Release Notes for Cisco Catalyst 9800 Series Wireless Controller, Cisco IOS XE Cupertino Release 17.7.x

First Published: 2021-12-07

Last Modified: 2022-02-08

Release Notes for Cisco Catalyst 9800 Series Wireless Controller, Cisco IOS XE Cupertino 17.7.x

Introduction to Cisco Catalyst 9800 Series Wireless Controllers

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

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

- The controllers come with high availability and seamless software updates that are enabled by hot and cold patching. This keeps your clients and services up and running always, both during planned and unplanned events.
- The controllers come with built-in security, including secure boot, run-time defenses, image signing, integrity verification, and hardware authenticity.
- The controllers can be deployed anywhere to enable wireless connectivity, for example, on an on-premise device, on cloud (public or private), or embedded on a Cisco Catalyst switch (for SDA deployments) or a Cisco Catalyst access point (AP).
- The controllers can be managed using Cisco Catalyst Center, programmability interfaces, for example, NETCONF and YANG,or web-based GUI or CLI.
- The controllers are built on a modular operating system. Open and programmable APIs enable the automation of your day zero to day *n* network operations. Model-driven streaming telemetry provides deep insights into your network and client health.

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

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

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

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

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

What's New in Cisco IOS XE Cupertino 17.7.1

Table 1: New and Modified Software Features

Feature Name	Description and Documentation Link
6-GHz Client Steering Support in Cisco Catalyst 9136I Access Points	From Cisco IOS XE Cupertino 17.7.1 onwards, 6-GHz client steering is supported on Cisco Catalyst 9136I Access Points. 6-GHz client steering takes place when the controller receives a periodic client statistics report from a 2.4-GHz band or the 5-GHz band. The client-steering configuration is enabled under WLAN, and is configured only for clients that are 6-GHz capable. If a client in the report is 6-GHz capable, then client steering is triggered, and the client is steered to the 6-GHz band. The following commands are introduced: • **client-steering** • **wireless client client-steering client-count** • **wireless client client-steering window-size** • **wireless client client-steering util-threshold** • **wireless client client-steering min-rssi-24ghz -70** • **wireless client client-steering min-rssi-5ghz -75** For more information, see the chapter 6-GHz Band Operations.

Feature Name	Description and Documentation Link
6-GHz Radio Band Support in Cisco Catalyst 9136I Access Points	From Cisco IOS XE Cupertino 17.7.1 onwards, Cisco Catalyst 1936I Access Points support the 6-GHz radio band. The following commands are introduced: • **channel psc** • **dot11ax bcast-probe-response time-interval** • **dot11ax fils-discovery** • **dot11ax multi-bssid-profile** • **dot11ax {downlink-mumimo | downlink-ofdma | target-waketime | twt-broadcast | uplink-mumimo | uplink-ofdma}**
Ciphersuite Selection for Local EAP Authentication	From Cisco IOS XE Cupertino 17.7.1 onwards, the controller is equipped with a knob that controls the list of ciphersuites when using local authentication. For more information, see the chapter Local EAP Ciphersuite.
Cisco AI Enhanced RRM	AI-enhanced Radio Resource Management (RRM) is the latest in Cisco's award winning RRM. AI-enhanced RRM is coordinated through Cisco's DNA Center (on-prem appliance) as a service. The current RRM sites are seamlessly transitioned to an intelligent and centralized service. AI-enhanced RRM, along with other Cisco DNA Center services, brings a host of new features with it. For more information, see the chapter Radio Resource Management.
Cisco OEAP Split Tunneling	The split tunneling feature in Cisco OfficeExtend Access Point (OEAP) provides a mechanism to classify client traffic, based on packet content, using access control lists (ACLs). The following command is introduced: • **show split-tunnel client access-list** For more information, see the chapter Cisco OEAP Split Tunneling.

Feature Name	Description and Documentation Link
Coexistence of Intelligent Capture (iCAP) or IoT Services - Dual gRPC Channel	From Cisco IOS XE Cupertino 17.7.1, IoT Services and Intelligent Capture (iCAP) port configurations are allowed to co-exist. That is, when both IoT Services and iCAP features are enabled on the controller, there will be two gRPC connections from the corresponding AP. The following are the gRPC connections from AP: • One gRPC connection from AP to Cisco DNA Center for iCAP. • Another gRPC connection from AP to Cisco DNA Spaces Connector for IoT services. For more information, see the chapter IoT Services Management.
Configure Customized String in NAS-ID	Network access server identifier (NAS-ID) is used to notify the source of a RADIUS access request, which enables the RADIUS server to choose a policy for that request. You can configure one on each WLAN profile, VLAN interface, or access point group. The following command is modified: • **nas-id** For more information, see the chapter Network Access Server Identifier.
Converting IOS Commands to XML	This feature helps to automatically translate Cisco IOS commands into relevant NETCONF-XML or RESTCONF/JSON request messages. For more information, see the Programmability Configuration Guide.
Fast Teardown for a Mesh Access Point	This feature detects the root access point uplink failure and addresses the fast teardown of a mesh network when an uplink failure occurs. The following commands are introduced: • **fast-teardown** • **wireless profile mesh** **Note** Fast Teardown for Mesh APs is not supported on Cisco Industrial Wireless (IW) 3702 Access Points. For more information, see the chapter Mesh Access Points.

Feature Name	Description and Documentation Link
gNOI Factory Reset Services	The gNOI factory reset service provides an interface that instructs target devices to clean the existing state, and start the devices in the same condition they were shipped from the factory. For more information, see the Programmability Configuration Guide.
Installing the Cisco Catalyst 9800-CL Cloud Wireless Controller in Microsoft Azure Cloud Service	Microsoft Azure Cloud Service provides users with the capability to launch the controller in the cloud infrastructure. For more information, see the Cisco Catalyst 9800-CL Cloud Wireless Controller Installation Guide.
Managing Rogue Devices	From Cisco IOS XE Cupertino 17.7.1 onwards, you can use the following signatures to identify if an AP impersonator is using a channel number that is different from the one used by the managed AP. • Beacon DS Attack • Beacon Wrong Channel For more information, see the chapter Managing Rogue Devices.
Mesh Serial Backhaul	The Mesh Serial Backhaul feature is supported in the controller from Cisco IOS XE Cupertino 17.7.1 onwards, for Cisco Catalyst 9124AXE Series outdoor Access Points. A new knob is introduced under the radio profile, and that radio profile is associated to a RF tag to enable the Mesh Serial Backhaul feature. The following commands are introduced: • **mesh backhaul** • **mesh designated downlink** • **show ap name config slot 2 | inc Mesh** For more information, see the chapter Mesh Access Points.
Real-Time Access Points Statistics	From Cisco IOS XE Cupertino 17.7.1 onwards, for radio monitoring, you can reset the radios based on the statistics sent by the corresponding AP for a sampling period. When you configure the radios in the controller, if there is no increment in the Tx or Rx statistics when the radio is up, the radio reset is triggered. The following commands are introduced: • **show wireless stats ap join summary** • **show wireless stats ap history** For more information, see the chapter Real-Time Access Points Statistics.

Feature Name	Description and Documentation Link
Remote LAN Support in Cisco Catalyst 9124AXE Access Points	From Cisco IOS XE Cupertino 17.7.1 onwards, remote LAN is supported in Cisco Catalyst 9124AXE Access Points, in local mode and dual-radio mode. For more information, see the chapter Remote LANs.
RLAN Support for Fabric	From Cisco IOS XE Cupertino 17.7.1 onwards, the RLAN feature is supported on fabric. For more information, see the chapter Remote LANs.
Smart Licensing Using Policy: Account Information Included in the ACK and show command outputs	A RUM acknowledgement (ACK) includes the Smart Account and Virtual Account that was reported to, in CSSM. You can then display account information using various **show**commands. The account information that is displayed is always as per the latest available ACK on the product instance. For more information, see the chapter Smart Licensing Using Policy.
Smart Licensing Using Policy: CSLU Support for Linux	CSLU can now be deployed on a machine (laptop or desktop) running Linux. For more information, see the chapter Smart Licensing Using Policy.
Smart Licensing Using Policy: Factory-installed Trust Code	For new hardware orders, a trust code is now installed at the time of manufacturing. Note: You cannot use a factory-installed trust code to communicate with CSSM. For more information, see the chapter Smart Licensing Using Policy.
Smart Licensing Using Policy: Resource Utilization Measurement (RUM) Reporting and Acknowledgment (ACK) Requirement for Cisco Catalyst 9800-CL Wireless Controller	If you are using a *Cisco Catalyst 9800-CL Wireless Controller*, you must complete RUM reporting and ensure that the ACK is made available on the product instance - at least once. This is to ensure that correct and up-to-date usage information is reflected in CSSM. The following command is introduced: • **show license air entities** For more information, see the chapter Smart Licensing Using Policy.
Smart Licensing Using Policy: RUM Report Optimization and Availability of Statistics	RUM report generation and related processes have been optimized. This includes a reduction in the time it takes to process RUM reports, better memory and disk space utilization, and visibility into the RUM reports on the product instance (how many there are, the processing state each one is in, if there are errors in any of them, and so on). For more information, see the chapter Smart Licensing Using Policy.
Smart Licensing Using Policy: Support for Trust Code in Additional Topologies	A trust code is automatically obtained in topologies where the product instance initiates the sending of data to *CSLU* and in topologies where the product instance is in an air-gapped network. For more information, see the chapter Smart Licensing Using Policy.

Feature Name	Description and Documentation Link
Smart Licensing Using Policy: Support to Collect Software Version Through Smart License Agent	If version privacy is disabled (**no license smart privacy version** global configuration command), the Cisco IOS-XE software version running on the product instance and Smart Agent version information is *included* in the RUM report. For more information, see the chapter Smart Licensing Using Policy.
Software-Defined Application Visibility and Control	Software-Defined Application Visibility and Control (SD-AVC) is a network-level AVC controller that aggregates application data from multiple devices and sources, and provides composite application information. The following commands are introduced: • **address** • **avc sd-service** • **controller** • **destination-ports** • **dscp** • **segment** • **source-interface** • **transport application-updates** • **vrf** • **show sdavc ap download status** • **show sdavc status ap** For more information, see the chapter Software-Defined Application Visibility and Control.
Streaming Telemetry	From Cisco IOS XE Cupertino 17.7.1 onwards, on-change telemetry support is provided to a subset of XPaths. The following commands are introduced: • **show ap name dot11 neighbor summary** • **show wireless stats ap join summary sort** • **show ap summary sort name** For more information, see the chapter Streaming Telemetry.

Feature Name	Description and Documentation Link
SUDI99 Certificate Support	Some of the certificates used in the controller and AP platforms are expiring in May 2029 and require migration to a new set of certificates. SUDI99 certificate support addresses this migration scenario. The following commands are introduced: • **no platform sudi cmca3** • **show platform sudi pki** For more information, see the chapter SUDI99 Certificate Support.
Support for Federal Information Processing Standard (FIPS) Mode in Mesh Access Points	From this release onwards, FIPS mode is supported in Mesh Access Points.
Wi-Fi Protected Access 3 Hash-to-Element (H2E) Support for SAE Authentication	The Hash-to-Element (H2E) is a new method for password element generation which is used in the SAE protocol. It is a computationally efficient technique to mitigate side-channel attacks. The following are the supported password element methods in the WLAN configuration: • h2e: Hash-to-Element only; disables HnP. • hnp: Hunting and Pecking only; disables H2E. • Both-h2e-hnp: Both Hash-to-Element and Hunting and Pecking support is the default option. The following command is modified: • **security wpa akm sae pwe {h2e | hnp | both-h2e-hnp}** For more information, see the chapter Wi-Fi Protected Access 3.
Wi-Fi Protected Access 3 Support for Transition Disable	Transition Disable is an indication from an AP to an STA. This feature disables a few transition modes for subsequent connections to the AP's network. The following command is introduced: • **transition-disable** For more information, see the chapter Wi-Fi Protected Access 3.

Feature Name	Description and Documentation Link
YANG Model Version 1.1	Cisco IOS XE Cupertino 17.7.1 uses YANG Version 1.0. However, you can download YANG Version 1.1 from the GitHub folder. For inquiries related to the migrate_yang_version.py script or the Cisco IOS XE YANG migration process, send an email to xe-yang-migration@cisco.com. For more information, see the Programmability Configuration Guide.
ZTP Configuration through YANG	Zero Touch Provisioning is enabled through YANG models when NETCONF is enabled. For more information, see the Programmability Configuration Guide.

Table 2: New and Modified GUI Features

Feature Name	GUI Path
6-GHz Client Steering Support in Cisco Catalyst 9136I Access Points	• **Configuration > Tags and Profiles > WLANs**
6-GHz Radio Band Support in Cisco Catalyst 9136I Access Points	• **Configuration > Tags & Profiles > RF/Radio > RF**
Fast Teardown for a Mesh Access Point	• **Configuration > Wireless > Mesh > Profiles**
Mesh Serial Backhaul	• **Configuration > Tags & Profiles > RF/Radio**
Network Access Server Identifier	• **Configuration > Security > Wireless AAA Policy**
Real-Time Access Points Statistics	• **Configuration > Tags & Profiles > AP Join**
SUDI99 Certificate Support	• **Configuration > Security > PKI Management > Trustpoint**
Wi-Fi Protected Access 3 Hash-to-Element (H2E) Support for SAE Authentication	• **Configuration > Tags & Profiles > WLANs**

MIBs

The following MIBs are newly added or modified:

- AIRESPACE-WIRELESS-MIB.my
- CISCO-LWAPP-AP-MIB.my

- CISCO-LWAPP-AP-RADIOSTUCK-MIB.my
- CISCO-LWAPP-REAP-MIB.my
- CISCO-LWAPP-RRM-MIB.my
- CISCO-LWAPP-RF-MIB.my

Behavior Change

- Console access over serial ports is allowed only when the console activity is low. We recommend that you use a console over a Telnet session.
- If 802.11w is enabled in local mode, the controller rejects the reassociation request and sends the security association query only if the previous authentication is successful.
- Cisco TrustSec (CTS) manual and 802.1x configurations can co-exist when Security Association Protocol (SAP) is not configured.
- Downgrade to Cisco IOS XE Bengaluru 17.6.1 is not allowed on a HA system (GRUB3 instances) when smart licensing or license level is configured. Therefore, smart licensing or license data will not be retained as smart licensing with HA does not work in Cisco IOS XE Bengaluru 17.6. We recommend that you use the 17.6.2 versions to retain the license Truststore and license level configurations across HA systems.
- From this release, predownload of the AP image is based on the AP model rather than the image type. Predownload is allowed only when the model exists in the new capability XML file. Also, with appropriate modification of the capability XML, the controller can override the existing AP image for a particular model.

Interactive help

Interactive help is a user interface feature that

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

Modes of starting the interactive Help

You can start the interactive help in the these ways.

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

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

Additional troubleshooting information

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

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

Important Notes

- To migrate public IP address from 16.12.x to 17.x. ensure that you configure the **service internal** command. If you do not configure the **service internal** command, the IP address does not carry forward.
- The Cisco Aironet 2800 and 3800 APs do not reset an interface (to clear any Ethernet interface physical layer issues) if the Dynamic Host Configuration Protocol (DHCP) does not resolve the IP address within a certain duration.
- Avoid enabling AP sniffer mode when the controller is connected to Cisco Application Centric Infrastructure (ACI) that uses default endpoint learning. For more information, refer to CSCwa45713.

Supported Hardware

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

Table 3: Supported Virtual and Hardware Platforms

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

Platform	Description
Cisco Catalyst 9800 Wireless Controller for Cloud	A virtual form factor of the Catalyst 9800 Wireless Controller that can be deployed in a private cloud (supports VMware ESXi, Kernel-based Virtual Machine [KVM], Microsoft Hyper-V, and Cisco Enterprise NFV Infrastructure Software [NFVIS] on Enterprise Network Compute System [ENCS] hypervisors), or in the public cloud as Infrastructure as a Service (IaaS) in Amazon Web Services (AWS), Google Cloud Platform (GCP) marketplace, and Microsoft Azure.
Cisco Catalyst 9800 Embedded Wireless Controller for Switch	The Catalyst 9800 Wireless Controller software for the Cisco Catalyst 9000 switches brings the wired and wireless infrastructure together with consistent policy and management. This deployment model supports only Software Defined-Access (SDA), which is a highly secure solution for small campuses and distributed branches.

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

Table 4: Supported Host Environments for Public and Private Cloud

Host Environment	Software Version
VMware ESXi	• VMware ESXi vSphere 6.0, 6.5, 6.7, and 7.0 • VMware ESXi vCenter 6.0, 6.5, 6.7, and 7.0
KVM	• Linux KVM-based on Red Hat Enterprise Linux 7.6, 7.8, and 8.2 • Ubuntu 16.04.5 LTS, Ubuntu 18.04.5 LTS, Ubuntu 20.04.5 LTS
AWS	AWS EC2 platform
NFVIS	ENCS 3.8.1 and 3.9.1
GCP	GCP marketplace
Microsoft Hyper-V	Windows Server 2019, and Windows Server 2016 (Version 1607) with Hyper-V Manager (Version 10.0.14393)
Microsoft Azure	Microsoft Azure

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

The base PIDs are the model numbers of the controller.

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

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

Table 5: Supported PIDs and Ports

Controller Model	Description
C9800-CL-K9	Cisco Catalyst Wireless Controller as an infrastructure for cloud.
C9800-80-K9	Eight 1/10-Gigabit Ethernet SFP or SFP+ ports and two power supply slots. The following SFPs are supported: • GLC-BX-D • GLC-BX-U • GLC-EX-SMD • GLC-LH-SMD • GLC-SX-MMD • GLC-ZX-SMD • GLC-TE

Controller Model	Description
	The following enhanced SFPs are supported: • SFP-10G-AOC1M • SFP-10G-AOC2M • SFP-10G-AOC3M • SFP-10G-AOC5M • SFP-10G-AOC7M • SFP-10G-AOC10M • SFP-10G-SR • SFP-10G-SR-S • SFP-10G-SR-X • SFP-10G-LR • SFP-10G-LRM • SFP-10G-LR-X • SFP-10G-ER • SFP-10G-ZR • SFP-H10GB-CU1M • SFP-H10GB-CU1.5M • SFP-H10GB-CU2M • SFP-H10GB-CU2.5M • SFP-H10GB-CU3M • SFP-H10GB-CU5M • SFP-H10GB-ACU7M • SFP-H10GB-ACU10M • DWDM-SFP10G-30.33 • DWDM-SFP10G-61.41

Controller Model	Description
	The following QSFP+s are supported: • QSFP-40G-SR4 • QSFP-40G-LR4 • QSFP-40GE-LR4 • QSFP-40G-ER4 • QSFP-40G-SR4-S • QSFP-40G-LR4-S • QSFP-40G-SR-BD • QSFP-40G-BD-RX • QSFP-100G-SR4-S • QSFP-100G-LR4-S
C9800-40-K9	Four 1/10-Gigabit Ethernet SFP or SFP+ ports and two power supply slots. The following SFPs are supported: • GLC-BX-D • GLC-BX-U • GLC-LH-SMD • GLC-SX-MMD • GLC-EX-SMD • GLC-ZX-SMD • GLC-TE

Controller Model	Description
	The following enhanced SFPs are supported: • SFP-10G-AOC1M • SFP-10G-AOC2M • SFP-10G-AOC3M • SFP-10G-AOC5M • SFP-10G-AOC7M • SFP-10G-AOC10M • SFP-10G-SR • SFP-10G-SR-S • SFP-10G-SR-X • SFP-10G-LR • SFP-10G-LRM • SFP-10G-LR-X • SFP-10G-ER • SFP-10G-ZR • SFP-H10GB-CU1M • SFP-H10GB-CU1.5M • SFP-H10GB-CU2M • SFP-H10GB-CU2.5M • SFP-H10GB-CU3M • SFP-H10GB-CU5M • SFP-H10GB-ACU7M • SFP-H10GB-ACU10M • DWDM-SFP10G-30.33 - DWDM-SFP10G-61.41

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

The following table lists the supported SFP models.

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

Supported APs

The following Cisco APs are supported in this release.

Indoor Access Points

- Cisco Catalyst 9105AX (I) Access Points
  - VID 04 or later - supported from 17.6.4
  - VID 03 or earlier
- Cisco Catalyst 9105AX (W) Access Points
  - VID 02 or later - supported from 17.6.4
  - VID 01 or earlier
- Cisco Catalyst 9115AX (I/E) Access Points
- Cisco Catalyst 9117AX (I) Access Points
- Cisco Catalyst 9120AX (I/E) Access Points
  - VID 07 or later - supported from 17.6.4
  - VID 06 or earlier
- Cisco Catalyst 9120AX (P) Access Points
- Cisco Catalyst 9130AX (I/E) Access Points
  - VID 03 or later - supported from 17.6.4
  - VID 02 or earlier

  (For information about Cisco Catalyst 9105, 9120, or 9130 Access Points version support, see the Field Notice 72424.)
- Cisco Catalyst 9136 Access Points
- Cisco Aironet 1815 (I/W), 1830 (I), 1840 (I), and 1852 (I/E) Access Points
- Cisco Aironet 2800 (I/E) Series Access Points
- Cisco Aironet 3800 (I/E/P) Series Access Points
- Cisco Aironet 4800 Series Access Points
- Cisco Catalyst 9120AXP Access Points - supported from 16.12.2s

Outdoor Access Points

- Cisco Aironet 1540 Series Access Points

- Cisco Aironet 1560 Series Access Points
- Cisco Industrial Wireless 3700 Series Access Points
- Cisco Catalyst Industrial Wireless 6300 Heavy Duty Series Access Point
- Cisco 6300 Series Embedded Services Access Point
- Cisco Catalyst 9124AX (I/D/E) Access Points

Integrated Access Points

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

Network Sensor

- Cisco Aironet 1800s Active Sensor

Pluggable Modules

- Wi-Fi 6 Pluggable Module for Industrial Routers

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 6: Compatibility Informaton

Cisco Catalyst 9800 Series Wireless Controller Software	Cisco Identity Services Engine	Cisco Prime Infrastructure	Cisco AireOS-IRCM Interoperability	Cisco Catalyst Center	Cisco CMX
IOS XE 26.1.2	3.4 3.3 3.2 3.1 3.0 2.7 * all with latest patches	Not Available	8.10.196.0 8.10.190.0 8.10.185.0 8.10.183.0 8.10.182.0 8.10.181.0 8.10.171.0 8.10.162.0 8.10.151.0 8.10.142.0 8.10.130.0 8.5.176.2 8.5.182.104	See Cisco Catalyst Center Compatibility Information	11.1.1 11.1.0 11.0.1 11.0.0 10.6.3
IOS XE 26.1.1	3.4 3.3 3.2 3.1 3.0 2.7 * all with latest patches	Not Available	8.10.196.0 8.10.190.0 8.10.185.0 8.10.183.0 8.10.182.0 8.10.181.0 8.10.171.0 8.10.162.0 8.10.151.0 8.10.142.0 8.10.130.0 8.5.176.2 8.5.182.104	See Cisco Catalyst Center Compatibility Information	11.1.1 11.1.0 11.0.1 11.0.0 10.6.3

Table 7: Compatibility Information

Cisco Catalyst 9800 Series Wireless Controller Software	Cisco Identity Services Engine	Cisco Prime Infrastructure	Cisco AireOS-IRCM Interoperability	Cisco Catalyst Center	Cisco CMX
Cupertino 17.7.x	3.0 2.7 2.6 2.4	3.10 MR1 3.10 3.9	8.10.171.0 8.10.162.0 8.10.151.0 8.10.142.0 8.10.130.0 8.8.130.0 8.5.176.2 8.5.182.104 8.5.152.103 8.5.164.216	See Cisco Catalyst Center Compatibility Information	10.6.3

GUI System Requirements

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

Table 8: Hardware Requirements

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

1 We recommend 1 GHz.
2 We recommend 1-GB DRAM.

Software Requirements

Operating Systems:

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

Browsers:

- Google Chrome: Version 59 or later (on Windows and Mac)

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

Note Firefox Version 63.x is not supported.

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

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

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

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

Before You Upgrade

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

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

Other guidelines before you upgrade

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

- ERSPAN is not supported on the Cisco Catalyst 9800 Series Wireless Controller platform. Although the CLI allows you to enter **monitor session** commands for ERSPAN configuration, do not configure monitor session for ERSPAN on the controller. If an ERSPAN monitor session is configured, the configuration cannot be deleted from the controller.
- When you upgrade from Cisco IOS XE 17.9.5 or 17.12.2 to Cisco IOS XE 17.15.x, the controller WebUI does not support images greater than 1.5 GB.

  Workaround:

  - Upgrade using the CLI commands, or,
  - Upgrade to a fixed release first, and then upgrade to 17.15.x.
- When you upgrade from Cisco IOS XE Dublin 17.12.3 to 17.12.4 or Cisco IOS XE 17.15.1, the Cisco Catalyst Wi-Fi 6 and 6E APs fail to upgrade the AP image.

Workaround:

- Reboot the impacted APs through the power cycle.

For more information, see CSCwm08044

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

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

Cisco Catalyst APs may enter a boot loop if you upgrade software versions earlier than 17.9.4 over a WAN link. For more information, see: https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/220443-how-to-avoid-boot-loop-due-to-corrupted.html.

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

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

Note

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

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

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

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

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

     ```
     Device# capwap ap restart
     ```

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

- You might observe a high Confd CPU when full synchronization occurs between NETCONF datastore and Cisco IOS configuration. This behavior is normal and is triggered by the **line vty** command.
- From Cisco IOS XE Cupertino 17.7.1 onwards, for Cisco Catalyst 9800-CL Wireless Controller, ensure that you complete Resource Utilization Measurement (RUM) reporting and ensure that the ACK is made available on the product instance at least once. This is to ensure that correct and up-to-date usage information is reflected in the Cisco Smart Software Manager (CSSM).
- From Cisco IOS XE Amsterdam 17.3.1 onwards, the Cisco Catalyst 9800-CL Wireless Controller requires 16 GB of disk space for new deployments.

  If you are upgrading to Cisco IOS XE Amsterdam 17.3.x from a previous release, resizing of disk space is not supported. If the current disk space is lesser than 16 GB, you need to redeploy the VM to meet the new disk space requirements.
- Fragmentation lower than 1500 is not supported for the RADIUS packets generated by wireless clients in the Gi0 (OOB) interface.

- Cisco IOS XE allows you to encrypt all the passwords used on the device. This includes user passwords and SSID passwords (PSK). For more information, see the "Password Encryption" section of the Cisco Catalyst 9800 Series Configuration Best Practices document.
- While upgrading to Cisco IOS XE 17.3.x and later releases, if the **ip http active-session-modules none** command is enabled, you will not be able to access the controller GUI using HTTPS. To access the GUI using HTTPS, run the following commands in the order specified below:

  1. **ip http session-module-list pkilist OPENRESTY_PKI**
  2. **ip http active-session-modules pkilist**

- Cisco Aironet 1815T OfficeExtend Access Point will be in local mode when connected to the controller. However, when it functions as a standalone AP, it gets converted to FlexConnect mode.
- The Cisco Catalyst 9800-L Wireless Controller may fail to respond to the BREAK signals received on its console port during boot time, preventing users from getting to the ROMMON. This problem is observed on the controllers manufactured until November 2019, with the default config-register setting of 0x2102. This problem can be avoided if you set config-register to 0x2002. This problem is fixed in the 16.12(3r) ROMMON for Cisco Catalyst 9800-L Wireless Controller. For information about how to upgrade the ROMMON, see the Upgrading ROMMON for Cisco Catalyst 9800-L Wireless Controllers section of the Upgrading Field Programmable Hardware Devices for Cisco Catalyst 9800 Series Wireless Controllers document.
- By default, the controller uses a TFTP block size value of 512, which is the lowest possible value. This default setting is used to ensure interoperability with legacy TFTP servers. If required, you can change the block size value to 8192 to speed up the transfer process, using the **ip tftp blocksize** command in global configuration mode.
- We recommend that you configure the **password encryption aes** and the **key config-key password-encrypt** *key* commands to encrypt your password.
- If the following error message is displayed after a reboot or system crash, we recommend that you regenerate the trustpoint certificate:

  ```
  ERR_SSL_VERSION_OR_CIPHER_MISMATCH
  ```

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

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

- Do not deploy OVA files directly to VMware ESXi 6.5. We recommend that you use an OVF tool to deploy the OVA files.

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

  The following protocols and features are supported through this port:
  - Cisco Catalyst Center
  - Cisco Smart Software Manager
  - Cisco Prime Infrastructure
  - Telnet
  - Controller GUI
  - DNS
  - File transfer
  - GNMI
  - HTTP
  - HTTPS
  - LDAP
  - Licensing for Smart Licensing feature to communicate with CSSM
  - Netconf
  - NetFlow

  - NTP
  - RADIUS (including CoA)
  - Restconf
  - SNMP
  - SSH
  - SYSLOG
  - TACACS+

- During device upgrade using GUI, if a switchover occurs, the session expires and the upgrade process gets terminated. As a result, the GUI cannot display the upgrade state or status.
- From Cisco IOS XE Bengaluru 17.4.1 onwards, the telemetry solution provides a name for the receiver address instead of the IP address for telemetry data. This is an additional option. During the controller downgrade and subsequent upgrade, there is likely to be an issue—the upgrade version uses the newly named receivers, and these are not recognized in the downgrade. The new configuration gets rejected and fails in the subsequent upgrade. Configuration loss can be avoided when the upgrade or downgrade is performed from Cisco Catalyst Center.
- From Cisco IOS XE Bengaluru 17.4.1 onwards, session timeout under the policy profile is supported.
- 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 Cupertino 17.7.x

Table 9: Upgrade Path to Cisco IOS XE Cupertino 17.7.x

Current Software	Upgrade Path for Deployments with 9130 or 9124	Upgrade Path for Deployments without 9130 or 9124
16.10.x	—	Upgrade first to 16.12.5 or 17.3.x and then to 17.7.x.
16.11.x	—	Upgrade first to 16.12.5 or 17.3.x and then to 17.7.x.
16.12.x	Upgrade first to 17.3.4c or later and then to 17.7.x.	You can upgrade directly to 17.7.x.
17.1.x	Upgrade first to 17.3.4c or later and then to 17.7.x.	Upgrade first to 17.3.x and then to 17.7.x.
17.2.x	Upgrade first to 17.3.4c or later and then to 17.7.x.	Upgrade first to 17.3.x and then to 17.7.x.

Current Software	Upgrade Path for Deployments with 9130 or 9124	Upgrade Path for Deployments without 9130 or 9124
17.3.1 to 17.3.4	Upgrade first to 17.3.4c or later and then to 17.7.x.	You can upgrade directly to 17.7.x.
17.3.4c or later	You can upgrade directly to 17.7.x.	You can upgrade directly to 17.7.x.
17.4.x	Upgrade first to 17.6.x and then to 17.7.x.	Upgrade first to 17.6.x and then to 17.7.x.
17.5.x	Upgrade first to 17.6.x and then to 17.7.x.	Upgrade first to 17.6.x and then to 17.7.x.
17.6.x	You can upgrade directly to 17.7.x.	You can upgrade directly to 17.7.x.

Upgrade Path to Cisco IOS XE Cupertino 17.7.x

Table 10: Upgrade Path to Cisco IOS XE Cupertino 17.7.x

Current Software	Upgrade Path for Deployments with 9130 or 9124	Upgrade Path for Deployments Without 9130 or 9124
16.10.x	—[3]	Upgrade first to 16.12.5 or 17.3.x and then to 17.7.x.
16.11.x	—	Upgrade first to 16.12.5 or 17.3.x and then to 17.7.x.
16.12.x	Upgrade first to 17.3.4c or later and then to 17.7.x.	Upgrade directly to 17.7.x.
17.1.x	Upgrade first to 17.3.4c or later and then to 17.7.x.	Upgrade first to 17.3.x and then to 17.7.x.
17.2.x	Upgrade first to 17.3.4c or later and then to 17.7.x.	Upgrade first to 17.3.x and then to 17.7.x.
17.3.1 to 17.3.4	Upgrade first to 17.3.4c or later and then to 17.7.x.	Upgrade directly to 17.7.x.
17.3.4c or later	Upgrade directly to 17.7.x.	Upgrade directly to 17.7.x.
17.4.x	Upgrade first to 17.6.x and then to 17.7.x.	Upgrade first to 17.6.x and then to 17.7.x.
17.5.x	Upgrade first to 17.6.x and then to 17.7.x.	Upgrade first to 17.6.x and then to 17.7.x.
17.6.x	Upgrade first to 17.3.5 and then to 17.7.x.	Upgrade directly to 17.7.x.

[3] 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.

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

Finding the Software Version

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

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

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

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

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

Software Images

- **Release**: Cisco IOS XE Cupertino 17.7.x
- **Image Names (9800-80, 9800-40, and 9800-L)**:
  - C9800-80-universalk9_wlc.17.07.01.SPA.bin
  - C9800-40-universalk9_wlc.17.07.01.SPA.bin
  - C9800-L-universalk9_wlc.17.07.01.SPA.bin
- **Image Names (9800-CL)**:
  - **Cloud**: C9800-CL-universalk9.17.07.01.SPA.bin
  - **Hyper-V/ESXi/KVM**: C9800-CL-universalk9.17.07.01.iso, C9800-CL-universalk9.17.07.01.ova
  - **KVM**: C9800-CL-universalk9.17.07.01.qcow2
  - **NFVIS**: C9800-CL-universalk9.17.07.01.tar.gz

Software Installation Commands

Cisco IOS XE, Cupertino, 17.7.x	
To install and activate a specified file, and to commit changes to be persistent across reloads, run the following command: **device# install add file** *filename* **[activate |commit]** To separately install, activate, commit, end, or remove the installation file, run the following command: **device# install ?** **Note** We recommend that you use the GUI for installation.	
add file tftp: *filename*	Copies the install file package from a remote location to a device, and performs a compatibility check for the platform and image versions.
activateauto-abort-timer]	Activates the file and reloads the device. The **auto-abort-timer** keyword automatically rolls back image activation.
commit	Makes changes that are persistent over reloads.
rollback to committed	Rolls back the update to the last committed version.
abort	Cancels file activation, and rolls back to the version that was running before the current installation procedure started.
remove	Deletes all unused and inactive software installation files.

Licensing

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

Note Starting from Cisco IOS XE Cupertino 17.7.1, the Cisco Catalyst 9800-CL Wireless Controller will not accept more than 50 APs if the smart licensing is not connected and up.

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, Cupertino, 17.7.x
Cisco Wireless Controller	See Supported Hardware, on page 11.
Access Points	See Supported APs.
Radio	• 802.11ax • 802.11ac • 802.11a • 802.11g • 802.11n
Security	Open, PSK (WPA2-AES), 802.1X (WPA2-AES) (EAP-FAST, EAP-TLS) 802.11ax
RADIUS	See Compatibility Matrix, on page 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.

Table 12: 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	OS Sierra 10.12.6
Apple Macbook Air 13 inch	OS High Sierra 10.13.4
Macbook Pro Retina	OS Catalina
Macbook Pro Retina 13 inch early 2015	OS Mojave 10.14.3
Macbook Pro OS X	OS X 10.8.5
Macbook Air	OS Sierra v10.12.2
Macbook Air 11 inch	OS X Yosemite 10.10.5
MacBook M1 Chip	OS Catalina
Dell Inspiron 2020 Chromebook	Chrome OS 75.0.3770.129
Google Pixelbook Go	Chrome OS 97.0.4692.27

Client Type and Name	Driver or Software Version
HP chromebook 11a	Chrome OS 76.0.3809.136
Samsung Chromebook 4+	Chrome OS 77.0.3865.105
Dell Latitude (Intel AX210)	Windows 11 (22.110.x.x)
Dell Latitude 3480 (Qualcomm DELL wireless 1820)	Win 10 Pro (12.0.0.242)
Dell Inspiron 15-7569 (Intel Dual Band Wireless-AC 3165)	Windows 10 Home (21.40.0)
Dell Latitude E5540 (Intel Dual Band Wireless AC7260)	Windows 7 Professional (21.10.1)
Dell Latitude E5430 (Intel Centrino Advanced-N 6205)	Windows 7 Professional (15.18.0.1)
Dell Latitude E6840 (Broadcom Dell Wireless 1540 802.11 a/g/n)	Windows 7 Professional (6.30.223.215)
Dell XPS 12 v9250 (Intel Dual Band Wireless AC 8260)	Windows 10 Home (21.40.0)
Dell Latitude 5491 (Intel AX200)	Windows 10 Pro (21.20.1.1)
Dell XPS Latitude12 9250 (Intel Dual Band Wireless AC 8260)	Windows 10 Home
Dell Inspiron 13-5368 Signature Edition	Windows 10 Home (18.40.0.12)
FUJITSU Lifebook E556 Intel 8260 (Intel Dual Band Wireless-AC 8260 (802.11n))	Windows 8 (19.50.1.6)
Lenovo Yoga C630 Snapdragon 850 (Qualcomm AC 2x2 Svc)	Windows 10 Home
Lenovo Thinkpad Yoga 460 (Intel Dual Band Wireless-AC 9260)	Windows 10 Pro (21.40.0)
Note For clients using Intel wireless cards, we recommend that you to update to the latest Intel wireless drivers if the advertised SSIDs are not visible.	
Tablets	
Apple iPad 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

Client Type and Name	Driver or Software Version
Apple iPad Mini 2 ME279LL/A	iOS 11.4.1
Apple iPad Mini 4 9.0.1 MK872LL/A	iOS 11.4.1
Microsoft Surface Pro 3 13 inch (Intel AX201)	Windows 10 (21.40.1.3)
Microsoft Surface Pro 3 15 inch (Qualcomm Atheros QCA61x4A)	Windows 10
Microsoft Surface Pro 7 (Intel AX201)	Windows 10
Microsoft Surface Pro 6 (Marvell Wi-Fi chipset 11ac)	Windows 10
Microsoft Surface Pro X (WCN3998 Wi-Fi Chip)	Windows
Mobile Phones	
Apple iPhone 5	iOS 12.4.1
Apple iPhone 6s	iOS 13.5
Apple iPhone 7 MN8J2LL/A	iOS 11.2.5
Apple iPhone 8	iOS 13.5
Apple iPhone 8 Plus	iOS 14.1
Apple iPhone 8 Plus MQ8D2LL/A	iOS 12.4.1
Apple iPhone X MQA52LL/A	iOS 13.1
Apple iPhone 11	iOS 15.1
Apple iPhone 12	iOS 15.1
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 SR1
Drager Delta	VG9.0.2
Drager M300.3	VG2.4
Drager M300.4	VG2.4
Drager M540	DG6.0.2 (1.2.6)
Google Pixel 3a	Android 11

Client Type and Name	Driver or Software Version
Google Pixel 4	Android 11
Google Pixel 5	Android 11
Google Pixel 6	Android 11
Huawei Mate 20 pro	Android 9.0
Huawei P20 Pro	Android 10
Huawei P40	Android 10
LG v40 ThinQ	Android 9.0
One Plus 8	Android 11
Oppo Find X2	Android 10
Redmi K20 Pro	Android 10
Samsung Galaxy S9+ - G965U1	Android 10.0
Samsung Galaxy S10 Plus	Android 11.0
Samsung S10 (SM-G973U1)	Android 11.0
Samsung S10e (SM-G970U1)	Android 11.0
Samsung S20 Ultra	Android 10.0
Samsung S21 Ultra 5G	Android 11.0
Samsung Fold 2	Android 10.0
Samsung Note20	Android 10.0
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

Client Type and Name	Driver or Software Version
Vocera Badges B3000n	4.3.3.18
Vocera Smart Badges V5000	5.0.6.35
Zebra MC40	Android 4.4.4
Zebra MC40N0	Android 4.1.1
Zebra MC92N0	Android 4.4.4
Zebra MC9090	Windows Mobile 6.1
Zebra MC55A	Windows 6.5
Zebra MC75A	OEM ver 02.37.0001
Zebra TC51	Android 6.0.1
Zebra TC52	Android 10.0
Zebra TC55	Android 8.1.0
Zebra TC57	Android 10.0
Zebra TC70	Android 6.1
Zebra TC75	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 6.4
Zebra ZQ610 Industrial Printer	LINK OS 6.4
Zebra ZQ620 Mobile Printer	LINK OS 6.4
Wireless Module	
Intel 11ax 200	Driver v22.20.0
Intel AC 9260	Driver v21.40.0
Intel Dual Band Wireless AC 8260	Driver v19.50.1.6
Intel AX 210	Driver v22.110.x.x (or above)
Samsung S21 Ultra	Driver v20.80.80
QCA WCN6855	Driver v1.0.0.901
PhoenixContact FL WLAN 2010	Firmware version: 2.71

Issues

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

Note All incremental releases contain fixes from the current release.

Cisco Bug Search Tool

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

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

Open Caveats for Cisco IOS XE, Cupertino, 17.7.1

Caveat ID	Description
CSCvz89115	Flexconnect APs are not forwarding DHCP packets after change-of-authorization (CoA) with a change of VLAN using 802.1x encryption.
CSCvz94692	AP crash is observed due to radio failure (too many radio failures).
CSCwa01168	Controller reloads unexpectedly due to mobilityd crash.
CSCwa12278	Cisco Catalyst 9115 AP is crashing due to kernel panic.
CSCwa13091	Radio Resource Management (RRM): Tx power changes are not getting applied to the AP.
CSCwa14307	AP crash is observed due to kernel panic.
CSCvz82490	Suite B: Incorrect APUT response to STA using incorrect TLS authentication parameters test.
CSCwa23783	IOS-XE based RLAN capable AP's are unable to join AireOS or Cisco Catalyst 9800 controllers.
CSCwm95849	Cisco Catalyst 9136 AP does not receive the 6e SSID

Resolved Caveats for Cisco IOS XE, Cupertino, 17.7.1

Caveat ID	Description
CSCvv94885	The **show ap cdp neighbours** command displays the name of the switch instead of the domain name.

Caveat ID	Description
CSCvx71141	Cisco Catalyst 9800-80 Wireless Controller crashes due to a CPU hog in the radio resource management (RRM) process.
CSCvx78215	An IOS XE device might crash at DoubleExceptionVector.
CSCvx81815	Controller does not send server hello packets to AP when enabling Datagram Transport Layer Security (DTLS) encryption.
CSCvy01360	Cisco Catalyst 9115AX AP is reporting false radar detection on channels 100-112.
CSCvy02120	Cisco Catalyst 9130AX AP fails to send reassociation response to roaming clients and deletes the client.
CSCvy05019	The output of the **show platform software system all** command output does not display interfaces greater than 10.
CSCvy11011	Controller displays a traceback similar to: EVENTLIB-3-CPUHOG - ewlc_client_location - remove_weakest_radio_measurement.
CSCvy11394	Controller allows configuring netflow on L2 port-channel.
CSCvy11981	Controller reloads unexpectedly when AP name is more than 31 characters.
CSCvy14956	Controller sends DHCP as relay proxy even when the client SVI interface is shutdown.
CSCvy25684	Different data rates are observed in CLI and RF profiles.
CSCvy36744	Controller stops forwarding broadcasts intermittently to clients.
CSCvy46043	Controller reloads unexpectedly for switch integrated security features (SISF) heap pointer to l2_socket_counter record.
CSCvy58934	Controller is not sending the CAPWAP restart payload when filter is applied and AP name is changed.
CSCvy72750	Unable to use the **wireless broadcast vlan** command.
CSCvy73836	Cisco Catalyst 9800-80 Controller goes to ROMMON after multiple failovers due to power cycling.
CSCvy74904	AP authorization related RADIUS request does not include the calling station ID and NAS port type.
CSCvy76922	Switch stack with Cisco IOS XE 17.3.2a displays high memory alerts.
CSCvy87749	Controller sends DHCP as relay proxy even after removing IP helper from the client SVI interface.
CSCvy89423	WNCMGRD process has crashed due to segmentation fault.

Caveat ID	Description
CSCvy89508	The primary member displays "standby hot" even though the standby is in recovery mode.
CSCvy90646	Controller drops the incoming CAPWAP keepalive for random APs.
CSCvy94284	Controller crashes after running **clear wlan id** command.
CSCvy99116	A crash is observed when a wireless client attempts to connect and the connection times out.
CSCvz11154	Continuous memory leak with multiple table entries is observed in FMAN database.
CSCvz14394	Custom-page in web authentication parameter map is not loaded into running configuration after a reload.
CSCvz15015	Cisco Catalyst 9130AX AP loses its WLAN configuration after moving between controllers.
CSCvz17623	Memory leak is observed in emulated database and AP join.
CSCvz28378	Memory leak is observed in WNCD process running 17.3.3 of around 200MB per day.
CSCvz39749	Client location probe displays error when probe request parsing fails.
CSCvz45305	Controller is missing fields in the access-request when sending it for a sleeping client.
CSCvz45488	Memory leak is observed in the OPERATIONAL_DB causing dbm crash.
CSCvz45576	Rogue telemetry updates need to be throttled as the controller sends lot of rogue reports to Cisco DNAC.
CSCvz51976	Include AP ethernet speed and duplex information in the output of **show ap config general** command.
CSCvz52851	SSO switchover does not re-establish LISP sessions to the CPs.
CSCvz53408	Fast Transition IE is sent as 0 in M3 after session timeout.
CSCvz63742	Controller does not provide cLApAdminStatus information through SNMP when forensic Advanced Wireless Intrusion Prevention System (aWIPS) is configured.
CSCvz68857	Optimize bsnMobileData OID query to improve performance.
CSCvz77768	Cisco IOS AP brings the radio down after encountering Dynamic Frequency Selection (DFS) event even when non-DFS channels are available.

Caveat ID	Description
CSCvz80697	Controller does not remove old NMSP entries when new probes are received in a different slot.
CSCvz84691	Controller crashes due to WNCD process when learning an IP address for a client.
CSCvz89976	Controller running 17.3.4 crashes due to workgroup bridge (WGB).

Troubleshooting

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

Related Documentation

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

Cisco Wireless Controller

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

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

The installation guide for your controller is available at:

- Hardware Installation Guides

All Cisco Wireless Controller software-related documentation

Cisco Wireless Access Points Detailed Channels and Maximum Power Settings

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

Detailed Channels and Maximum Power Settings Document for Supported Access Points

Feature Matrix for Cisco Wireless Access Points

Feature Matrix for Cisco Wireless Access Points

Cisco Catalyst 9800 Series Wireless Controller Data Sheets

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

Cisco Embedded Wireless Controller on Catalyst Access Points

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

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

Wireless Product Comparison

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

Cisco Access Points–Statement of Volatility

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

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

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

Cisco Prime Infrastructure

Cisco Prime Infrastructure Documentation

Cisco Connected Mobile Experiences

Cisco Connected Mobile Experiences Documentation

Cisco Catalyst Center

Cisco Catalyst Center Documentation

Communications, Services, and Additional Information

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

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2021 Cisco Systems, Inc. All rights reserved.