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

First Published: 2024-08-14

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 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.

Revision History

Modification Date	Modification Details
September 17th, 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".
September 26th, 2024	Updated: **Compatibility Matrix** section—Added version 3.3 to the **Cisco Identity Services Engine** information in the **Compatibility Information** table.

What's New in Cisco IOS XE 17.15.1

Table 1: 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.
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.

Feature Name	Description and Documentation Link
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.
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.

Feature Name	Description and Documentation Link
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
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.

Feature Name	Description and Documentation Link
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 2: 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, and 9800-CL). 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) 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

- System unresponsiveness and reloads are observed in Standby when image upgrades to Cisco IOS XE 17.15.1 in Cisco Catalyst CW9800M, and CW9800H1 and CW9800H2 Wireless Controllers. A switchover is initiated at the time of standby initialization.

  This is a rare case scenario. You will need design changes to fix the issue.

- 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 Cisco IOS XE 17.15.1, 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 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.

Supported Hardware

The following table lists the supported virtual and hardware platforms. (See Table 5: Supported PIDs and Ports for the list of supported modules.)

Table 3: Supported Virtual and Hardware Platforms

Platform	Description
Cisco Catalyst 9800-80 Wireless Controller	A modular wireless controller with up to 100-GE modular uplinks and seamless software updates. The controller occupies a 2-rack unit space and supports multiple module uplinks.
Cisco Catalyst 9800-40 Wireless Controller	A fixed wireless controller with seamless software updates for mid-size to large enterprises. The controller occupies a 1-rack unit space and provides four 1-GE or 10-GE uplink ports.
Cisco Catalyst 9800-L Wireless Controller	The Cisco Catalyst 9800-L Wireless Controller is the first low-end controller that provides a significant boost in performance and features.

Platform	Description
Cisco Catalyst 9800 Wireless Controller for Cloud	A virtual form factor of the Catalyst 9800 Wireless Controller that can be deployed in a private cloud (supports VMware ESXi, Kernel-based Virtual Machine [KVM], Microsoft Hyper-V, and Cisco Enterprise NFV Infrastructure Software [NFVIS] on Enterprise Network Compute System [ENCS] hypervisors), or in the public cloud as Infrastructure as a Service (IaaS) in Amazon Web Services (AWS), Google Cloud Platform (GCP) marketplace, 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.
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 4: Supported Host Environments for Public and Private Cloud

Host Environment	Software Version
VMware ESXi	• VMware ESXi vSphere 6.0, 6.5, 6.7, and 7.0 • VMware ESXi vCenter 6.0, 6.5, 6.7, and 7.0

Host Environment	Software Version
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 2019 Server and Windows Server 2016 (Version 1607) with Hyper-V Manager (Version 10.0.14393)
Microsoft Azure	Microsoft Azure
Oracle Cloud Infrastructure (OCI)	Oracle Cloud Infrastructure (OCI)

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

The base PIDs are the model numbers of the controller.

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

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

Table 5: Supported PIDs and Ports

The following table lists the supported SFP models.

Table 6: Supported SFPs

SFP Name	C9800-80-K9	C9800-40-K9	C9800-L-F-K9	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

SFP Name	C9800-80-K9	C9800-40-K9	C9800-L-F-K9	CW9800H1	CW9800H2	CW9800M
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	—
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	—

SFP Name	C9800-80-K9	C9800-40-K9	C9800-L-F-K9	CW9800H1	CW9800H2	CW9800M
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-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 Name	C9800-80-K9	C9800-40-K9	C9800-L-F-K9	CW9800H1	CW9800H2	CW9800M
SFP-10/25G-CSR-S	—	—	—	Supported	—	Supported
SFP-10/25G-BXD-I	—	—	—	Supported	—	Supported
SFP-10/25G-BXU-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-H10GB-CU5M	Supported	Supported	Supported	Supported	Supported	Supported
SFP-H10GB-CU1-5M	—	—	—	Supported	Supported	Supported
Finisar-LR (FTLX1471D3BCL)	—	—	Supported	Supported	Supported	Supported
Finisar-SR (FTLX8574D3BC)	—	—	—	Supported	Supported	Supported

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

Optics Modules

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

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

Network Protocols and Port Matrix

Table 7: Cisco Catalyst 9800 Series Wireless Controller - Network Protocols and Port Matrix

Source	Destination	Protocol	Destination Port	Source Port	Description
Any	Cisco Catalyst 9800 Series Wireless Controller	TCP	22	Any	SSH
Any	Cisco Catalyst 9800 Series Wireless Controller	TCP	23	Any	Telnet
Any	Cisco Catalyst 9800 Series Wireless Controller	TCP	80	Any	HTTP
Any	Cisco Catalyst 9800 Series Wireless Controller	TCP	443	Any	HTTPS
Any	Cisco Catalyst 9800 Series Wireless Controller	UDP	161	Any	SNMP Agent
Any	Any	UDP	5353	5353	mDNS
Any	Cisco Catalyst 9800 Series Wireless Controller	UDP	69	69	TFTP
Any	DNS Server	UDP	53	Any	DNS
Any	Cisco Catalyst 9800 Series Wireless Controller	TCP	830	Any	NetConf

Source	Destination	Protocol	Destination Port	Source Port	Description
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)
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

Source	Destination	Protocol	Destination Port	Source Port	Description
Cisco Catalyst 9800 Series Wireless Controller	TACACS+	TCP	49	Any	TACACS+
Cisco Catalyst 9800 Series Wireless Controller	Cisco Catalyst 9800 Series Wireless Controller	UDP	16667	16667	Mobility
Cisco Catalyst 9800 Series Wireless Controller	NTP Server	UDP	123	Any	NTP
Cisco Catalyst 9800 Series Wireless Controller	Syslog Server	UDP	514	Any	SYSLOG
Cisco Catalyst 9800 Series Wireless Controller	NetFlow Server	UDP	9996	Any	NetFlow
Cisco Catalyst 9800 Series Wireless Controller	Cisco Connected Mobile Experiences (CMX)	UDP	16113	Any	NMSP
Cisco Catalyst Center	Cisco Catalyst 9800 Series Wireless Controller	TCP	32222	Any	Device Discovery

Supported APs

The following Cisco APs are supported in this release.

Indoor Access Points

- Cisco Catalyst 9105AX (I/W) Access Points
- Cisco Catalyst 9115AX (I/E) Access Points
- Cisco Catalyst 9117AX (I) Access Points
- Cisco Catalyst 9120AX (I/E/P) Access Points
- Cisco Catalyst 9130AX (I/E) Access Points

- Cisco Catalyst 9136AX Access Points
- Cisco Catalyst 9162 (I) Series Access Points
- Cisco Catalyst 9164 (I) Series Access Points
- Cisco Catalyst 9166 (I/D1) Series Access Points
- Cisco Aironet 1815 (I/W/M/T), 1830 (I), 1840 (I), and 1852 (I/E) Access Points
- Cisco Aironet 1800i Access Point
- Cisco Aironet 2800 (I/E) Series Access Points
- Cisco Aironet 3800 (I/E/P) Series Access Points
- Cisco Aironet 4800 (I) Series Access Points

Outdoor Access Points

- Cisco Aironet 1540 (I/D) Series Access Points
- Cisco Aironet 1560 (I/D/E) Series Access Points
- Cisco Aironet 1570 (IC/EC/EAC) Series Access Points
- Cisco Industrial Wireless 3700 Series Access Points
- Cisco Catalyst Industrial Wireless 6300 Heavy Duty Series Access Point
- Cisco 6300 Series Embedded Services Access Point
- Cisco Catalyst 9124AX (I/D/E) Access Points
- Cisco Catalyst 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 8: 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 17.15.1	3.3 3.2 3.1 3.0 2.7 * all with latest patches	3.10.6 (base version) **Note** Base release of Cisco Prime Infrastructure that supports corresponding Cisco Catalyst 9800 Series Wireless Controller platform release and its features.	8.10.196.0 8.10.190.0 8.10.185.0 8.10.183.0 8.10.182.0 8.10.181.0 8.10.171.0 8.10.162.0 8.10.151.0 8.10.142.0 8.10.130.0 8.5.176.2 8.5.182.104	See Cisco Catalyst Center Compatibility Information	11.0 10.6.3

GUI System Requirements

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

Table 9: 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:

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.

- 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 10: Upgrade Path to Cisco IOS XE Dublin 17.15.x

Current Software	Upgrade Path for Deployments with 9130 or 9124	Upgrade Path for Deployments Without 9130 or 9124
16.10.x	—[4]	Upgrade first to 16.12.5 or 17.3.x and then to 17.15.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, 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.
17.1.x	Upgrade first to 17.3.5 or later and then to 17.15.x.	Upgrade first to 17.3.5 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
17.2.x	Upgrade first to 17.3.5 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, and then to 17.15.x.	Upgrade directly to 17.15.x.
17.3.4c or later	Upgrade directly 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 directly to 17.15.x.	Upgrade directly to 17.15.x.
17.7.x	Upgrade directly to 17.15.x.	Upgrade directly to 17.15.x.
17.8.x	Upgrade directly to 17.15.x.	Upgrade directly to 17.15.x.
17.9.x	Upgrade directly to 17.15.x	Upgrade directly to 17.15.x
17.10.x	Upgrade directly to 17.15.x	Upgrade directly to 17.15.x
17.11.x	Upgrade directly 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
8.9.x or any 8.10.x version prior to 8.10.171.0	Upgrade first to 17.3.5 or later or 17.6.x or later, and then to 17.15.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.

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

Cisco IOS XE 17.15.x	
To install and activate a specified file, and to commit changes to be persistent across reloads, run the following command: **device# install add file** *filename* **[activate |commit]** To separately install, activate, commit, end, or remove the installation file, run the following command: **device# install ?** **Note** We recommend that you use the GUI for installation.	
add file tftp: *filename*	Copies the install file package from a remote location to a device, and performs a compatibility check for the platform and image versions.
activateauto-abort-timer]	Activates the file and reloads the device. The **auto-abort-timer** keyword automatically rolls back image activation.
commit	Makes changes that are persistent over reloads.

Cisco IOS XE 17.15.x	
rollback to committed	Rolls back the update to the last committed version.
abort	Cancels file activation, and rolls back to the version that was running before the current installation procedure started.
remove	Deletes all unused and inactive software installation files.

Licensing

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

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

Interoperability with Clients

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

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

Table 11: 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 9.
Access Points	See Supported APs, on page 17.
Radio	• 802.11ac • 802.11a • 802.11g • 802.11n
Security	Open, PSK (WPA2-AES), 802.1X (WPA2-AES) (EAP-FAST, EAP-TLS)
RADIUS	See Compatibility Matrix, on page 19.
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.

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 17.15.1

Identifier	Headline
CSCwh63050	Controller sends IGMP queries without IP address and MAC address on Cisco IOS XE Cupertino 17.9.3
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

Identifier	Headline
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
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 17.15.1

Identifier	Headline
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

Identifier	Headline
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
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

Identifier	Headline
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
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

Identifier	Headline
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
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

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.