.5 or later, then to 17.9.6 or later or 17.12.x or later, and then to 17.15.x.	Upgrade first to 17.3.5 or later and then to 17.15.x.
17.2.x	Upgrade first to 17.3.5 or later, then to 17.9.6 or later or 17.12.x or later, and then to 17.15.x.	Upgrade first to 17.3.5 or later and then to 17.15.x.
17.3.1 to 17.3.4	Upgrade first to 17.3.5 or later or 17.6.x or later, then to 17.9.6 or later or 17.12.x or later, and then to 17.15.x.	Upgrade directly to 17.15.x.
17.3.4c or later	Upgrade to 17.9.6 or later or 17.12.x or later, and then to 17.15.x.	Upgrade directly to 17.15.x.
17.4.x	Upgrade first to 17.6.x and then to 17.15.x.	Upgrade directly to 17.15.x.
17.5.x	Upgrade first to 17.6.x and then to 17.15.x.	Upgrade directly to 17.15.x.
17.6.x	Upgrade to 17.9.6 or later or 17.12.x or later, and then to 17.15.x.	Upgrade directly to 17.15.x.
17.7.x	Upgrade to 17.9.6 or later or 17.12.x or later, and then to 17.15.x.	Upgrade directly to 17.15.x.
17.8.x	Upgrade to 17.9.6 or later or 17.12.x or later, and then to 17.15.x.	Upgrade directly to 17.15.x.
17.9.1 to 17.9.5	Upgrade to 17.9.6 or later or 17.12.x or later, and then to 17.15.x	Upgrade directly to 17.15.x
17.9.6 or later	Upgrade directly to 17.15.x	Upgrade directly to 17.15.x
17.10.x	Upgrade to 17.12.x or later, and then to 17.15.x	Upgrade directly to 17.15.x
17.11.x	Upgrade to 17.12.x or later, and then to 17.15.x	Upgrade directly to 17.15.x
17.12.x	Upgrade directly to 17.15.x	Upgrade directly to 17.15.x
17.13.x	Upgrade directly to 17.15.x	Upgrade directly to 17.15.x
17.14.x	Upgrade directly to 17.15.x	Upgrade directly to 17.15.x

Current Software	Upgrade Path for Deployments with 9130 or 9124	Upgrade Path for Deployments Without 9130 or 9124
8.9.x or any 8.10.x version prior to 8.10.171.0	Upgrade first to 8.10.171.0 or later, 17.3.5 or later or 17.6.x or later, then to 17.9.6 or later or 17.12.x or later, and then to 17.15.x	Upgrade directly to 17.15.x.

[4] The Cisco Catalyst 9130 and 9124 APs are not supported in 16.10.x and 16.11.x releases.

Note Cisco IOS XE 17.15.1 or later releases have a file size of more than 1.5 GB, which is not supported by Cisco IOS XE 17.11.1 or earlier releases. If you are running Cisco IOS XE 17.11.1 or earlier releases, you must first upgrade to Cisco IOS XE 17.12.x (for example, 17.12.5), and then upgrade to Cisco IOS XE 17.15.x or later. Additionally, an AP running Cisco IOS XE 17.9.5 or an earlier release does not have enough storage space to download Cisco IOS XE 17.15.x releases.Therefore, if you upgrade an AP image from 17.9.5 to 17.15.x would also fail.

Upgrading the Controller Software

This section describes the various aspects of upgrading the controller software.

Finding the Software Version

The package files for the Cisco IOS XE software are stored in the system board flash device (flash:).

Use the **show version** privileged EXEC command to see the software version that is running on your controller.

Note Although the **show version** output always shows the software image running on the controller, the model name shown at the end of the output is the factory configuration, and does not change if you upgrade the software license.

Use the **show install summary** privileged EXEC command to see the information about the active package.

Use the **dir** *filesystem:* privileged EXEC command to see the directory names of other software images that you have stored in flash memory.

Software Images

- **Release**: Cisco IOS XE 17.15.x
- **Image Names (9800-80, 9800-40, and 9800-L)**:
  - C9800-80-universalk9_wlc.17.15.x.SPA.bin
  - C9800-40-universalk9_wlc.17.15.x.SPA.bin
  - C9800-L-universalk9_wlc.17.15.x.SPA.bin
- **Image Names (9800-CL)**:

- **Cloud**: C9800-CL-universalk9.17.15.x.SPA.bin
- **Hyper-V/ESXi/KVM**: C9800-CL-universalk9.17.15.x.iso, C9800-CL-universalk9.17.15.x.ova
- **KVM**: C9800-CL-universalk9.17.15.x.qcow2
- **NFVIS**: C9800-CL-universalk9.17.15.x.tar.gz

Software Installation Commands

<table>
<tr><th colspan="2">Cisco IOS XE 17.15.x</th></tr>
<tr><td colspan="2">To install and activate a specified file, and to commit changes to be persistent across reloads, run the following command:
<b>device# install add file</b> <i>filename</i> <b>[activate |commit]</b>
To separately install, activate, commit, end, or remove the installation file, run the following command:
<b>device# install ?</b>
<b>Note</b>
We recommend that you use the GUI for installation.</td></tr>
<tr><td><b>add file tftp:</b> <i>filename</i></td><td>Copies the install file package from a remote location to a device, and performs a compatibility check for the platform and image versions.</td></tr>
<tr><td><b>activateauto-abort-timer</b>]</td><td>Activates the file and reloads the device. The <b>auto-abort-timer</b> keyword automatically rolls back image activation.</td></tr>
<tr><td><b>commit</b></td><td>Makes changes that are persistent over reloads.</td></tr>
<tr><td><b>rollback to committed</b></td><td>Rolls back the update to the last committed version.</td></tr>
<tr><td><b>abort</b></td><td>Cancels file activation, and rolls back to the version that was running before the current installation procedure started.</td></tr>
<tr><td><b>remove</b></td><td>Deletes all unused and inactive software installation files.</td></tr>
</table>

Licensing

Cisco Wireless Licences

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

The Cisco Wireless licenses consist of the following tiers:

- **Cisco Wireless Essentials**: The tier that provides fundamental features and functionalities that are essential to manage a network.

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

For more information, see Cisco Wireless Licensing.

Smart 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 16: Test Configuration for Interoperability

Hardware or Software Parameter	Hardware or Software Type
Release	Cisco IOS XE 17.15.x
Cisco Wireless Controller	See Supported Hardware, on page 23.
Access Points	See Supported APs, on page 32.
Radio	• 802.11ac • 802.11a • 802.11g • 802.11n • 802.11ax in 6GHz (Wi-Fi 6E) • 802.11be (Wi-Fi 7)
Security	Open, PSK (WPA2-AES), 802.1X (WPA2-AES) (EAP-FAST, EAP-TLS)
RADIUS	See Compatibility Matrix, on page 33.
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 17: Client Types

Client Type and Name	Driver or Software Version
Laptops	
Acer Aspire E 15 E5-573-3870 (Qualcomm Atheros QCA9377)	Windows 10 Pro (12.0.0.832)
Apple Macbook Air 11 inch	macOS Sierra 10.12.6
Apple Macbook Air 13 inch	macOS High Sierra 10.13.4
Macbook Pro Retina	macOS Catalina
Macbook Pro Retina 13 inch early 2015	macOS Mojave 10.14.3
Macbook Pro OS X	macOS X 10.8.5
Macbook Air	macOS Sierra v10.12.2
Macbook Air 11 inch	macOS Yosemite 10.10.5
MacBook M1 Chip	macOS Catalina
MacBook M1 Chip	macOS Ventura 13.2.1
MacBook Pro M2 Chip	macOS Ventura 13.3 beta
MacBook Pro M2 Chip	macOS Ventura 13.1
Dell Inspiron 2020 Chromebook	Chrome OS 75.0.3770.129
Google Pixelbook Go	Chrome OS 97.0.4692.27
HP chromebook 11a	Chrome OS 76.0.3809.136
Samsung Chromebook 4+	Chrome OS 77.0.3865.105
Dell Latitude (Intel AX210)	Windows 11 (22.110.x.x)
Dell Latitude 3480 (Qualcomm DELL wireless 1820)	Win 10 Pro (12.0.0.242)
Dell Inspiron 15-7569 (Intel Dual Band Wireless-AC 3165)	Windows 10 Home (21.40.0)
Dell Latitude E5540 (Intel Dual Band Wireless AC7260)	Windows 7 Professional (21.10.1)
Dell Latitude E5430 (Intel Centrino Advanced-N 6205)	Windows 7 Professional (15.18.0.1)
Dell Latitude E6840 (Broadcom Dell Wireless 1540 802.11 a/g/n)	Windows 7 Professional (6.30.223.215)
Dell XPS 12 v9250 (Intel Dual Band Wireless AC 8260)	Windows 10 Home (21.40.0)
Dell Latitude 5491 (Intel AX200)	Windows 10 Pro (21.20.1.1)

Client Type and Name	Driver or Software Version
Dell XPS Latitude12 9250 (Intel Dual Band Wireless AC 8260)	Windows 10 Home
Dell Inspiron 13-5368 Signature Edition	Windows 10 Home (18.40.0.12)
FUJITSU Lifebook E556 Intel 8260 (Intel Dual Band Wireless-AC 8260 (802.11n))	Windows 8 (19.50.1.6)
Lenovo Yoga C630 Snapdragon 850 (Qualcomm AC 2x2 Svc)	Windows 10 Home
Lenovo Thinkpad Yoga 460 (Intel Dual Band Wireless-AC 9260)	Windows 10 Pro (21.40.0)
Note For clients using Intel wireless cards, we recommend that you to update to the latest Intel wireless drivers if the advertised SSIDs are not visible.	
Tablets	
Apple iPad Pro (12.9 inch) 6th Gen	iOS 16.4
Apple iPad Pro (11 inch) 4th Gen	iOS 16.4
Apple iPad 2021	iOS 15.0
Apple iPad 7the Gen 2019	iOS 14.0
Apple iPad MD328LL/A	iOS 9.3.5
Apple iPad 2 MC979LL/A	iOS 11.4.1
Apple iPad Air MD785LL/A	iOS 11.4.1
Apple iPad Air2 MGLW2LL/A	iOS 10.2.1
Apple iPad Mini 4 9.0.1 MK872LL/A	iOS 11.4.1
Apple iPad Mini 2 ME279LL/A	iOS 11.4.1
Apple iPad Mini 4 9.0.1 MK872LL/A	iOS 11.4.1
Microsoft Surface Pro 3 13 inch (Intel AX201)	Windows 10 (21.40.1.3)
Microsoft Surface Pro 3 15 inch (Qualcomm Atheros QCA61x4A)	Windows 10
Microsoft Surface Pro 7 (Intel AX201)	Windows 10
Microsoft Surface Pro 6 (Marvell Wi-Fi chipset 11ac)	Windows 10
Microsoft Surface Pro X (WCN3998 Wi-Fi Chip)	Windows
Mobile Phones	
Apple iPhone 5	iOS 12.4.1
Apple iPhone 6s	iOS 13.5

Client Type and Name	Driver or Software Version
Apple iPhone 7 MN8J2LL/A	iOS 11.2.5
Apple iPhone 8	iOS 13.5
Apple iPhone 8 Plus	iOS 14.1
Apple iPhone 8 Plus MQ8D2LL/A	iOS 12.4.1
Apple iPhone X MQA52LL/A	iOS 13.1
Apple iPhone 11	iOS 15.1
Apple iPhone 12	iOS 16.0
Apple iPhone 12 Pro	iOS 15.1
Apple iPhone 13	iOS 15.1
Apple iPhone 13 Mini	iOS 15.1
Apple iPhone 13 Pro	iOS 15.1
Apple iPhone SE MLY12LL/A	iOS 11.3
Apple iPhone SE	iOS 15.1
ASCOM i63	Build v 3.0.0
ASCOM Myco 3	Android 9
Cisco IP Phone 8821	11.0.6 SR4
Drager Delta	VG9.0.2
Drager M300.3	VG3.0
Drager M300.4	VG3.0
Drager M540	VG4.2
Google Pixel 3a	Android 11
Google Pixel 4	Android 11
Google Pixel 5	Android 11
Google Pixel 6	Android 12
Google Pixel 7	Android 13
Huawei Mate 20 pro	Android 9.0
Huawei P20 Pro	Android 10
Huawei P40	Android 10
LG v40 ThinQ	Android 9.0
One Plus 8	Android 11
Oppo Find X2	Android 10

Client Type and Name	Driver or Software Version
Redmi K20 Pro	Android 10
Samsung Galaxy S9+ - G965U1	Android 10.0
Samsung Galaxy S10 Plus	Android 11.0
Samsung S10 (SM-G973U1)	Android 11.0
Samsung S10e (SM-G970U1)	Android 11.0
Samsung Galaxy S20 Ultra	Android 10.0
Samsung Galaxy S21 Ultra 5G	Android 13.0
Samsung Galaxy S22 Ultra	Android 13.0
Samsung Fold 2	Android 10.0
Samsung Galaxy Z Fold 3	Android 13.0
Samsung Note20	Android 12.0
Samsung G Note 10 Plus	Android 11.0
Samsung Galaxy A01	Android 11.0
Samsung Galaxy A21	Android 10.0
Sony Experia 1 ii	Android 11
Sony Experia	Android 11
Xiaomi Mi 9T	Android 9
Xiaomi Mi 10	Android 11
Spectralink 84 Series	7.5.0.x257
Spectralink 87 Series	Android 5.1.1
Spectralink Versity Phones 92/95/96 Series	Android 10.0
Spectralink Versity Phones 9540 Series	Android 8.1.0
Vocera Badges B3000n	4.3.3.18
Vocera Smart Badges V5000	5.0.6.35
Zebra MC40	Android 4.4.4
Zebra MC40N0	Android 4.1.1
Zebra MC92N0	Android 4.4.4
Zebra MC9090	Windows Mobile 6.1
Zebra MC55A	Windows 6.5

Client Type and Name	Driver or Software Version
Zebra MC75A	OEM ver 02.37.0001
Zebra TC51	Android 6.0.1
Zebra TC52	Android 10.0
Zebra TC55	Android 8.1.0
Zebra TC57	Android 10.0
Zebra TC58	Android 11.0
Zebra TC70	Android 6.1
Zebra TC75	Android 10.0
Zebra TC520K	Android 10.0
Zebra TC8000	Android 4.4.3
Printers	
Zebra QLn320 Mobile Printer	LINK OS 5.2
Zebra ZT230 IndustrialPrinter	LINK OS 6.4
Zebra ZQ310 Mobile Printer	LINK OS 6.4
Zebra ZD410 Industrial Printer	LINK OS 6.4
Zebra ZT410 Desktop Printer	LINK OS 6.2
Zebra ZQ610 Industrial Printer	LINK OS 6.4
Zebra ZQ620 Mobile Printer	LINK OS 6.4
Wireless Module	
Intel AX 411	Driver v22.230.0.8
Intel AX 211	Driver v22.230.0.8, v22.190.0.4
Intel AX 210	Driver v22.230.0.8, v22.190.0.4, v22.170.2.1
Intel AX 200	Driver v22.130.0.5
Intel 11AC	Driver v22.30.0.11
Intel AC 9260	Driver v21.40.0
Intel Dual Band Wireless AC 8260	Driver v19.50.1.6
Samsung S21 Ultra	Driver v20.80.80
QCA WCN6855	Driver v1.0.0.901
PhoenixContact FL WLAN 2010	Firmware version: 2.71

Issues

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

Note All incremental releases contain fixes from the current release.

Cisco Bug Search Tool

The Cisco Bug Search Tool (BST) allows partners and customers to search for software bugs based on product, release, and keyword, and aggregates key data such as bug details, product, and version. The BST is designed to improve the effectiveness in network risk management and device troubleshooting. The tool has a provision to filter bugs based on credentials to provide external and internal bug views for the search input.

To view the details of an issue, click the corresponding identifier.

Open Issues for Cisco IOS XE 17.15.4

Identifier	Headline
CSCwk79990	Controller encounters kernel unresponsiveness due to IntelResetRequest
CSCwp14628	Cisco Aironet 3800 APs display client authentication issue after AP Migration to a controller running 17.15.3
CSCwp20385	Cisco Catalyst 9136 AP wired 0 interface gets stranded, and Rx packets are not processed
CSCwp20530	Controller does not forward downstream packets to the wireless client after switchover
CSCwp21518	Cisco Catalyst Wireless 9164I and Cisco Catalyst IW9167IH APs experiences radio firmware kernel unresponsiveness
CSCwp27215	Cisco Catalyst 9124 AP in Mesh mode encounters poor iperf traffic performance
CSCwp32113	Controller reloads due to kernel unresponsiveness with segmentation fault (11) in process IGMPSN
CSCwp61179	Cisco Catalyst 9130 AP fails in port authentication with ClearPass Server
CSCwp65769	Wave 2 APs performing with fast transition with 802.1X authentication send incorrect M2 message during re-key on session timeout
CSCwn55495	Cisco Catalyst 9800-40 controller displays random CPU spikes on EZMAN
CSCwo86312	Controller shows a mismatch between client count from show client commands and SNMP walk total
CSCwo92511	Controller has inconsistent default MTU settings for mobility tunnels

Identifier	Headline
CSCwp07279	Controller unexpectedly reloads due to local software fatal error
CSCwp39409	Controller reboots unexpectedly due to an assertion failure in WNCd process
CSCwp63176	Cisco IOx app channel is down due to a state mismatch between the IOx and CAF apps on the Cisco Catalyst 9136 AP
CSCwp93598	Memory leak found in the controller process related to handling a specific database string

Open Issues for Cisco IOS XE 17.15.3

Identifier	Headline
CSCwn11160	Controller running in High Availability in guest anchor sends traffic to the wrong tunnel after switchover for already connected clients
CSCwn18885	Cisco Catalyst 9136 series APs encounter kernel unresponsiveness with last reload reason 'unknown'
CSCwn36778	Cisco Catalyst 9800-80 controller displays low memory leak potentially in the 'ipv4_addr' field
CSCwn83970	Cisco Catalyst 9162 AP does not respond to probe and open auth request on 5GHz
CSCwn90360	Controller does not start EAP process due to the packet transmission delay from AP
CSCwn90855	Controller overrides client's IP address in the device tracking database causing packet loss
CSCwn94597	Cisco Catalyst 9136 AP displays client stale entry due to delete reason NACK_IFID_EXISTS
CSCwo03840	Multiple AP modes encounter CAPWAPd crash while changing from dualstack to IPv6
CSCwo08534	Cisco Catalyst 9120 AP encounters kernel unresponsiveness due to: Radio firmware beacon TX stuck
CSCwk53741	Anchor controller drops mobility tunnel even when keepalive timers aren't hit
CSCwn31021	Controller fails to represent the correct format of AP Name and VLAN ID in option 82
CSCwn73024	Cisco Catalyst 9130AX AP fails PKCS certificate enrollment to support special characters on WGB
CSCwn76129	Controller fails to handle loadbalance discovery message resulting in stale AP entries
CSCwn79857	URL with multiple IPs do not work in FlexConnect Local Switching

Identifier	Headline
CSCwn83397	Wired Mesh AP client flaps between VLAN 0 and numbered native VLAN on Root AP
CSCwo04476	Cisco Catalyst 9130AX AP encounters kernel unresponsiveness
CSCwo05017	Cisco Catalyst 9162 AP encounters OOM reset due to Unbounded/tmp
CSCwo15057	Cisco Catalyst 9120 AP encounters kernel unresponsiveness
CSCwo16038	Cisco Catalyst 9124 AP's WGB becomes unreachable after connecting to a Cisco Aironet 2800 Root AP when WMM is disabled
CSCwo19025	Cisco Catalyst 9166D AP reports high channel utilization
CSCwo20395	Controller's rogue classification rules do not apply configured classifications
CSCwo29017	Controller encounters kernel unresponsiveness after issuing command 'show ap config slots'
CSCwo30925	Cisco Wi-Fi 6 and above APs do not support disabling WMM on radios that support 802.11n/11ac/11ax operation
CSCwo31854	RA Trace / Always-on traces do not generate past logs when collected over several hours
CSCwo32255	Anchor controller's AVC statistics show in the controller's CLI but not in the Web UI
CSCwo37680	Controller initiates client deletion with code: CO_CLIENT_DELETE_REASON_DOT11_MAX_STA
CSCwo37756	Cisco Aironet 1815t AP does not receive an internal DHCP IP address when connected to LAN3

Open Issues for Cisco IOS XE 17.15.2b

Identifier	Headline
CSCwm57815	The RF group name is empty after assigning AI-RF profile to sites
CSCwn85632	Client disconnects when switching from standalone mode to connected mode in FlexConnect

Open Issues for Cisco IOS XE 17.15.2

Identifier	Headline
CSCwm99449	Kernel panic is observed in CW9176 and CW9178 APs at pc: stile_mpe_conv_set_signatures+0xb8/0x720 [ntdp]
CSCwm95758	Kernel panic is observed in CW9176 at pc: dp_tx_mon_process_tlv_2_0+0xb18/0x18d0

Identifier	Headline
CSCwn27951	Cisco Catalyst 9105W AP: RLAN fast switching breaks DHCP for non-native VLAN wireless
CSCwj16930	Cisco Catalyst 9800-M controller does not connect the 25G port to the Nexus 9K Switch
CSCwj80614	Clients are unable to connect due to assignment of IP address that is in use by stale client entry in device-tracking database in FlexConnect local switching
CSCwk26966	Cisco Aironet 3802 AP displays false radar detection only on UNI-II after upgrading the software
CSCwk55656	AP shadow record support in standby
CSCwk58326	Controller sends multicast packets with previous WMI
CSCwk64840	Controller unexpectedly reboots due to memory depletion due to mobilityd process
CSCwk79990	Controller encounters kernel unresponsiveness due to IntelResetRequest
CSCwk81946	Controller experiences kernel unresponsiveness due to tdl memory corruption
CSCwm58430	Cisco Catalyst 9115 AP experiences kernel unresposiveness due to: Beacon Stuck Reset Radio
CSCwm86679	Cisco Catalyst 9800-40 controllers encounter kernel unresponsiveness and reboot unexpectedly at rogue_start_containers
CSCwm97615	Cisco Aironet 1562 MAP does not form mesh with Cisco Catalyst 9124 RAP running 17.9
CSCwm99135	802.11ax client faces latency in AP.
CSCwn03468	Clients encounter slow speeds while connecting to slot 2 operating in the 5-GHz band on CM66
CSCwn10992	DTLS timeout because of improper client load balancing
CSCwn11160	Controller running in High Availability in guest anchor sends traffic to the wrong tunnel after switchover for already connected clients
CSCwk53741	Anchor controller drops mobility tunnel even when keepalive timers aren't hit
CSCwk78480	Controller's WNCd experiences kernel unresponsiveness due to SISF
CSCwm09484	Controller encounters kernel unresponsiveness for WNCd in SSL Code
CSCwm37410	Cisco Catalyst 9120 AP does not forward large packets when MTU=1500
CSCwm57534	Controller experiences kernel unresponsiveness due to Critical process WNCd fault
CSCwm73020	Controller relays unicast DHCP requests

Identifier	Headline
CSCwm74173	Cisco Catalyst 9500 experiences kernel unresponsiveness when loading the controller package to enable EWC
CSCwm80845	OEAP LAN Ports 2 and 3 become non-functional on RLAN Profile after the controller code is upgraded
CSCwm88338	Displaying Standby Chassis STANDBY HOT stopped when the default gateway is unreachable
CSCwm89379	Controller should permit duplicate IPv6 while IP Theft is disabled
CSCwm93080	IP address of the TACACS server disappears when the GUI timeout is changed
CSCwm95682	Controller does not use the latest APSP after failover, causing AP to download new image after rejoining
CSCwm97684	AP gets removed from the controller due to an intermittent SW kernel unresponsiveness on the CAPWAPd process
CSCwm98000	Cisco Catalyst 9105 AP displays Short Preamble "Allowed" but then rejects association with SP "Not Allowed"
CSCwn00375	Controller does not generate AP disjoin event message syslog after the AP is disconnected
CSCwn03574	Cisco Catalyst 9800-80 contoller reloads unexpectedly and experiences kernel unresponsiveness
CSCwn06317	Controller does not send RADIUS request for web admin user
CSCwn08464	Cisco Catalyst 9120 AP experiences kernel unresponsiveness due to ktime_get_update_offsets_now+0x6c/0xb8
CSCwn08479	Cisco Catalyst 9120 Wi_Fi 6 AP experiences kernel unresponsiveness due to wlc_bsscfg_find_by_target_bssid+0xb8/0xe0
CSCwn11697	Controller experiences unexpected kernel unresponsiveness while client association with key-wrap is enabled
CSCwn12549	Controller unexpectedly reloads with CPUHOGS writing /tmp/rp/tdldb/0/NMSPD_DB on NMSPd process

Open Issues for Cisco IOS XE 17.15.1

Identifier	Headline
CSCwn17412	The FlexConnect local switching traffic is centralized randomly during a web-auth SSID.
CSCwh63050	Controller sends IGMP queries without IP address and MAC address on Cisco IOS XE Cupertino 17.9.3

Identifier	Headline
CSCwi04855	APs repeatedly join and disjoin controller with traceback
CSCwj39057	Cisco Catalyst 9130 AP experiences traffic loss and delays due to perceived channel utilization and interference
CSCwj42305	Client is unable to connect due to delete reason NACK_IFID_EXISTS
CSCwj80614	Clients are unable to connect due to assignment of IP address that is in use by stale client entry in device-tracking database in FlexConnect local switching
CSCwj83526	APs become non-operational when connected to Cisco Catalyst 9300 Switch via mGig port
CSCwj85091	Controller unexpectedly reloads while running the **show wireless client mac-address detail** command
CSCwj89538	Cisco Aironet 2802 AP fails to send reassociation response or association request
CSCwj93876	Controller unexpectedly reloads with reason "Critical process wncmgrd fault on rp_0_0 (rc=134)"
CSCwk03445	AP experiences slowness on 5-GHz and 6-GHz band
CSCwk05809	%EVENTLIB-3-CPUHOG message observed on Cisco IOS XE 17.12
CSCwk14917	Controller reloads unexpectedly
CSCwk17102	Client experiences unexpected disconnect due to missing M1 packet
CSCwk17667	Controller reboots due to high ODM memory consumption
CSCwk32111	Controller shows "-1 day" logs when registering with AirGap SLUP
CSCwk37983	Client VLAN is retained after changing SSIDs if \"vlan-persistent\" is enabled
CSCwk39866	Client page is stuck in loading state
CSCwk46105	Controller experiences unexpected reloads with high WNCd memory
CSCwk48338	Cisco Catalyst 9130 does not accept clients on the 5 GHz band
CSCwk48634	FlexConnect local switching dropping upstream broadcast ARP from Android devices in data path in Cisco Catalyst 9130 AP
CSCwk52996	Cisco Catalyst 9120 AP unexpectedly reloads along with radio abnormalities on wlc_bmac_suspend_mac
CSCwk54291	Controller voice CAC BW is not cleared
CSCwk58326	Controller sends multicast packets with previous WMI
CSCwk61068	Controller unexpectedly reloads on 17.9.4 with reason "critical process WNCd fault"
CSCwk61854	Configuration update failure when AP is in delete pending state

Identifier	Headline
CSCwk62836	Cisco Catalyst 9120 AP running on Cisco IOS XE Cupertino 17.9.5 drops downstream ARP reply
CSCwk64235	URL filter inconsistency observed post modification
CSCwk66988	Cisco Catalyst 9130 experiences radio failure
CSCwi85439	Cisco IW916x WGB: association is 802.11n, but the uplink statistics counts all Tx packets as MCS9
CSCwi72935	Cisco IW916x WGB: configure beacon miss-count 1000, roaming is never triggered

Resolved Issues for Cisco IOS XE 17.15.4

Identifier	Headline
CSCwn18885	Cisco Catalyst 9136 series APs encounter kernel unresponsiveness with last reload reason 'unknown'
CSCwo98644	RRM does not update the default channel when using IPv6 only on the controller
CSCwp06711	Static AP Location is overwritten as per Location Tag Configuration on WLC
CSCwn77030	Controller does not process analytics action frames received from MLD for MLO clients
CSCvy53719	Cisco Catalyst 9800-80 controller displays stale, non-impacting "mce: [Hardware Error]" messages during IOS-XE 17.x boot-up
CSCwp59171	Users unable to add allowed user on Lobby admin page
CSCwo89539	Controller reload unexpectedly when adding "location civic-location-id" to multiple interfaces
CSCwn45380	Controller uses registry to initialize the trap queue length in SNMP
CSCwo21938	AFC is using manual geolocation co-ordinates
CSCwo95396	Cisco Catalyst 9800 CL and 9800L controllers reload while provisioning the controller from Cisco Catalyst Center
CSCwn99763	Noise floor value is always displayed as 0 for a few x-paths
CSCwo00821	IoT Orchestrator is unable to start after an upgrade or a reload
CSCwo52310	Wireless cloud service consumes 100% CPU due to geolocation derivation
CSCwp31397	Controller DFS Radar Detection results in most of the APs allocated to the same channel
CSCwo62157	Controller with CAPWAP enabled display memory leak in tdl_mac_addr object

Identifier	Headline
CSCwo68664	Cisco Catalyst 9800-L controller in Software-Defined Access (SDA) Wireless does not enforce the Extensible Authentication Protocol (EAP) timeout
CSCwn39428	Error message "Flow Monitor is Required" is shown even when flow monitor name is available
CSCwp21187	Controller unexpectedly reboots due to due to mDNS packet
CSCwo29017	wncmgrd kernel unresponsiveness after issue command \u2018show ap config slots\u2019
CSCwo67294	Controller unexpectedly reloads due to a corrupted value in IGMP Layer 2 Snooping process
CSCwn92827	Secondary controller fails with rsync error
CSCwn93586	Cisco Catalyst 9176 AP operates in XOR mode, Channel and CW changes are not pushed post the DCA cycle
CSCwo15982	Controller unexpectedly reboots with 17.15.3.14 image
CSCwo54553	Controller displays traceback messages when default-policy-tag APs block initiates a configuration change for other APs due to Ref-count not zero
CSCwj80614	Clients are unable to connect due to assignment of IP address that is in use by stale client entry in device-tracking database in FlexConnect local switching
CSCwp16968	1562 WGB FT Roaming client disconnection issue due to MAC record Mismatch
CSCwo07767	Controller's active chassis get stuck in active recovery state on 17.12.4
CSCwn92477	Controller unexpectedly reboots during WNCd process due to assertion failure with invalid BSSID
CSCwo62333	Cisco Catalyst 9800-L controller in FlexConnect/Software Defined Access (SDA) fails to start MAB on association request
CSCwn90855	Controller overrides client's IP address in the device tracking database causing packet loss
CSCwn94511	The factory-reset all command is unsecure but functions as if it has a secure option
CSCwo97886	Controller displays out of order packet issue with fragmented packet when Auto QoS is enabled
CSCwo35645	NETCONF over SSH fails to return all the records for wireless-client-oper and shows 'invalid XML' before everything is returned
CSCwo67413	Controller pushes aWIPS profiles from FQDN-only setup for intrusion detection
CSCwp12959	wireless client gets excluded with one authentication failure or never gets excluded

Identifier	Headline
CSCwn11160	Controller running in High Availability in guest anchor sends traffic to the wrong tunnel after switchover for already connected clients
CSCwo37680	Controller initiates client deletion with code: CO_CLIENT_DELETE_REASON_DOT11_MAX_STA
CSCwn96363	Remove redundant counters from "show wireless stats ap name &lt;ap-name&gt; dot11 5GHz" output
CSCwo70030	Rogue processing is performed by WNCd even though the "bssid-neighbor-stats" configuration is disabled
CSCwm48458	Detecting radar on 5-GHz CH100 causes controller to mismatch to CM66 and switch dual mode from 6-GHz to 5-GHz
CSCwn31021	Controller fails to represent the correct format of AP Name and VLAN ID in option 82
CSCwo19011	Controller observes unexpected SISF reboot with WNCD core
CSCwo30925	Cisco Wi-Fi 6 and above APs do not support disabling WMM on radios that support 802.11n/11ac/11ax operation
CSCwp25552	BSSID-mac dispatched as 00:00:00:00:00:00 for slot 1 WLAN 1
CSCwn33501	Controller connected to the AP does not give any output while executing the show ap summary sort name command
CSCwp03988	Unexpected Reload Due to Unsuccessful copy of the MAC address
CSCwo20395	Controller's rogue classification rules do not apply configured classifications
CSCwo53638	Client error: High-availability data path setup failed on standby device in RA trace
CSCwo61286	Audit session ID changes after inter-WNCd roam on Central Web Authentication (CWA) with PSK
CSCwn94159	Controller with 6 GHz support AP's radio channel bandwidth changes due to DCA happening frequently
CSCwn36778	Cisco Catalyst 9800-80 controller displays low memory leak potentially in the 'ipv4_addr' field
CSCwp26707	Controller fails to start L2 authentication for 802.11r clients with vlan-persitent configured in 17.12.5
CSCwp86129	Client connected to local mac-auth PSK or MPSK SSIDs get disconnected and do not remain connected to the controller
CSCwo98083	Access points are unreachable in inventory on Cisco Connected Cloud version 2.3.7.9
CSCwo64967	Mobility tunnel with data-link encryption intermittently disconnects when the fourth octet of the WMI address is 255

Identifier	Headline
CSCwp13687	Cisco Catalyst 9800-CL controller modifies the script generating SSC to avoid issues with RSA key generation impacting AP join
CSCwo41248	Controller display wrong message when configuring 2 radios on the same UNII band (100 - 144)
CSCwo80904	Cisco Catalyst 9164 and 9166 APs encounter kernel unresponsiveness due to radio failures (Beacon Stuck)
CSCwo33572	Failed to collect RA tracing logs on Cisco IOS XE Release 17.9.5
CSCwk48338	Cisco Catalyst 9130AX AP does not accept clients on the 5 GHz radio
CSCwk79057	AP does not failover to the RADIUS server in FlexConnect Local Switching Local Authentication
CSCwn88092	Unable to view the events for wireless clients in the Client 360 section of the Event Viewer
CSCwn96529	Cisco Catalyst 9136I-ROW AP in Site-Survey mode cannot add country code "IN"
CSCwo38789	Cisco Catalyst 9176 AP encounters watchdog reset (WCPD) kernel unresponsiveness due to memory leak in RRM module
CSCwo48539	Cisco Catalyst 9124 MAP powered with 30W and joined to a Cisco Catalyst 9124 EWC RAP can enable Tri-Radio with the EWC GUI
CSCwo60793	IOX app channel down as IOX app and CAF app state are mismatched
CSCwo61838	Cisco Catalyst 9120 / 17.12.4 ESW13 encounters kernel unresponsiveness due to OOM process gRPC
CSCwo68312	Cisco Catalyst 9124AXE-E APs identifies antennas wrongly CSCwo76564
CSCwo76564	Cisco Catalyst 9130, 9136 and 9166 APs display memory leak in ble_transport
CSCwp07242	Cisco Catalyst 9105 AP stops acking frames due to rxstuck
CSCwp17376	Cisco Catalyst 9130AXI-C AP's slot 1 does not announce HE capabilities
CSCwp34935	Cisco Wireless 9176 AP Site Survey mode radio down with country code other than US
CSCwn55534	IP theft is observed on the controller when the client receives a second DHCP offer following DORA
CSCwn73024	Cisco Catalyst 9130AX AP fails PKCS certificate enrollment to support special characters on WGB
CSCwn83397	Wired Mesh AP (MAP) client flaps between VLAN 0 and numbered native VLAN on Root AP (RAP)

Identifier	Headline
CSCwn88567	Cisco Aironet 1815i AP does not display correct syslog timestamps
CSCwn92047	Cisco Catalyst 9105 Access Point controller fails to start after reboot when internal AP is configured as 802.1X supplicant
CSCwn99070	Radio core fails to generate properly causing operational issues
CSCwo05017	Cisco Catalyst 9162 Access Point experiences out-of-memory reset due to unbounded /tmp usage causing system instability
CSCwo14129	Wave 2 APs experience unresponsiveness due to soft lockup in version 17.12.4 causing system instability
CSCwo16038	Cisco Catalyst 9124 AP workgroup Bridge becomes unreachable connecting to Cisco 2800 Root Access Point when Wi-Fi Multimedia (WMM) is disabled
CSCwo34769	Access point in FlexConnect mode does not advertise RSNxE in probe response frames
CSCwo37756	Cisco Aironet 1815 AP does not receive an internal DHCP IP address when connected to LAN3
CSCwo43801	AP duplicates DHCP request packets when using FlexConnect mode with Central Switching WLAN
CSCwo46493	Cisco Catalyst 9136 AP dual ethernet failover reboots
CSCwo53891	AP reboots with incorrect reason 'Controller Last Sent: Channel0 Detected'
CSCwo72236	AP prints logs every 30 seconds : \"RTNETLINK answers: No such file or directory\"
CSCwo74316	NTP synchronization failure for AP occurs when the controller is NTP server
CSCwo75325	SST:17.12.6: Crash due to radio failures (Beacon Stuck) seen on 1832 or 1852 APs
CSCwo75806	Reassociation Response from AP is delayed for over 200ms on AP WCP component intermittently
CSCwo75908	MTU value of some APs are not 1600 byte
CSCwo82821	Cisco Catalyst 9120 Series APs experience kernel panic at txq_hw_fill+0x394
CSCwo89749	Cisco Catalyst 9105 Series APs reboot due to kernel panic
CSCwo94810	Cisco Wireless 916x Series, 9130 Series, and 917x Series APs reject association from IoT client TI module
CSCwp20425	Roaming failure in FlexConnect mode with WPA3-SAE and OKC enabled
CSCwo14012	AP with filter as tag source remains correctly configured after 2.4 GHz RF profile deletion

Resolved Issues for Cisco IOS XE 17.15.3

Caveat ID	Description
CSCwm89597	High CPU utilization due to SAEvLogShowLogIn
CSCwj30587	Memory leak observed in wncd_x caused by CAPWAP messaging
CSCwm42613	Wireless clients are unable to join due to high memory usage - AAA_CHUNK_ATTR_SUBLIST
CSCwn27877	Cisco Catalyst 9105 Series APs stop responding to clients on 5-GHz [CS00012380774]
CSCwn45670	Controller GUI FlexConnect configuration page fails after upgrade to Cisco IOS XE 17.15.1
CSCwn61711	Cisco Catalyst 912X AP: PSM microcode watchdog fired [CS00012386346]
CSCwn17412	FlexConnect local switching traffic gets randomly centralized on a WebAuth SSID
CSCwn92652	Radio ucode crash seen in Cisco Catalyst 9105 APs in monitor mode [CS00012389487]
CSCwj84377	Client detail for 'Associated' Client does not display some info element when using Cisco Spaces with Connector
CSCwk09142	Cisco Catalyst 9136 AP radio unresponsive due to radio firmware failure
CSCwk26966	Cisco Aironet 3802 AP displays false radar detection only on UNI-II after upgrading the software
CSCwk58326	Controller sends multicast packets with previous WMI
CSCwk64840	Controller unexpectedly reboots due to memory depletion due to mobilityd process
CSCwk81946	Controller experiences kernel unresponsiveness due to tdl memory corruption
CSCwm48283	Controller is stuck in internal-error state after upgrade to HP5
CSCwm58430	Cisco Catalyst 9115 AP experiences kernel unresposiveness due to: Beacon Stuck Reset Radio
CSCwm67254	RadSec messages are missing CUI attributes
CSCwm73020	Controller relays unicast DHCP requests
CSCwm79348	AP remains stuck in the activate state without progressing to RUN when IOX-APP starts before USB detection
CSCwm86679	Cisco Catalyst 9800-40 controllers encounter kernel unresponsiveness and reboot unexpectedly at rogue_start_container
CSCwn03468	Clients encounter slow speeds while connecting to slot 2 operating in the 5-GHz band on CM66
CSCwn09549	Cisco Catalyst 9124 AP unable to join and intermittently disconnects with Cisco Catalyst 9124 AP

Caveat ID	Description
CSCwn10606	Cisco Catalyst 9120 Wi_Fi 6 AP fails to report RFID packets to the controller
CSCwn10992	DTLS timeout because of improper client load balancing
CSCwn15048	Controller does not filter out the expansion module SN field before sending it to DNAC, causing the collection to fail
CSCwn26561	RFID measurement is missing during RFID statistics collection window
CSCwn26989	Cisco Catalyst 9178 AP experiences radio1 unresponsiveness
CSCwn27951	Cisco Catalyst 9105W AP: RLAN fast switching breaks DHCP for non-native VLAN wireless
CSCwn36115	iPhone 16 device is listed as unclassified in iOS 18.0.1
CSCwn44019	Cisco Catalyst 9172I AP encounters kernel unresponsiveness during 200 client scale test
CSCwn44287	APs running on Cisco Catalyst 9300 Series switches FiaB generate CAPWAP crash files
CSCwn50926	Acct-Session-ID attribute is missing from access request after client deletion
CSCwn52205	AP IOX wait for time it takes for AP to detect and add USB device entry before starting IOX APP
CSCwn61980	Rogues detected on inactive bands by dual-band radio APs fail to display properly on the UI
CSCwn66225	Invalid Tx power on beacon frame causes iPhone clients to disconnect
CSCwn76273	Cisco Catalyst 9172I AP running on Cisco IOS XE 17.15.2.201 experiences radio1 unresponsiveness
CSCwn76347	Cisco Catalyst 9172H AP experiences unresponsivness "crash ar_wal_mlo_ipc.c:2047"
CSCwn81268	IOX AP in RUN state ends up in activate state after switch reload
CSCwn82037	Cisco Catalyst 9120 AP does not report RFID packets to controller intermittently
CSCwn83869	AP sleep count timer value stuck in 80 while configuring speed after the radar event in MFG
CSCwn87525	917X APs -Wi-Fi 7 MLO clients drop traffic due to 5-GHz channel change during CAC
CSCwn89252	APs running IOS XE 17.15.2 unable to install Solum IOX APP
CSCwn90874	Guest anchor controller shows error message when creating anchor-export-ACK
CSCwn98574	Corrupt VRF name causes client to frequent disconnects and get stuck at mobility while roamining

Caveat ID	Description
CSCwo02178	FT-SAE clients fails to roam between controller in same mobility group due to PMKID mismatch
CSCwo03789	Cisco Catalyst 9176 AP unrepsonsive due to kernel panic when resetting radio umac_reset_rx_event_handler
CSCwo03804	Cisco Catalyst 9176 AP broadcasts slot 2 6-GHz BSSIDs with 6M data rate
CSCwo08256	Cisco Catalyst 9176 AP sends probes responses with retry bit set in IOS XE 17.15.2
CSCwo08289	Cisco Catalyst 9166 AP does not accept clients due to channel mismatch between the driver and wcpd
CSCwo26102	Cisco Aironet 1800i AP shows wrong compile time after joining latest controller version
CSCwi48178	WNCd error in SafeC Validation for memcmp_s: dmax is 0
CSCwj53257	APs detected for the first time set timer to 3600 seconds instead of 1800 seconds
CSCwj72174	Cisco Aironet 2800 Series AP connected to same controller is detected as rogue by other connected APs
CSCwk33513	WGB takes time to roam for Cisco Catalyst 9120, 9105 AP
CSCwk70598	Event-Driven RRM is unresponsive on 6-GHz band
CSCwk76786	AP radio service is down after DFS is set to CH100 and automatically changes to sniffer mode on CH100 and then back to client serving
CSCwm37410	Cisco Catalyst 9120 AP does not forward large packets when MTU=1500
CSCwm56315	Cisco Aironet 2800, 3800, 4800 AP: STA-ID list mismatch with radio rriver client summary after veriwave roaming test
CSCwm60850	DFS L1 test fails to run due to sleep_count while configuring width and channel on CM66
CSCwm66425	BLE operations with RadioActive trace enabled encounters kernel unresponsiveness
CSCwm72142	Cisco Catalyst 9136 AP's tmp directory is exhausted
CSCwm78841	Over the Air (OTA) packet does not display increment in AP after setting truncate value to 25bytes and enabling OTA
CSCwm84898	Cisco Catalyst 9178 AP encounters kernel unresponsiveness at wlan_vdev_mlme_clear_mlo_vdev
CSCwm88275	Cisco Catalyst 9166 AP experiences ble_transport core dumps with message: E1015..28434 call.cc:1740] assertion failed: grpc_cq_begin_op(cq_, notify_tag)
CSCwm91684	DNAC SSID monitor does not work for ICAP RF-Stats
CSCwm92779	DNAC Wireless Client Assurance Dashboard displays no data for "Avg Latency"

Caveat ID	Description
CSCwm92836	Request ID mismatch observed at max connections for AP Tx profile configuration
CSCwn00375	Controller does not generate AP disjoin event message syslog after the AP is disconnected
CSCwn08479	Cisco Catalyst 9120 Wave 2 APs encounter kernel unresponsiveness at wlc_bsscfg_find_by_target_bssid+0xb8/0xe0 CS00012376904
CSCwn02863	FlexConnect Wi-Fi 7 AP does not send association responses for unsupported securities
CSCwn14495	Cisco Catalyst 91XX AP detects its own BSSID as rogue
CSCwn15002	Cisco Catalyst 9120 AP encounters kernel unresponsiveness at wlc_low_txq_enq
CSCwn19804	Cisco Aironet 1562D AP doesn't deploy in indoor mode
CSCwn29991	Firmware assert observed at "ar_wal_mlo_ipc.c:2033" while running overnight Longevity with MLO/non-MLO clients
CSCwn43094	RLAN clients do not show up in the controller's client table after a CAPWAP drop/join
CSCwn48978	AP incorrectly send ARP requests for the DHCP IP address even after a DHCP release packet
CSCwn77377	IP addresses cannot be retrieved from the status file when the DHCP options on lease are available
CSCwn84552	Cisco Catalyst 9105 APs get stuck in a code download loop while upgrading or downgrading
CSCwn85035	Cisco Catalyst 9172I AP encounters radio 0/1 kernel unresponsiveness during longevity test
CSCwn85374	Controller displays memory usage increasing in the cloudm process
CSCwn91239	FlexConnect WiFi7 AP does not send association responses for unsupported securities

Resolved Issues for Cisco IOS XE 17.15.2b

Identifier	Headline
CSCwj84377	Client detail for 'Associated' Client does not display some info element when using Cisco Spaces with Connector
CSCwk58326	Controller sends multicast packets with previous WMI
CSCwm86679	Cisco Catalyst 9800-40 controllers encounter kernel unresponsiveness and reboot unexpectedly at rogue_start_containers
CSCwn44019	Cisco Catalyst 9172i AP encounters kernel unresponsiveness during 200 client scale test
CSCwk94110	NMSP config related timers are not initialised post process restart

Identifier	Headline
CSCwn14242	The "show ap geolocation ranging request " command displays incorrect output related ranging data post controller SSO

Resolved Issues for Cisco IOS XE 17.15.2

Identifier	Headline
CSCwm12544	Controller unexpectedly reloads with cpp-ucode exception due to a rbuf out-of-handle
CSCwi04855	APs repeatedly join and disjoin controller with traceback
CSCwi78109	Controller GUI displays error messages: %CLI_AGENT-1-NVGEN_ERR while processing NVGEN command
CSCwj39057	Cisco Catalyst 9130 AP experiences traffic loss and delays due to perceived channel utilization and interference
CSCwj85091	Controller unexpectedly stops working while running the show wireless client mac-address detail command
CSCwj88071	Controller sends an invalid XML character (Unicode: 0x4) found in RPC response for ap-model
CSCwj93876	Controller unexpectedly reloads with reason "Critical process wncmgrd fault on rp_0_0 (rc=134)"
CSCwk05809	%EVENTLIB-3-CPUHOG message observed on Cisco IOS XE 17.12
CSCwk12169	Cisco Catalyst 9105/9115/9120 AP fails for clients connected in 5G slot
CSCwk17102	Client experiences unexpected disconnect due to missing M1 packet
CSCwk24352	Wireless clients are unable to receive the splash page and gets stuck due to webauth requirement
CSCwk37983	Client VLAN is retained after changing SSIDs if \"vlan-persistent\" is enabled
CSCwk39263	Cisco Catalyst 9115 and 9120 APs loses its port 802.1X configuration on upgrade
CSCwk39866	Client page is stuck in loading state
CSCwk52996	Cisco Catalyst 9120 AP unexpectedly reloads along with radio abnormalities on wlc_bmac_suspend_mac
CSCwk54291	Controller voice CAC BW is not cleared
CSCwk63163	Controller does not respond to CoA
CSCwk70277	FRA sets slot 2 to 6 GHz in Cisco Catalyst 9166 AP even when 6-GHz network is disabled
CSCwk76746	Controller stops responding constantly when running specific UDN related commands

Identifier	Headline
CSCwk82371	Cisco Catalyst 9120AXI-S AP does not detect the RFIDs in Monitor mode
CSCwk84121	Local switching clients are assigned to Zone ID 0 when IP overlap is configured and FlexConnect VLAN central switching
CSCwk97948	Controller ends abnormally during an ISSU upgrade from Cisco IOS XE 17.3 to 17.12
CSCwk98117	Cisco Catalyst 9166D APs are unable to transmit NDP packets over the air
CSCwm03016	Controller experiences kernel unresponsiveness abnormally pointing to client_orch
CSCwm07499	Cisco Catalyst 91xx AP does not rotate awipsd.log causing an upgrade issue "tar: write error: No space left on device"
CSCwm08044	APs do not upgrade without a power cycle displaying error: unlzma: write: No space left on device
CSCwm09148	EWC rogue syslogs are missing
CSCwm29051	Controller experiences kernel unresponsiveness two times due to Critical process WNCd fault on rp_0_0 (rc=139)
CSCwm29437	Controller reboots handling AP radio payloads due to Critical process wncd fault on rp_0_0 (rc=139)
CSCwm30964	EWC does not start on RAP after factory reset
CSCwm31864	Cisco Wave APs experience kernel unresponsiveness due to memory leak reason OOM
CSCwm36607	Controller displays fman_rp memory leak in FMAN_RP_DB at /tmp/rp/tdldb
CSCwm40646	Clients stuck in IP learning state as DHCP option 82 field is left empty with EoGRE tunnel enabled
CSCwm49453	Controller upgrading to 17.9.5 removes the NAS Port-ID in Access-Request
CSCwm49467	FlexConnect APs disable u-APSD in the assoc request if clients don't have it enabled
CSCwm52551	Cisco Catalyst 9124 AP in FlexConnect mode with the FlexConnect EoGRE tunnel enabled leaves the Option 82 field unfilled
CSCwm66129	Cisco Wave 2 APs 2800, 3800, and 4800 display duplicate entries for stale clients in the Wi-Fi driver
CSCwm67710	Cisco Catalyst 9800-80 controller encounters critical process WNCd failure (rc 0)
CSCwm74071	Controller encounters kernel unresponsiveness due to client being stuck in 802.11r preauth and BSSID/AP going down at the same time
CSCwn06627	Controller encounters kernel unresponsiveness with geolocation config pointing towards geo_cloudm_graph_shortest_path
CSCwi83037	Cisco Aironet 4800 AP: Radio Core data files generated Radio 1 during longevity testing

Identifier	Headline
CSCwj03060	Cisco Aironet 1815w AP encounters kernel unresponsiveness on image version 17.9.4.205
CSCwj66264	Cisco Catalyst 9300 and 9400 switches' mGig port displays half-duplex mismatch messages
CSCwj69312	Loadbalancer feature does not work when AP sends negative SNR value
CSCwj69642	Cisco Catalyst 9166 APs stop forwarding traffic for some seconds.
CSCwj82407	Controller's Web UI enhancement shows login banner while using TACACS/RADIUS
CSCwj85339	Controller displays no effect on disabling DCA Aggressive on startup
CSCwk11417	ewlc_cert_mgr, SafeC Validation: strncpy_s: does not have enough space after assigning new WebAdmin cert
CSCwk52242	Clients using Cisco IW3702 AP in FlexConnect mode cannot obtain IP addresses while behind third-party WGB
CSCwk52366	Controller encounters fix flow control display issue
CSCwk59342	Controller using channels 1, 5, 6, 9, 11, and 13 on 2.4GHz RF profiles causes discrepancies
CSCwk66729	FlexConnect AP with Client QoS policy changes WLAN-VLAN mapping without manual configuration change
CSCwk70785	AP does not update the MTU value for PMTU probe causing disconnection
CSCwk74269	SNMP query with bsnAPIfTable OID fails for Cisco Catalyst 9166D APs
CSCwk74699	Controller GUI does not change AP tags displaying "System Busy! Please retry after sometime"
CSCwk77222	Cisco Aironet 2802 AP encounters kernel unresponsiveness after upgrading to 17.9.5.47
CSCwk77766	Cisco Catalyst 9800-80 encounters kernel unresponsiveness due to incorrect delete reason code in the AP delete mobile payload
CSCwk77862	AP does not disjoin automatically when the AP-name is changed in the Regex filter
CSCwk80486	APs mark own BSSID as rogue in 2.4 GHz and in 5 GHz
CSCwk85707	SSH access remains unrestricted for EWC-capable APs connecting to the Cisco Embedded Wireless Controller
CSCwk93880	Cisco IW-6300H-AC-E-K9 APs encounter kernel unresponsiveness due to FIQ/NMI reset
CSCwm00078	Cisco Catalyst 9136 AP sends M5 with incorrect index 0, resulting in Apple Macbooks not responding

Identifier	Headline
CSCwm04379	Cisco Catalyst 9115AX displays BcmRadioStats error : Failed to add multicast MAC address for RRM as dot11_client entry
CSCwm08261	Controller RADSEC fix using a Samsung device displays wrong Acct-Terminate-Code when manually disabling Wi-Fi
CSCwm14401	Controller experiences an unexpected reset of WNCd
CSCwm28542	OKC roam fails after a brief WAN drop
CSCwm34600	AAA override VLAN does not apply upon roaming in FlexConnect local authentication
CSCwm36501	Controller encounters kernel unresponsiveness due to TLB miss
CSCwm49168	Cisco Catalyst 9164I-ROW AP VAP driver drops EAP identity requests packet intermittently
CSCwm50811	AP displays BSSID as rogue intermittently, causing the control packet to be considered for impersonation detection
CSCwm52604	Controller experiences unexpected reload while parsing null password on '? password encryption aes?' command
CSCwm56700	Controller does not answer to A/AAAA queries for wired devices (mDNS gateway)
CSCwm56949	Removing 'tls match-server-identity hostname <URL>' doesn't work
CSCwm61128	AAA override VLAN is not used for FT 11R roam-in local authentication
CSCwm65107	Cisco Catalyst 9130 AP encounters kernel unresponsiveness due to OOM
CSCwm73271	Cisco Wave 2 AP does not send syslog messages if the receiver is using an IPv6 address
CSCwm80472	Controller's UI and CLI fail to delete a mobility peer due to 'invalid transversal ctx for walker next rec'
CSCwn04950	Cisco Embedded Wireless Controller in the Site Survey mode does not connect with the internal AP
CSCwn05795	Cisco Catalyst 9120AXI-I AP's 2.4-GHz band does not activate due to a 'Regulatory domain check failed' error
CSCwk26007	Controller RP undergoes unexpected reload while displaying OPSSL Handshake Errors
CSCwk81268	IPv6 buffer overrun encounters kernel unresponsiveness when client IPv6 address removal happens in a larger number
CSCwm08255	Controller RADSEC's accounting stop messages are missing when user disconnects from Wi-Fi
CSCwm42613	Clients are unable to join due to high memory usage: AAA_CHUNK_ATTR_SUBLIST
CSCwj97570	Controller running 17.9.4a code encounters kernel unresponsiveness when configuring "ip http server"

Identifier	Headline
CSCwk77301	Controller RADSEC's accounting does not stop while accounting starts including framed-IP
CSCwm04614	WNCd logs display a CPU hog during association request processing
CSCwm31586	AP in FlexConnect mode reports an erroneous client count

Resolved Issues for Cisco IOS XE 17.15.1

Identifier	Headline
CSCwi39486	During controller switchover, a client using static IP is assigned to the wrong VLAN
CSCwh56566	Controller experiences flow monitor failure due to manual flow record parameters
CSCwh80060	Cisco Wave 2 APs connected to the controller are losing the FlexConnect WLAN-VLAN mapping
CSCwh81071	Slot 2 is down for GB country after performing factory reset
CSCwi16509	APs do not join the controller with invalid radio slot ID error
CSCwi22895	Controller becomes unresponsive within Radio Resource Management (RRM) service due to ReloadReason=Critical process rrm fault
CSCwi27380	Media stream feature does not work
CSCwi28382	Controller reloads unexpectedly due to Keymgmt: Failed to eapol key m1 retransmit failure
CSCwi55714	Controller unexpectedly reboots when handling NMSP TLS connection
CSCwi56780	MAC Authentication Bypass (MAB) is not initiated unless the client device is deauthenticated
CSCwi69251	Cisco Catalyst 9800-40 Wireless Controller becomes unresponsive on Critical process Radio Resource Management (RRM) fault on rp_0_0
CSCwi75759	Cisco Catalyst 9800-40 Wireless Controller reloads due to critical process WNCd fault
CSCwi99276	Controller does not have Network Access Control (NAC) in the policy profile configuration enabled on Prime Infrastructure
CSCwj08367	Cisco Catalyst 9800 Wireless Controller encounters unresponsiveness generating system report, segmentation fault - Process = IGMPSN
CSCwj09698	Cisco Catalyst 9800 Wireless Controller encounters an unexpected reset in wncmgrd with a scaled setup while being managed by the Meraki Dashboard
CSCwj25187	Controller does not display the redundancy details on the Web-UI, only on the CLI

Identifier	Headline
CSCwj26196	Controller encounters an unexpected reset while trying to validate the MAC address with the EWLC_APP_INFRA_ID_MAGIC
CSCwj31356	Controller reboots due to Radio Resource Management (RRM) process fault on rp_0_0 (rc=139)
CSCwj36962	Controller reboots unexpectedly due to invalid QoS parameters
CSCwj42408	Controller posture flow does not work when PMF is optional
CSCwj34379	Cisco Catalyst 9800-80 Wireless Controller encounters WNCd issues when accessing Crimson Database
CSCwj79545	Controller unexpectedly reboots during WNCd process due to assertation failure with invalid BSSID
CSCwj86938	Memory leak in scale network with telemetry shared user events with Cisco Catalyst Center
CSCwj93153	Controller becomes unresponsive during WNCd process
CSCwk05030	Controller becomes unresponsive due to critical software exception
CSCwj40202	Controller does not send RADIUS accounting messages WLAN with PSK/MAB authentication
CSCwj60910	Controller and PI report observe RRM message mismatch
CSCwh88246	AP does not allow you to apply URL filter after invalid configuration
CSCwi01382	5-GHz and 2.4-GHz radios remain non-operational in an AP
CSCwj67158	Controller does not send mobile address to AP if the CoA is received when the user is in the ip_learn state
CSCwj72370	Controller uses incorrect username for "show platform" command when logging in GUI
CSCwi47294	Per client rate limit with FlexConnect AP is not functioning
CSCwi48980	Controller local password policy does not take effect on GUI login as expected
CSCwi50732	VLAN group support for DHCP and static IP clients feature does not work on FlexConnect Central Switching mode
CSCwi64010	Controller accepts the reserved IPv6 multicast address to be configured as a mobility multicast IPv6 address
CSCwi66582	Controller returns with error while uploading backup file with FTP on GUI
CSCwi69093	Controller GUI shows incorrect number of clients connected to the AP
CSCwj76892	Controller configures aggregation scheduler parameter incorrectly, causing low downlink speed

Identifier	Headline
CSCwi83124	Pop-ups are not displayed correctly in dark mode in the controller
CSCwj00465	Active controller becomes ActiveRecovery when the redundancy port link is down
CSCwj01446	Personal Identity Verification (PIV) authentication requires an additional backslash in the redirection URL to work successfully
CSCwj04177	AP undergoing Extensible Authentication Protocol (EAP) fails if the password is more than 31 characters
CSCwj15376	Cisco NMSP runs into security protocol issues
CSCwj25110	Controller reports incorrect values during SNMP polling
CSCwj77128	URL filter allows only letters as the first character
CSCwj33376	Incorrect selection of APs in load balancing
CSCwj94201	Controller experiences unresponsiveness CPUHOG
CSCwj68763	Enhanced URL is missing after FlexConnect AP CAPWAP flap
CSCwk35891	Controller experiences unresponsiveness after displaying "\clear ap geolocation derivation\" message
CSCwj42562	GUI does not display PC analytics statistics
CSCwk44459	Loadbalancer server holds incorrect AP IP address and stale entries
CSCwi44211	The "show run" command results are different from restore configuration
CSCwj29406	The "show ap summary sort descending client-count" command shows wrong client count
CSCwi29216	Unsupportive characters in the description field prevents re-sync
CSCwj83935	Controller shows tech X is empty when previous tech X term length stop didn't finish before SSH close
CSCwi70760	Controller encrypts ApDnaGlobalCfg token when the password encryption is configured using AES
CSCwj96620	Syntax errors observed in CISCO-LWAPP-DOT11-CLIENT-MIB
CSCwj96666	Syntax errors observed in CISCO-LWAPP-DOT11-MIB
CSCwj97107	Standby controller does not take active role after reloading the active controller with "reload slot" command
CSCwk02633	An RSA key pair is configured in the truspoint configuration when an EC keypair is selected when creating a trustpoint on the controller.
CSCwk25182	Controller throws password policy alert while logging in GUI using TACACS+ credentials after upgrading to Cisco IOS XE 17.14

Identifier	Headline
CSCwk28680	Controller unexpectedly reloads due to Cisco QuantumFlow Processor (QFP) ucode while updating the drop statistics
CSCwj33979	Output for the **show ap summary** command takes lengthy duration to complete
CSCwk67341	Cisco IW916x WGB: wcpd crash during 802.11v neighbor list updates after multiple roams
CSCwj26036	COS uWGB: Does not translate the client MAC address of Broadcast DHCP offer
CSCwk30230	Cisco IW9167: Clients cannot associate to APs in bridge mode (RAP) when the AP is on a fiber connection
CSCwk33139	Cisco IOS XE controller software encounters an arbitrary file upload vulnerability

Troubleshooting

For the most up-to-date, detailed troubleshooting information, see Troubleshooting TechNotes.

Related Documentation

- Information about Cisco IOS XE
- Cisco Validated Design documents
- MIB Locator to locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets

Cisco Wireless Controller

For more information about the Cisco wireless controller, lightweight APs, and mesh APs, see these documents:

- Cisco Wireless Solutions Software Compatibility Matrix
- Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide
- Cisco Catalyst 9800 Series Wireless Controller Command Reference
- Cisco Catalyst 9800 Series Configuration Best Practices
- In-Service Software Upgrade Matrix
- Upgrading Field Programmable Hardware Devices for Cisco Catalyst 9800 Series Wireless Controllers

The installation guide for your controller is available at:

- Hardware Installation Guides

All Cisco Wireless Controller software-related documentation

Cisco Catalyst 9800 Series and Cisco Catalyst CW9800 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 Catalyst CW9800H1 and CW9800H2 Wireless Controllers Data Sheet*
- *Cisco Catalyst CW9800M 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

Cloud Monitoring for Cisco Catalyst 9800 Hardware Wireless Controllers

Cloud Monitoring for Catalyst

Communications, services, and additional information

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

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a gateway to the Cisco bug-tracking system, which maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. The BST provides you with detailed defect information about your products and software.

Documentation feedback

To provide feedback about Cisco technical documentation, use the feedback form available in the right pane of every online document.