Release Notes for Cisco Catalyst 9800 Series Wireless Controller, Cisco IOS XE Dublin 17.12.x

First Published: 2023-07-31

Last Modified: 2024-04-01

Release Notes for Cisco Catalyst 9800 Series Wireless Controller, Cisco IOS XE Dublin 17.12.x

Introduction to Cisco Catalyst 9800 Series Wireless Controllers

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

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

- The controllers come with high availability 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 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 Catalyst 9800 Series controllers are available in multiple form factors to cater to your deployment options:

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

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

What's New in Cisco IOS XE Dublin 17.12.3

Table 1: New and Modified Software Features

Feature Name	Description and Documentation Link
Support for Cisco Catalyst 9163E Access Point and CW-ANT-D1-NS-00 Antenna on Cisco Catalyst 9163E Access Point	From this release, support for Cisco Catalyst 9163 Access Point and CW-ANT-D1-NS-00 Antenna on this access point is introduced. For more information, see Cisco Catalyst 9163E Access Point.
Automated Frequency Coordination (AFC) Support	This release supports the Automated Frequency Coordination (AFC) feature, a coordination system in cloud, that allocates the channels and power levels to APs to operate in standard power mode in the 6-GHz frequency spectrum. To begin with, the feature will be available only in the U.S., subject to final approval from the FCC. **Note** The AFC support will be enabled in Cisco Catalyst 9800 Wireless Controllers running IOS-XE 17.12.3, through Cisco cloud-based software service, after a final approval is obtained from the FCC. The feature is supported in the following APs: • Cisco Catalyst Wireless 9166D1 Access Point • Cisco Catalyst Wireless 9162I Series Access Point • Cisco Catalyst Wireless 9164I Series Access Point • Cisco Catalyst 9136 Series Access Point • Cisco Catalyst Wireless 9163E Access Point For more information, see the chapter Automated Frequency Coordination.
Cloud Monitoring for Catalyst Controllers	The Cloud Monitoring for Catalyst Controllers feature helps to monitor controllers using the Meraki dashboard. Currently, this feature is in a limited customer beta and is not supported by Cisco TAC. For more information about this feature, see Cloud Monitoring for Catalyst. For further help, write to: c9800-dashboard-monitoring@external.cisco.com

Feature Name	Description and Documentation Link
Electronic Shelf Label (ESL) Support Through Internal IoT Radio	This release supports Application Hosting (IOx App) on APs to access its internal IoT radio. The IOx App supports the capability to load custom or proprietary firmware onto the internal IoT radio. For example, running third-party proprietary firmware on the AP's IoT radio for ESL.
Support for Automatic Log Deletion for Wireless	The Automatic Log Deletion feature allows you to delete entries from the logging buffer automatically after a configurable time. You must configure the local syslog retention period after which the entries are purged from the device. This feature also allows one buffer clean up per day, which cleans the buffer log based on the configured duration every 24 hours. The following command is introduced as part of this feature: • **logging purge-log buffer days** For more information about the command, see https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/17-12/cmd-ref/b_wl_17_12_cr/configuration-commands-g-to-z.html#wp1458580136.
Cisco Catalyst 9800 Wireless Controller for Cloud - Ultra-Low Profile	The Cisco Catalyst 9800 Wireless Controller for Private Cloud - Ultra-Low Profile is introduced to cater to the Cisco FlexConnect deployment mode, targeting a maximum of 100 APs and 1000 clients; and compute resource requirements of two virtual Central Processing Units (vCPUs), 6-GB RAM, and 16-GB hard disk. The supported private cloud providers are VMware ESXi, KVM, Hyper-V, and Cisco NFVIS (on ENCS). For more information, see *Cisco Catalyst 9800-CL Cloud Wireless Controller Installation Guide*.
AP Power Distribution Support for Cisco Catalyst 9162 Series Access Points	From this release, AP power distribution is supported in Cisco Catalyst 9162 Series APs. This allows the network administrator to determine how the AP radios operate when it is powered with less than 30W.

What's New in Cisco IOS XE Dublin 17.12.2

From this release, Layer 2 VRF is also supported with WGB, RADSEC, and TRUSTSEC capabilities. However, RLAN is not supported with VRF. For more information, see Remote LANs.

What's New in Cisco IOS XE Dublin 17.12.1

Table 2: New and Modified Software Features

Feature Name	Description and Documentation Link
Access Point Auto Location Support	This feature enables support for Access Point Auto Location, which helps to effectively self-locate APs on a map by combining various ranging technologies and algorithms. This feature requires the use of Cisco Spaces to interpret the AP location information and place the APs on maps. The following commands are introduced: • **ap geolocation derivation ranging** • **geolocation ftm initiator burst-size** • **geolocation ftm initiator burst-duration** • **ap name ap-name floor** • **ap geolocation ranging all accurate** • **ap geolocation ranging site ap-site-tag accurate** • **show ap geolocation ranging** **Note** Fine Timing Measurement (FTM) ranging is a disruptive process and may cause disturbances in radio. We recommend that you run FTM ranging during offpeak or quiet hours. FTM ranging is not supported with FRA (dual 5G) operation. For more information, see AP Management.

Feature Name	Description and Documentation Link
Modified Trustpoints for Secure Unique Device Identity (SUDI) Certificates	

Feature Name	Description and Documentation Link

	From Cisco IOS XE Dublin 17.12.1 onwards, the following changes have been introduced for trustpoints:
	• Trustpoint names for existing SUDI certificates
	If your device supports Cisco Manufacturing CA III certificate and is not disabled, the trustpoint names are as follows:
	• For *Cisco Manufacturing CA III* certificate, the trustpoint name has changed from CISCO_IDEVID_SUDI to CISCO_IDEVID_CMCA3_SUDI
	• For *Cisco Manufacturing CA SHA2* certificate, the trustpoint name has changed from CISCO_IDEVID_SUDI_LEGACY to CISCO_IDEVID_CMCA2_SUDI
	If your device does not support Cisco Manufacturing CA III certificate or if the certificate is disabled using **no platform sudi cmca3** command, the trustpoint names are as follows:
	• For *Cisco Manufacturing CA SHA2* certificate, the trustpoint name has changed from CISCO_IDEVID_SUDI to CISCO_IDEVID_CMCA2_SUDI
	• For *Cisco Manufacturing CA* certificate, the trustpoint name has changed from CISCO_IDEVID_SUDI_LEGACY to CISCO_IDEVID_CMCA_SUDI
	• Hardware SUDI certificates
	• If your device supports *High Assurance SUDI CA* certificate, this certificate is loaded under CISCO_IDEVID_SUDI trustpoint.
	• If your device does not support *High Assurance SUDI CA* certificate, *ACT2 SUDI CA* certificate is loaded under CISCO_IDEVID_SUDI trustpoint.
	• **show wireless management trustpoint** command output
	If Cisco Catalyst 9300 Series Switch is used with a Cisco Catalyst 9800 Series Wireless Controller for wireless deployments, the trustpoint name in the output of **show wireless management trustpoint** command is updated to the modified trustpoint name as mentioned previously.
	The following example shows a sample output of **show wireless management trustpoint** command. Note that if your device does not support Cisco Manufacturing CA III certificate or if the certificate is disabled, the Trustpoint Name in the following output displays CISCO_IDEVID_CMCA2_SUDI.
	`Device# show wireless management trustpoint`
	`Trustpoint Name  : CISCO_IDEVID_CMCA3_SUDI`
	`Certificate Info : Available`

Feature Name	Description and Documentation Link

	<pre>Certificate Type : MIC
	Certificate Hash : <SHA1 - hash>
	Private key Info : Available
	FIPS suitability : Not Applicable</pre>
	• **show ip http server status** command output
	If you configure the trustpoint for the HTTP server as CISCO_IDEVID_SUDI, the output of **show ip http server status** command displays the operating trustpoint along with the configured trustpoint.
	The following example shows a sample output of **show ip http server status** command with both the configured and the operating trustpoint names. Note that if your device does not support Cisco Manufacturing CA III certificate or if the certificate is disabled, the operating trustpoint in the following output displays CISCO_IDEVID_CMCA2_SUDI.
	<pre>Device# show ip http server status
	…
	HTTP secure server trustpoint: CISCO_IDEVID_SUDI
	HTTP secure server operating trustpoint:
	CISCO_IDEVID_CMCA3_SUDI</pre>

Archive less than 1 day	The **request platform software trace archive last** command has been enhanced to archive all the trace logs relevant to all the processes running on a system.
Cisco Catalyst 9166D Series Wi-Fi 6E Access Point	The Cisco Catalyst 9166D Series Wi-Fi 6E Access Point is an enterprise-class tri-band (2.4 GHz, 5 GHz, 6 GHz) indoor access point with integrated directional antennas. The AP supports full interoperability with leading 802.11ax and 802.11ac clients and a hybrid deployment with other APs and controllers. For a full listing of the AP's features and specifications, see the *Cisco Catalyst 9166D Series Wi-Fi 6E Access Point Data Sheet.*
Cisco Catalyst 9800 Wireless Controller for Cloud - Ultra-Low Profile (**Beta, No TAC Support**)	The ultra-low profile memory variant of the Catalyst 9800 Wireless Controller for Cloud comes with 4GB RAM and 2vCPUs and is deployed in a private cloud (supports ESXi, KVM, and NFVIS on ENCS hypervisors) as Infrastructure as a Service (IaaS). This controller can support up to 50 APs and 1000 clients. For more information and technical support, see the *Cisco Catalyst 9800 Wireless Controller for Cloud - Ultra-Low Profile Installation Guide*.
Cisco Catalyst IW9167I Heavy Duty Access Point	The Cisco Catalyst IW9167I Wi-Fi 6 Access Point is a heavy-duty tri-band (2.4 GHz, 5 GHz, 6 GHz ready) outdoor access point with integrated antennas. For a full listing of the AP's features and specifications, see the Cisco Catalyst IW9167 Heavy Duty Series Data Sheet.

Feature Name	Description and Documentation Link
Ease of Debugging	The following commands are introduced on the AP console to enable or disable the client debug bundle and to verify the client debug status: • **debug client-bundle start** • **show client-bundle status** • **debug client-bundle stop**
Embedded Packet Capture Enhancement	In this release, the Embedded Packet Capture (EPC) feature is enhanced to support increased buffer size, continuous capture, and filtering of multiple MAC addresses in one EPC session. The following commands are introduced: • **monitor capture epc-session-name buffer circular file** • **monitor capture epc-session-name continuous-capture** • **monitor capture epc-session-name inner mac** For more information, see Embedded Packet Capture.
FIPS 140-3 compliance	This release enables all Wave 2 APs to achieve FIPS 140-3 compliance, ensuring adherence to security standards. The Cisco Catalyst 9800 controllers, however, are FIPS 140-2 compliant. **Caution** Downgrading to versions below 17.12.1 can have a negative impact on Wave 2 APs in the following scenarios: • When FIPS or WLANCC security modes are enabled. • When the ECDHE-RSA-AES128-GCM-SHA256 cipher suite is not selected for AP DTLS (by default it is selected). **Note** There is no impact on the Cisco IOS AP models. The **show wireless certification config** command has been introduced to verify whether downgrade is impacted or not. For more information, see FIPS.
Improve crash datacollection, kernel panics, out of memory	A new command is introduced to limit the number of kernel core dumps collected on the AP: • **core-dump kernel limit**
Indoor deployment support for UK -ROW domain on IW9167I and IW9167E	Indoor deployment for UK -ROW domain is supported on Cisco Catalyst IW9167I and IW9167E Heavy Duty Access Point from this release. For more information, see the *Cisco Catalyst IW9167 Heavy Duty Series Software Configuration Guide* .

Feature Name	Description and Documentation Link
Intelligent Capture (iCAP) Hardening	This feature aims at making troubleshooting for wireless clients and APs easier. In this release, the following enhancements are made to the iCAP feature: • Anomaly Detection • RF Statistics The following commands are introduced: • **icap subscription client anomaly-detection report-individual enable** • **icap subscription client anomaly-detection report-individual per-client throttle** • **icap subscription client anomaly-detection report-individual per-type throttle** • **ap name icap subscription client anomaly-detection report-individual enable** • **ap name icap subscription client anomaly-detection report-individual per-client throttle** • **ap name icap subscription client anomaly-detection report-individual per-type throttle** For more information, see Intelligent Capture Hardening.
MacBook Analytics	This feature is supported on the controller when the MacBook device sends 11k action frames along with the model information. For more information, see Device Analytics.
Mesh Support in Cisco Catalyst 9130AX Series Access Points	From this release, mesh support is included in the Cisco Catalyst 9130AX Series Access Points. All traditional capabilities of mesh are included in the Cisco Catalyst 9130AX Series APs operating in Cisco IOS XE Dublin 17.12.1. For more information, see Mesh Access Points.
New Countries Supporting 6-GHz Radio Band	From this release, Australia, Brazil, Costa Rica, Honduras, Hong Kong, Japan, Jordan, Kenya, Malaysia, Morocco, New Zealand, Peru, Qatar, Saudi Arabia, and United Arab Emirates are added to the list of countries that supports 6-GHz radio band. For more information, see Regulatory Compliance Domain.

Feature Name	Description and Documentation Link
RF based Automatic Load Balancing	The RF based Automatic AP Load Balancing feature uses Radio Resource Management (RRM) neighbor report-based AP grouping and load-balancing across WNCd instances. The following commands are introduced: • **ap neighborhood load-balance** • **ap neighborhood calendar-profile** • **wireless load-balance ap method rf** • **show ap neighborhood summary** • **show ap neighborhood details** • **show ap neighborhood** • **show ap neighborhood mac details** • **show ap neighborhood wncd** For more information, see RF based Automatic AP Load Balancing.
Rogue Channel Width	From this release, you can specify the channel width and the band for rogue detection. The following command is introduced: • **condition chan-width** For more information, see Radio Resource Management.
Rogue PMF	From this release, the controller will contain rogue APs with 802.11w Protected Management Frame (PMF) on centrally switched WLANs. The following commands are introduced: • **rogue detection containment pmf-denial** • **pmf-deauth** For more information, see Radio Resource Management.
Software entropy enhancement for FIPS 140-3	From Cisco IOS XE Dublin 17.12.1 onwards, Federal Information Processing Standard (FIPS) 140-3 is supported as a security standard to validate cryptographic modules.

Feature Name	Description and Documentation Link
Support for Cisco Wave 1 Access Points	Support for the following Cisco Wave 1 APs are introduced in this release: • **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** Feature support is the same as in Release 17.3.x. Features introduced in 17.4.1 or later are not supported on these APs in Release 17.12.1.
VRF Support	From this release, Virtual Routing and Forwarding (VRF) is supported. For more information, see VRF Support.
Wakeup Threshold for AP Power Save Mode	This feature enables you to define the client threshold in the AP power profile configuration to determine when an AP wakes up from the power save mode or enters the power save mode. The following command is introduced: • **power-save-client-threshold** For more information, see AP Management.
Wireless Mesh Support for Cisco Software-Defined Access	From this release, wireless mesh is supported on Cisco Software-Defined Access. The following commands are introduced: • **show ap name mesh roam history** • **show wireless mesh ap fabric summary**

Table 3: New and Modified GUI Features

Feature Name	GUI Path
AP Location	• **Configuration >Wireless >Wireless Global** • **Configuration > Tags & Profiles > AP Join**
Configuring Transition Mode and Pure WPA3 (6-GHz) on the Same WLAN Profile	• **Configuration > Tags & Profiles > WLANs**
Rogue Channel Width	• **Configuration > Security >Wireless Protection Policies > Rogue AP Rules**

MIBs

The following MIBs are newly added or modified:

- AIRESPACE-WIRELESS-CAPABILITY.my
- AIRESPACE-WIRELESS-MIB.my
- CISCO-LWAPP-AP-CAPABILITY.my
- CISCO-LWAPP-CDP-CAPABILITY.my
- CISCO-LWAPP-DOT11-CAPABILITY.my
- CISCO-LWAPP-DOT11-CLIENT-CALIB-CAPABILITY.my
- CISCO-LWAPP-DOT11-CLIENT-CAPABILITY.my
- CISCO-LWAPP-DOWNLOAD-CAPABILITY.my
- CISCO-LWAPP-GUEST-LAN-CAPABILITY.my
- CISCO-LWAP P-IPV6-CAPABILITY.my
- CISCO-LWAPP-MESH-CAPABILITY.my
- CISCO-LWAPP-MESH-LINKTEST-CAPABILITY.my
- CISCO-LWAPP-MFP-CAPABILITY.my
- CISCO-LWAPP-MOBILITY-CAPABILITY.my
- CISCO-LWAPP-MOBILITY-EXT-CAPABILITY.my
- CISCO-LWAPP-QOS-CAPABILITY.my
- CISCO-LWAPP-QOS-MIB.my
- CISCO-LWAPP-REAP-CAPABILITY.my
- CISCO-LWAPP-RF-CAPABILITY.my
- CISCO- LWAPP-ROGUE-CAPABILITY.my
- CISCO-LWAPP-ROGUE-MIB.my
- CISCO-LWAPP-RRM-CAPABILITY.my
- CISCO-LWAPP-SI-CAPABILITY.my
- CISCO-LWAPP-TUNNEL-CAPABILITY.my
- CISCO-LWAPP-WLAN-CAPABILITY.my
- CISCO-LWAPP-WLAN-POLICY-CAPABILITY.my
- CISCO-LWAPP-WLAN-POLICY-MIB.my
- CISCO-LWAPP-WLAN-SECURITY-CAPABILITY.my
- CISCO-WIRELESS-HOTSPOT-CAPABILITY.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: Cisco is 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 Changes

- From Cisco IOS XE Dublin 17.12.2 onwards, 6-GHz radio band is not supported for Honduras country code (HN) in Cisco Catalyst 9136, 9162, 9164, and 9166 Series APs.
- From Cisco IOS XE Dublin 17.12.x, the Express Wi-Fi by Facebook feature is not supported.
- From Cisco IOS XE Dublin 17.12.2, the **show running-config wlan** command is modified. The *wlan_name* variable is removed.
- The following command output is modified for the KPIs for AP Health Via the Controller and AP feature:
  - **show ap name config general**
- The following command outputs are modified for the Configuring Transition Mode and Pure WPA3 (6 GHz) on the Same WLAN Profile feature:
  - **show wlan all**
  - **show wlan id**
  - **show wlan name**

- **show wlan summary**

- WPA2 should be disabled while WPA3, PMF and dot11ax are enabled to broadcast WLAN exclusively on 6-GHz band. WPA2 can be enabled when broadcasting on other bands, such as 2.4 and 5-GHz.
- The inner MAC filtering feature of Embedded Packet Capture (EPC), captures CAPWAP data fragments and CAPWAP control not filtered by MAC.
- When wireless interface is not available, the RMI +RP configuration on the Web UI is disabled.
- From this release, the **bssid-neighbor-stats interval** value has been changed from 1 to180 seconds to 30 to 600 seconds. The default value is 180 seconds.
- From this release, the default console baud rate of the 802.11AX APs is changed from 9600 bps to 115200 bps.
- Both internal and external APs in NAT deployments must use different AP join profiles when CAPWAP Discovery Private and Public are enabled separately. This is applicable to APs upgraded to Cisco IOS XE Dublin 17.12.x and later.
- If you have configured CISCO_IDEVID_SUDI trustpoint in your configuration, you will need to replace it with CISCO_IDEVID_CMCA3_SUDI to avoid client connection and AP join issues. The reason for this change being the CISCO_IDEVID_SUDI changed from SW-SUDI certificate in previous releases to HW-SUDI certificate. The processing of HW-SUDI certificate is much slower than the SW-SUDI. Here, CISCO_IDEVID_CMCA3_SUDI is the new SW-SUDI certificate.

Interactive Help

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

You can start the interactive help in the following ways:

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

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

The following features have an associated interactive help:

- Configuring AAA
- Configuring FlexConnect Authentication
- Configuring 802.1x Authentication
- Configuring Local Web Authentication
- Configuring OpenRoaming

- Configuring Mesh APs

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

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

Supported Hardware

The following table lists the supported virtual and hardware platforms. (See Table 6: Supported PIDs and Ports for the list of supported modules.)

Table 4: Supported Virtual and Hardware Platforms

Platform	Description
Cisco Catalyst 9800-80 Wireless Controller	A modular wireless controller with up to 100-GE modular uplinks and seamless software updates. The controller occupies a 2-rack unit space and supports multiple module uplinks.
Cisco Catalyst 9800-40 Wireless Controller	A fixed wireless controller with seamless software updates for mid-size to large enterprises. The controller occupies a 1-rack unit space and provides four 1-GE or 10-GE uplink ports.
Cisco Catalyst 9800-L Wireless Controller	The Cisco Catalyst 9800-L Wireless Controller is the first low-end controller that provides a significant boost in performance and features.
Cisco Catalyst 9800 Wireless Controller for Cloud	A virtual form factor of the Catalyst 9800 Wireless Controller that can be deployed in a private cloud (supports VMware ESXi, Kernel-based Virtual Machine [KVM], Microsoft Hyper-V, and Cisco Enterprise NFV Infrastructure Software [NFVIS] on Enterprise Network Compute System [ENCS] hypervisors), or in the public cloud as Infrastructure as a Service (IaaS) in Amazon Web Services (AWS), Google Cloud Platform (GCP) marketplace, 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 5: Supported Host Environments for Public and Private Cloud

Host Environment	Software Version
VMware ESXi	• VMware ESXi vSphere 6.0, 6.5, 6.7, 7.0, and 8.0 • VMware ESXi vCenter 6.0, 6.5, 6.7, 7.0, and 8.0
KVM	• Linux KVM-based on Red Hat Enterprise Linux 7.6, 7.8, and 8.2 • Ubuntu 16.04.5 LTS, Ubuntu 18.04.5 LTS, Ubuntu 20.04.5 LTS
AWS	AWS EC2 platform
NFVIS	ENCS 3.8.1 and 3.9.1
GCP	GCP marketplace
Microsoft Hyper-V	Windows 2019 Server 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 6: Supported PIDs and Ports

Controller Model	Description
C9800-CL-K9	Cisco Catalyst Wireless Controller as an infrastructure for cloud.
C9800-80-K9	Eight 1/10-Gigabit Ethernet SFP or SFP+ ports and two power supply slots.
C9800-40-K9	Four 1/10-Gigabit Ethernet SFP or SFP+ ports and two power supply slots.
C9800-L-C-K9	• 4x2.5/1-Gigabit ports • 2x10/5/2.5/1-Gigabit ports

Controller Model	Description
C9800-L-F-K9	• 4x2.5/1-Gigabit ports • 2x10/1-Gigabit ports

The following table lists the supported SFP models.

Table 7: Supported SFPs

SFP Name	C9800-80-K9	C9800-40-K9	C9800-L-C-K9	C9800-L-F-K9
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
FINISAR-FTL4C1QL2L	Supported	—	—	—
FINISAR-FTL4C1QE1C	Supported	—	—	—
GLC-BX-D	Supported	Supported	Supported	Supported
GLC-BX-U	Supported	Supported	Supported	Supported
GLC-EX-SMD	Supported	Supported	—	—
GLC-LH-SMD	Supported	Supported	Supported	—
GLC-SX-MMD	Supported	Supported	Supported	Supported
GLC-T	Supported	—	Supported	—
GLC-TE	Supported	Supported	Supported	Supported
GLC-ZX-SMD	Supported	Supported	Supported	Supported
QSFP-100G-LR4-S	Supported	—	—	—
QSFP-100G-SR4-S	Supported	—	—	—
QSFP-40G-BD-RX	Supported	—	—	—
QSFP-40G-CSR-S	Supported	—	—	—

SFP Name	C9800-80-K9	C9800-40-K9	C9800-L-C-K9	C9800-L-F-K9
QSFP-40G-ER4	Supported	—	—	—
QSFP-40G-LR4	Supported	—	—	—
QSFP-40G-LR4-S	Supported	—	—	—
QSFP-40G-SR-BD	Supported	—	—	—
QSFP-40G-SR4	Supported	—	—	—
QSFP-40G-SR4-S	Supported	—	—	—
QSFP-40GE-LR4	Supported	—	—	—
QSFP-H40G-ACU7M	Supported	—	—	—
SFP-10G-AOC10M	Supported	Supported	—	—
SFP-10G-AOC1M	Supported	Supported	—	—
SFP-10G-AOC2M	Supported	Supported	—	—
SFP-10G-AOC3M	Supported	Supported	—	—
SFP-10G-AOC5M	Supported	Supported	—	—
SFP-10G-AOC7M	Supported	Supported	—	—
SFP-10G-ER	Supported	Supported	—	—
SFP-10G-LR	Supported	Supported	—	Supported
SFP-10G-LR-S	Supported	Supported	—	Supported
SFP-10G-LR-X	Supported	Supported	—	Supported
SFP-10G-LRM	Supported	Supported	—	Supported
SFP-10G-SR	Supported	Supported	—	Supported
SFP-10G-SR-S	Supported	Supported	—	Supported
SFP-10G-SR-X	Supported	Supported	—	Supported
SFP-10G-ZR	Supported	Supported	—	—
SFP-H10GB-ACU10M	Supported	Supported	—	Supported
SFP-H10GB-ACU7M	Supported	Supported	—	Supported
SFP-H10GB-CU1.5M	Supported	Supported	—	Supported

SFP Name	C9800-80-K9	C9800-40-K9	C9800-L-C-K9	C9800-L-F-K9
SFP-H10GB-CU1M	Supported	Supported	—	Supported
SFP-H10GB-CU2.5M	Supported	Supported	—	Supported
SFP-H10GB-CU2M	Supported	Supported	—	Supported
SFP-H10GB-CU3M	Supported	Supported	—	Supported
SFP-H10GB-CU5M	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 8: Cisco Catalyst 9800 Series Wireless Controller - Network Protocols and Port Matrix

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

Source	Destination	Protocol	Destination Port	Source Port	Description
Any	Cisco Catalyst 9800 Series Wireless Controller	UDP	161	Any	SNMP Agent
Any	Any	UDP	5353	5353	mDNS
Any	Cisco Catalyst 9800 Series Wireless Controller	UDP	69	69	TFTP
Any	DNS Server	UDP	53	Any	DNS
Any	Cisco Catalyst 9800 Series Wireless Controller	TCP	830	Any	NetConf
Any	Cisco Catalyst 9800 Series Wireless Controller	TCP	443	Any	REST API
Any	WLC Protocol	UDP	1700	Any	Receive CoA packets.
AP	Cisco Catalyst 9800 Series Wireless Controller	UDP	5246	Any	CAPWAP Control
AP	Cisco Catalyst 9800 Series Wireless Controller	UDP	5247	Any	CAPWAP Data
AP	Cisco Catalyst 9800 Series Wireless Controller	UDP	5248	Any	CAPWAP MCAST
AP	Cisco Catalyst Center	UDP	57778	Any	Intelligent capture and RF telemetry
AP	AP	UDP	16670	Any	Client Policies (AP-AP)

Source	Destination	Protocol	Destination Port	Source Port	Description
Cisco Catalyst 9800 Series Wireless Controller	Cisco Catalyst 9800 Series Wireless Controller	UDP	16666	16666	Mobility Control
Cisco Catalyst 9800 Series Wireless Controller	SNMP	UDP	162	Any	SNMP Trap
Cisco Catalyst 9800 Series Wireless Controller	RADIUS	UDP	1812/1645	Any	RADIUS Auth
Cisco Catalyst 9800 Series Wireless Controller	RADIUS	UDP	1813/1646	Any	RADIUS ACCT
Cisco Catalyst 9800 Series Wireless Controller	TACACS+	TCP	49	Any	TACACS+
Cisco Catalyst 9800 Series Wireless Controller	Cisco Catalyst 9800 Series Wireless Controller	UDP	16667	16667	Mobility
Cisco Catalyst 9800 Series Wireless Controller	NTP Server	UDP	123	Any	NTP
Cisco Catalyst 9800 Series Wireless Controller	Syslog Server	UDP	514	Any	SYSLOG
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

Source	Destination	Protocol	Destination Port	Source Port	Description
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 9136 (I) 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 1700 (I) Series Access Point
- Cisco Aironet 1800i Access Point
- Cisco Aironet 2700 (I/E) Series Access Point
- Cisco Aironet 2800 (I/E) Series Access Points
- Cisco Aironet 3700 (I/E/P) Series Access Point
- 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

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.

Table 9: Compatibility Information

Cisco Catalyst 9800 Series Wireless Controller Software	Cisco Identity Services Engine	Cisco Prime Infrastructure	Cisco AireOS-IRCM Interoperability	Cisco Catalyst Center	Cisco Spaces: Connector	Cisco CMX
Dublin 17.12.3	3.2 3.1 3.0 2.7 * all with latest patches	3.10.4 update1 3.10.3	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 8.8.130.0 8.5.176.2 8.5.182.104	See Cisco Catalyst Center Compatibility Information	3, May 2023 2.3.4 2.3.3 2.3.2 2.3.1 See Cisco Spaces Compatibility Matrix	11.0 10.6.3
Dublin 17.12.2	3.2 3.1 3.0 2.7 * all with latest patches	3.10.4 update1 3.10.3	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 8.8.130.0 8.5.176.2 8.5.182.104	See Cisco Catalyst Center Compatibility Information	3, May 2023 2.3.4 2.3.3 2.3.2 2.3.1 See Cisco Spaces Compatibility Matrix	11.0 10.6.3

Cisco Catalyst 9800 Series Wireless Controller Software	Cisco Identity Services Engine	Cisco Prime Infrastructure	Cisco AireOS-IRCM Interoperability	Cisco Catalyst Center	Cisco Spaces: Connector	Cisco CMX
Dublin 17.12.1	3.2 3.1 3.0 2.7 * all with latest patches	3.10.3	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 8.8.130.0 8.5.176.2 8.5.182.104	See Cisco Catalyst Center Compatibility Information	3, May 2023 2.3.4 2.3.3 2.3.2 2.3.1 See Cisco Spaces Compatibility Matrix	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 10: 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:

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

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

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

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

- The Cisco Centralized Key Management (CCKM) feature is deprecated from Cisco IOS XE Dublin 17.10.x.
- 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.

Upgrade Path to Cisco IOS XE Dublin 17.12.x

Table 11: Upgrade Path to Cisco IOS XE Dublin 17.12.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 17.12.x.
16.11.x	—	Upgrade first to 16.12.5 or 17.3.x and then to 17.12.x.
16.12.x	Upgrade first to 17.3.5 or later or 17.6.x or later, and then to 17.12.x.	Upgrade first to 17.3.5 or later or 17.6.x or later, and then to 17.12.x.
17.1.x	Upgrade first to 17.3.5 or later and then to 17.12.x.	Upgrade first to 17.3.5 or later and then to 17.12.x.
17.2.x	Upgrade first to 17.3.5 or later and then to 17.12.x.	Upgrade first to 17.3.5 or later and then to 17.12.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 17.12.x.	Upgrade directly to 17.12.x.
17.3.4c or later	Upgrade directly to 17.12.x.	Upgrade directly to 17.12.x.
17.4.x	Upgrade first to 17.6.x and then to 17.12.x.	Upgrade directly to 17.12.x.
17.5.x	Upgrade first to 17.6.x and then to 17.12.x.	Upgrade directly to 17.12.x.
17.6.x	Upgrade directly to 17.12.x.	Upgrade directly to 17.12.x.
17.7.x	Upgrade directly to 17.12.x.	Upgrade directly to 17.12.x.
17.8.x	Upgrade directly to 17.12.x.	Upgrade directly to 17.12.x.
17.9.x	Upgrade directly to 17.12.x	Upgrade directly to 17.12.x
17.10.x	Upgrade directly to 17.12.x	Upgrade directly to 17.12.x
17.11.x	Upgrade directly to 17.12.x	Upgrade directly to 17.12.x
8.9.x or any version prior to 8.10.171.0	Upgrade first to 8.10.171.0 or later, 17.3.5 or later, or 17.6.x or later, and then to 17.12.x	Upgrade directly to 17.12.x.
8.10.171.0 and above	Upgrade directly to 17.12.x	Upgrade directly to 17.12.x.

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 Dublin 17.12.x
- **Image Names (9800-80, 9800-40, and 9800-L)**:
  - C9800-80-universalk9_wlc.17.12.x.SPA.bin
  - C9800-40-universalk9_wlc.17.12.x.SPA.bin
  - C9800-L-universalk9_wlc.17.12.x.SPA.bin
- **Image Names (9800-CL)**:
  - **Cloud**: C9800-CL-universalk9.17.12.x.SPA.bin
  - **Hyper-V/ESXi/KVM**: C9800-CL-universalk9.17.12.x.iso, C9800-CL-universalk9.17.12.x.ova
  - **KVM**: C9800-CL-universalk9.17.12.x.qcow2
  - **NFVIS**: C9800-CL-universalk9.17.12.x.tar.gz

Software Installation Commands

Cisco IOS XE Dublin 17.12.x	
To install and activate a specified file, and to commit changes to be persistent across reloads, run the following command: **device# install add file** *filename* **[activate |commit]** To separately install, activate, commit, end, or remove the installation file, run the following command: **device# install ?** **Note** We recommend that you use the GUI for installation.	
add file tftp: *filename*	Copies the install file package from a remote location to a device, and performs a compatibility check for the platform and image versions.
activateauto-abort-timer]	Activates the file and reloads the device. The **auto-abort-timer** keyword automatically rolls back image activation.
commit	Makes changes that are persistent over reloads.
rollback to committed	Rolls back the update to the last committed version.
abort	Cancels file activation, and rolls back to the version that was running before the current installation procedure started.
remove	Deletes all unused and inactive software installation files.

Licensing

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

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

Interoperability with Clients

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

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

Table 12: Test Configuration for Interoperability

Hardware or Software Parameter	Hardware or Software Type
Release	Cisco IOS XE Dublin 17.12.x

Hardware or Software Parameter	Hardware or Software Type
Cisco Wireless Controller	See Supported Hardware.
Access Points	See Supported APs.
Radio	• 802.11ax • 802.11ac • 802.11a • 802.11g • 802.11n • 802.11ax in 6GHz (Wi-Fi 6E)
Security	Open, PSK (WPA2-AES), 802.1X (WPA2-AES) (EAP-FAST, EAP-TLS) WPA3 AKM 802.11ax
RADIUS	See Compatibility Matrix, on page 23.
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 13: Client Types

Client Type and Name	Driver or Software Version
Laptops	
Acer Aspire E 15 E5-573-3870 (Qualcomm Atheros QCA9377)	Windows 10 Pro (12.0.0.832)
Apple Macbook Air 11 inch	macOS Sierra 10.12.6
Apple Macbook Air 13 inch	macOS High Sierra 10.13.4
Macbook Pro Retina	macOS Catalina
Macbook Pro Retina 13 inch early 2015	macOS Mojave 10.14.3
Macbook Pro OS X	macOS X 10.8.5
Macbook Air	macOS Sierra v10.12.2
Macbook Air 11 inch	macOS Yosemite 10.10.5
MacBook M1 Chip	macOS Catalina
MacBook M1 Chip	macOS Ventura 13.2.1
MacBook Pro M2 Chip	macOS Ventura 13.3 beta

Client Type and Name	Driver or Software Version
MacBook Pro M2 Chip	macOS Ventura 13.1
MacBook Pro M2 Chip (6Ghz Supported client)	macOS Sonoma 14.0
Dell Inspiron 2020 Chromebook	Chrome OS 75.0.3770.129
Google Pixelbook Go	Chrome OS 97.0.4692.27
HP chromebook 11a	Chrome OS 76.0.3809.136
Samsung Chromebook 4+	Chrome OS 77.0.3865.105
Dell Latitude (Intel AX210)	Windows 11 (22.110.x.x)
Dell Latitude 3480 (Qualcomm DELL wireless 1820)	Win 10 Pro (12.0.0.242)
Dell Inspiron 15-7569 (Intel Dual Band Wireless-AC 3165)	Windows 10 Home (21.40.0)
Dell Latitude E5540 (Intel Dual Band Wireless AC7260)	Windows 7 Professional (21.10.1)
Dell Latitude E5430 (Intel Centrino Advanced-N 6205)	Windows 7 Professional (15.18.0.1)
Dell Latitude E6840 (Broadcom Dell Wireless 1540 802.11 a/g/n)	Windows 7 Professional (6.30.223.215)
Dell XPS 12 v9250 (Intel Dual Band Wireless AC 8260)	Windows 10 Home (21.40.0)
Dell Latitude 5491 (Intel AX200)	Windows 10 Pro (21.20.1.1)
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)
Webex Room Bar Pro	RoomOS 11.5.2.4
Note For clients using Intel wireless cards, we recommend that you to update to the latest Intel wireless drivers if the advertised SSIDs are not visible.	
Tablets	
Apple iPad Pro (12 inch) 6th Gen	iOS 17 (beta)
Apple iPad Pro (12.9 inch) 6th Gen	iOS 16.4

Client Type and Name	Driver or Software Version
Apple iPad Pro (11 inch) 4th Gen	iOS 16.4
Apple iPad 2021	iOS 15.0
Apple iPad 7the Gen 2019	iOS 14.0
Apple iPad MD328LL/A	iOS 9.3.5
Apple iPad 2 MC979LL/A	iOS 11.4.1
Apple iPad Air MD785LL/A	iOS 11.4.1
Apple iPad Air 11 4th Gen	iOS 16.4
Apple iPad Air2 MGLW2LL/A	iOS 10.2.1
Apple iPad Mini 4 9.0.1 MK872LL/A	iOS 11.4.1
Apple iPad Mini 2 ME279LL/A	iOS 11.4.1
Apple iPad Mini 4 9.0.1 MK872LL/A	iOS 11.4.1
Microsoft Surface Pro 3 13 inch (Intel AX201)	Windows 10 (21.40.1.3)
Microsoft Surface Pro 3 15 inch (Qualcomm Atheros QCA61x4A)	Windows 10
Microsoft Surface Pro 7 (Intel AX201)	Windows 10
Microsoft Surface Pro 6 (Marvell Wi-Fi chipset 11ac)	Windows 10
Microsoft Surface Pro X (WCN3998 Wi-Fi Chip)	Windows
Mobile Phones	
Apple iPhone 5	iOS 12.4.1
Apple iPhone 6s	iOS 13.5
Apple iPhone 7 MN8J2LL/A	iOS 11.2.5
Apple iPhone 8	iOS 13.5
Apple iPhone 8 Plus	iOS 14.1
Apple iPhone 8 Plus MQ8D2LL/A	iOS 12.4.1
Apple iPhone X MQA52LL/A	iOS 13.1
Apple iPhone 11	iOS 15.1
Apple iPhone 12	iOS 16.0
Apple iPhone 12 Pro	iOS 15.1
Apple iPhone 13	iOS 15.1
Apple iPhone 13 Mini	iOS 15.1
Apple iPhone 13 Pro	iOS 15.1
Apple iPhone 14 Pro	iOS 17 (beta)

Client Type and Name	Driver or Software Version
Apple iPhone 14	iOS 16.6
Apple iPhone SE MLY12LL/A	iOS 11.3
Apple iPhone SE	iOS 15.1
ASCOM i63	Build v 3.0.0
ASCOM Myco 3	Android 9
Cisco IP Phone 8821	11.0.6 SR4
Cisco CP-840S	Android 10 (Version 16.0.34190)
Cisco CP-860S	Android 10 (Version 16.0.34190)
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
Google Pixel 4	Android 11
Google Pixel 5	Android 11
Google Pixel 6	Android 12
Google Pixel 7	Android 13
Huawei Mate 20 pro	Android 9.0
Huawei P20 Pro	Android 10
Huawei P40	Android 10
LG v40 ThinQ	Android 9.0
One Plus 8	Android 11
Oppo Find X2	Android 10
Redmi K20 Pro	Android 10
Samsung Galaxy S9+ - G965U1	Android 10.0
Samsung Galaxy S10 Plus	Android 11.0
Samsung S10 (SM-G973U1)	Android 11.0
Samsung S10e (SM-G970U1)	Android 11.0
Samsung Galaxy S20 Ultra	Android 10.0

Client Type and Name	Driver or Software Version
Samsung Galaxy S21 Ultra 5G	Android 13.0
Samsung Galaxy S22 Ultra	Android 13.0
Samsung Fold 2	Android 10.0
Samsung Galaxy Z Fold 3	Android 13.0
Samsung Note20	Android 12.0
Samsung G Note 10 Plus	Android 11.0
Samsung Galaxy A01	Android 11.0
Samsung Galaxy A21	Android 10.0
Sony Experia 1 ii	Android 11
Sony Experia	Android 11
Xiaomi Mi 9T	Android 9
Xiaomi Mi 10	Android 11
Spectralink 84 Series	7.5.0.x257
Spectralink 87 Series	Android 5.1.1
Spectralink Versity Phones 92/95/96 Series	Android 10.0
Spectralink Versity Phones 9540 Series	Android 8.1.0
Vocera Badges B3000n	4.3.3.18
Vocera Smart Badges V5000	5.0.6.35
Zebra MC40	Android 4.4.4
Zebra MC40N0	Android 4.1.1
Zebra MC92N0	Android 4.4.4
Zebra MC9090	Windows Mobile 6.1
Zebra MC55A	Windows 6.5
Zebra MC75A	OEM ver 02.37.0001
Zebra TC51	Android 6.0.1
Zebra TC52	Android 10.0
Zebra TC53	Android 11.0
Zebra TC55	Android 8.1.0
Zebra TC57	Android 10.0
Zebra TC58	Android 11.0

Client Type and Name	Driver or Software Version
Zebra TC70	Android 6.1
Zebra TC75	Android 10.0
Zebra TC520K	Android 10.0
Zebra TC8000	Android 4.4.3
Printers	
Zebra QLn320 Mobile Printer	LINK OS 5.2
Zebra ZT230 IndustrialPrinter	LINK OS 6.4
Zebra ZQ310 Mobile Printer	LINK OS 6.4
Zebra ZD410 Industrial Printer	LINK OS 6.4
Zebra ZT410 Desktop Printer	LINK OS 6.2
Zebra ZQ610 Industrial Printer	LINK OS 6.4
Zebra ZQ620 Mobile Printer	LINK OS 6.4
Wireless Module	
Intel AX 411	Driver v22.230.0.8
Intel AX 211	Driver v22.230.0.8, v22.190.0.4
Intel AX 210	Driver v22.230.0.8, v22.190.0.4, v22.170.2.1
Intel AX 200	Driver v22.130.0.5
Intel 11AC	Driver v22.30.0.11
Intel AC 9260	Driver v21.40.0
Intel Dual Band Wireless AC 8260	Driver v19.50.1.6
Samsung S21 Ultra	Driver v20.80.80
QCA WCN6855	Driver v1.0.0.901

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 Dublin 17.12.3

Identifier	Headline
CSCwi99296	Cisco Catalyst 9120 AP encounters multiple kernel unresponsiveness accompanied by AP disconnection from the controller.
CSCwi40659	Clients in the same Remote LAN (RLAN) of different OEAPs cannot communicate with each other.
CSCwj03495	Cisco Aironet 1562 as Mesh AP (MAP) recognizes Cisco Catalyst 9124 Root AP (RAP) as a parent and completes authentication, but fails in the CAPWAP join because Mesh Adjacent messages are undetected by the RAP.
CSCwj05365	Cisco Catalyst 9115 AP encounters a kernel unresponsiveness.
CSCwh63050	Controller sends Internet Group Management Protocol (IGMP) queries without the controller's Internet Protocol (IP) address and Media Access Control (MAC) address.
CSCwi16509	Cisco Aironet 3802 AP disjoins with the error "Invalid radio slot id" and does not reconnect to the controller.
CSCwh52553	Cisco Catalyst 9105 AP encounters high utilization and performance issues due to high Multicast Domain Name System (mDNS) traffic.
CSCwj01916	Cisco Catalyst 9162 APs in FlexConnect mode frequently disconnect from the controller.
CSCvy50798	Cisco Catalyst 9124 AP is not visible in the controller's WebUI even after it is registered.
CSCwj08379	Controller becomes nonoperational when rogue Network-Assurance is enabled.
CSCwi04855	Cisco Catalyst 9115 APs join and disjoin the controller repeatedly with traceback.
CSCwi96176	Cisco Catalyst 9130 and 9166 APs connected to the controller show high channel utilization with one single client connected.
CSCwi91590	Cisco Catalyst 9130 and 9136 APs encounter kernel unresponsiveness due to a free Socket Buffer (skb).
CSCwi95945	Cisco Catalyst 9130 APs stop forwarding router advertisements after 4-6 hours of operation.
CSCwi99437	Clients fail to connect when BSSID is broadcast by Cisco Aironet 1850 APs, but succeed in connecting in the same scenario if it is Cisco Aironet 3800 AP.

Identifier	Headline
CSCwi54064	APs connected to the same controller classify each other as rogue and generate an "AP Impersonation" threat warning.
CSCwj00434	A Cisco Catalyst 2800 AP in Workgroup Bridge (WGB) mode gets stuck after a Dynamic Frequency Channel (DFS) channel change occurs on the controller with CleanAir enabled.
CSCwi56780	Mac Authentication Bypass (MAB) is not initiated unless the client device is deauthenticated.
CSCwi69696	Cisco Aironet 1815 AP encounters random drops in traffic towards wireless clients during normal AP operation.
CSCwj04146	Cisco Aironet 4800 AP does not send traffic over the air when using the 802.1X WLAN.
CSCwi96508	Cisco Wave 2 APs allowing SKC roam cause client deletion with the reason as INVALID_PMKID.
CSCwj32623	Standard power AP is operating on low power in a high density Wi-Fi network.

Open Caveats for Cisco IOS XE Dublin 17.12.2

Caveat ID	Description
CSCwf29762	Controller system not responsive due to null check in mDNS.
CSCwf93063	Intel Wi-Fi 6E AX210 client connection unresponsive after a few minutes of traffic with 1815 AP.
CSCwh18613	The encrypted pre-shared key of a wireless mesh network changes when the **password encryption aes** command is run.
CSCwh20239	Cisco Catalyst 9105 AP experiences WCPd restart when generating core.
CSCwh56147	SNMP OID for AP location tag is missing on the controller.
CSCwh58099	The controller allows the clients to reconnect only after client deletion and CoA termination.
CSCwh59543	Radio FW_1 and CAPWAPd unresponsive during scale longevitiy.
CSCwh63050	The controller is sending Internet Group Management Protocol (IGMP) queries with a non-IP address using MAC address in range of controller MAC addresses.
CSCwh67349	Cisco Aironet 3800 Series AP continuously unresponsive in CAPWAPd.
CSCwh68219	Clients are failing to authenticate via 802.1X using Extensible Authentication Protocol-Transport Layer Security Authentication (EAP-TLS).
CSCwh80060	Cisco 802.11ax APs connected to the controller are losing the Flex WLAN-VLAN mapping.

Caveat ID	Description
CSCwh92459	Controller unresponsive due to process WNCd fault on rp_0_0
CSCwh88100	Cisco Aironet 3800 Series AP : Kernel panic with PC at skb_unlink+0x40/0x54
CSCwh92425	Cisco Catalyst 9136 Series AP does not process power save mode in the 2.4-GHz band.
CSCwe93421	Cisco Catalyst 9115 Series Wi-Fi 6 APs intermittently stops transmitting multicast traffic downstream.
CSCwh29442	Cisco Catalyst 9800-40 Wireless Controller unresponsive after In-Service Software Upgrade (ISSU) upgrade.
CSCwh46368	Cisco Catalyst 9800-40 Wireless Controller device tracking binds BSSID MAC to wired IP address causing reachability issues.
CSCwh49467	AP is leaking multicast traffic to wrong Basic service set identifiers (BSSID).
CSCwh49810	Client loses network access after inter-WNCd roaming.
CSCwh62342	AP does not respond to the query even when the service provider is on its Multicast Domain Name System (mDNS) cache table.
CSCwh67342	Cisco Catalyst 9130AX Series AP is not able to join when Controller-Based Application Recognition (CBAR) is enabled on the controller.
CSCwh68948	Client is not able to get an IP address over fiber link in Cisco Aironet 1562 AP in FlexConnect local switching mode + local DHCP.
CSCwh74415	APs are not working in per client rate limit with FlexConnect local switching.
CSCwh75431	Cisco Aironet 1800 Series APs reporting false high channel utilization causing performance issues across the 5-GHz band.
CSCwh82580	Cisco Catalyst 9120AX Series unresponsive when Cisco Prime Infrastructure turns off 1 SSID via the Schedule SSID availability feature.
CSCwh89539	CAPWAP messages are queued for longer than x seconds with client throttling being turned on.
CSCwh60483	Cisco Catalyst 9136 Series AP shows abnormal temperature readings.
CSCwh49406	Cisco Catalyst 9130AX Series AP are spamming the syslog controllers with thousands of logs per second.
CSCwh95315	Cisco Catalyst IW9167 Heavy Duty Series AP is changing its backhaul upon reload.
CSCwh67285	Controller reboots and causes a switchover in High Availability environments.
CSCwh68360	Cisco Catalyst 9120AX Series: Kernel panic due to wlc_key_set_data.
CSCwh63270	Cisco Catalyst 9130AX Series APs unresponsive due to radio failure.
CSCwh87903	Cisco Catalyst 9120AX Series AP sending authentication response failure for specific client MAC addresses due to suppressed by MAC filter.

Caveat ID	Description
CSCwh81332	When the controller upgrades to 17.6.6, most of the connected APs gets unresponsive.

Open Caveats for Cisco IOS XE Dublin 17.12.1

From this release, the list of caveats is displayed using BST tool. When you click the BST link, it opens a separate window and lists the bugs sorted by severity. You can filter it further using the options in the tool.

Click on the following link to view the Open Caveats: BST Link

Resolved Caveats for Cisco IOS XE Dublin 17.12.3

Identifier	Headline
CSCwf49289	The controller does not have its Secure Unique Device Identifier (SUDI) certificates initialized upon new APP registration.
CSCwh59543	Cisco Catalyst 9120 AP encounters a Radio FW_1 unresponsiveness and Capwapd unresponsiveness during scale longevity.
CSCwh88320	Controller reports false jammer alerts.
CSCwf79175	Pairwise Master Key Identification (PMKID) mismatch between FlexConnect central authentication Wave 2 AP and controller for 802.11X-SHA256 on roaming clients.
CSCwi35946	Cisco Catalyst 9120 AP encounters a kernel unresponsiveness.
CSCwi67013	Cisco Aironet 2800 APs running on the Taiwan domain are unable to send Wi-Fi signals on channels 52, 120, 124 and 128.
CSCwh09642	IP theft was observed due to the zone ID being 0x00000000 after the In Service Software Upgrade (ISSU) process.
CSCwh61007	Controller frequently becomes nonoperational when provisioning multiple APs.
CSCwh14232	Controllers do not send Logical Link Control (LLC) / XID spoofed frames following a mobility event.
CSCwi08442	APs are unable to join when Controller-Based Application Recognition (CBAR) is enabled on the controller.
CSCwi22270	Cisco Catalyst 9120 AP encounters a radio unresponsiveness during longevity run.
CSCwi69042	Cisco Aironet 1562 Mesh AP (MAP) is unable to join the network through the Root AP (RAP) using the Extensible Authentication Protocol (EAP) and the Flex+Bridge site tag.
CSCwf78066	Catalyst Center heat map displays the message "No radios in the selected band" for APs managed by the controller.
CSCwh68768	Controller in the public cloud fails to create a FlexConnect WLAN using Basic Wireless Setup.

Identifier	Headline
CSCwh63270	Cisco Catalyst 9130AXI APs joined to controller frequently become nonoperational due to radio failure.
CSCwf84639	Cisco Catalyst 9120 AP Dual Band (XOR) radio mode is not updated in the radio_oper_data database.
CSCwi07094	Apple Client cannot connect to the FlexConnect WPA2+WPA3 SSID when Secure Agile Exchange (SAE) is enabled and Opportunistic Key Caching (OKC) is disabled.
CSCwh91254	PHY High Txpower issue on Broadcom (BCM) APs causes increased coverage and clients are unable to authenticate.
CSCwh20334	Controller's Change of Authorization (CoA) server key appears blank in the GUI.
CSCwh49406	Cisco Catalyst 9130 series AP spams syslog controllers with thousands of CleanAir logs per second.
CSCwh95315	Cisco Catalyst IW9167E Heavy Duty AP changes its backhaul upon reload.
CSCwh60483	Cisco Catalyst 9136I AP shows incorrect temperature readings.
CSCwf96138	Roaming issues observed in iPhone SE 3rd generation.
CSCwi34051	The Cisco Aironet 2800 AP randomly encountered FIQ/NMI resets; PC at wl_get_staid_info.
CSCwh81332	Cisco Catalyst 9130 APs encountered kernel unresponsiveness after upgrade to Cisco IOS XE Bengaluru 17.6.6.
CSCwf92100	Embedded Wireless Controller: Preferred active configuration is lost after CAPWAP AP configuration update in WebUI.
CSCwi28174	Layer 3 multicast packets are sent on native VLAN when VLAN ID 1 is selected on policy profile with AAA override.
CSCwh12481	Cisco Catalyst 9130AXI and 9130AXE AP unable to join the controller when only TZ (Tanzania) country code is configured.
CSCwi03442	Cisco Catalyst 9130 APs does not honor unscheduled automatic power save delivery (U-APSD) trigger frame, which causes RTP stream disruption.
CSCwh30078	Cisco Wave 2 AP becomes nonoperational in throughput testing.
CSCwh33056	Policy tag description is blank after deleting WLAN location entries.
CSCwi19481	Cisco Catalyst 9130 AP in FlexConnect mode stops forwarding router advertisements after 4-6 hours of uptime.
CSCwh88100	Cisco Aironet 3800 AP becomes nonoperational due to kernel panic with PC at skb_unlink+0x40/0x54.
CSCwh37783	Controller Lobby Admin page is unable to load.

Identifier	Headline
CSCwf88890	GUI is stuck on loading in Monitoring > Wireless > AP Statistics > General for Cisco Aironet 3800 AP.
CSCwf87281	NULL Timer causes segmentation fault in the controller.
CSCwh74415	Per client rate limit is not working for FlexConnect local switching APs.
CSCwf54827	Uptime in Acct-Session-Time is high after idle timeout.
CSCwh87903	Cisco Catalyst 9120 AP sends authorization response failures for specific MAC addresses due to "suppressed by MAC filter".
CSCwf93747	Controller WebUI does not load policy profile page when large number of WLANs are configured.
CSCwf60519	Client is unable to connect due to invalid PMKID after an 802.11r reauthentication failure.
CSCwi42112	MAC address of wired clients are being learned from the Cisco Catalyst 9124 MAP port.
CSCwi19804	Cisco Catalyst 9105, 9115, 9120 AP radio are misconfigured after AP reload when admin state is down.
CSCwh76420	Controller becomes nonoperational while performing ISSU upgrade.
CSCwh75431	Cisco Aironet 1830, 1850 APs report false utilization affecting performance on 5 GHz.
CSCwi64652	802.11ax APs do not reset Bluetooth Low Energy (BLE) interface after 100 attempts.
CSCwi52692	Cisco Catalyst 9130 AP signals Universal PoE spare pair to turn off Type-Length-Value (TLV) fields in Cisco Discovery Protocol.
CSCwi49666	Cisco Catalyst 9136 AP environmental sensors are reporting incorrect ambient temperature.
CSCwh62342	FlexConnect AP as an mDNS gateway responds incorrectly when Location Specefic Services (LSS) filter is enabled in 5GHz-band.
CSCwh31966	Controller becomes nonoperational on WNCd process during database termination.
CSCwh44793	Cisco Catalyst 9130 AP on Cisco IOS XE Amsterdam 17.3.6 fails to join with error to set FT data in BSSID after site-tag is changed on the controller.
CSCwi11038	Cisco Catalyst 9115 OEAP experiences kernel unresponsiveness.
CSCwi35699	Cisco Catalyst 9120 AP detects its own BSSID as malicious after channel resets.
CSCwi06055	Cisco Industrial Wireless 3702 AP radios reset and stay down when board temperature is less than –20° C.
CSCwi05672	Wireless Driver is unable to decrypt ICAP packets in Cisco Catalyst 9130 AP.
CSCwf86242	Controller experiences unexpected reload with CAPWAP window size set to 0.

Identifier	Headline
CSCwi04705	Controller is not sending gARP broadcast announcements on behalf of the client on inter-controller roaming events.
CSCwf75646	Controller MIB update is required to include all coded integer values for cRFStatusLastSwactReasonCode.
CSCwh42002	Controller becomes nonoperational while processing CAPWAP data and generates WNCd core file.
CSCwf90646	Controller sends CAPWAP payload for DOT11R_WLC_MAC_IP_PAYLOAD as two packets with the same sequence number of 2 but there is no information about fragmentation or offset.
CSCwi38791	Cisco Catalyst 1850 AP becomes nonoperational due to kernel panic in Cisco IOS XE Dublin 17.11.

Resolved Caveats for Cisco IOS XE Dublin 17.12.2

This release provides a critical fix for a security vulnerability. See the following table for information.

Caveat ID	Description
CSCwh87343	Cisco IOS XE Software Web UI Privilege Escalation Vulnerability For more information, see Security Advisory: cisco-sa-iosxe-webui-privesc-j22SaA4z.
CSCwf14400	Cisco Catalyst 9166 AP: CAPWAP down/up during Dual Band operation changes between 5 GHz and 6 GHz.
CSCwf60151	Memory leak at kernel level with PUBd process triggering unexpected reloads on the controllers.
CSCwe11213	Cisco Catalyst 9130AX Series AP unresponsive due to radio failure.
CSCwf79458	802.11ax workgroup bridge (WGB) 2.4-GHz radio does not roam with 802.11r enabled.
CSCwh20306	Cisco Catalyst AP hyperlocation breaks when Adaptive Wireless Intrusion Prevention System (wIPS) is enabled.
CSCwf83278	Client traffic unresponsive with N+1 when AP sends CLIENT_DEL_STOP_REASSOC.
CSCwh08532	Differentiated Services Code Point (DSCP) marking on Cisco Catalyst AP for QoS metal policies not happening in slow path and fast path.
CSCwh20301	No telemetry data transfer from controller to Cisco Catalyst Center.
CSCwf53520	Kernel panic unresponsive when Cisco Aironet 1815 Series AP is running version 17.9.2.
CSCwh22038	Functional The Cisco Catalyst 9162 Series AP Radio1 unresponsive on 17.12.1.5
CSCwh42002	Controller unresponsive with WNCd core while processing CAPWAP data.

Caveat ID	Description
CSCwh61011	AP stops processing downstream frames after CAPWAP restart.
CSCwf59348	Beacon set Max Transmit Power Level to 128 dBm in Country IE, which happens in some 5G channels.
CSCwf63818	Cisco Aironet 1830 Series AP running version 17.9.2 is unresponsive due to kernel panic.
CSCwf93992	Cisco Aironet 2800 APs in FlexConnect mode are not processingExtensible Authentication Protocol-Transport Layer Security Authentication (EAP-TLS) fragmented packets if delay is more than 50 ms.
CSCwf99932	Functional Cisco Catalyst 9120 AP Radio1unresponsive on ap-17.12.0.116.
CSCwh09879	Clients are not able to connect to FlexConnect APs after country code change.
CSCwh20934	Systemd critical process not working when joining the Cisco Catalyst 9800-CL running 17.9.3
CSCwh54279	Cisco Aironet 1815 Series OEAP running 17.9.4 is unresponsive due to kernel panic.
CSCwh74663	Clients are stuck in authenticating or in IP learn for open SSIDs.
CSCwh81040	Cisco Catalyst 9120 AP in local mode is unresponsive when WGB associates with the SSID profile.
CSCwf87904	The Cisco Catalyst 9164 Series AP unresponsive on [<ffffffbffd6524e0>] cisco_wlan_crypto_decap+0x2a8/0x518 [umac](SF06713784)
CSCwh26854	Cisco Catalyst 9166 and 9162 APs adaptive 802.11r roam fails in Apple clients.
CSCwh54762	AP kernel panic due to not syncing.
CSCwf53331	Cisco Catalyst 9124 AP: Kernel panic observed after changing channel on the 5-GHz in Bridge mode.
CSCwf85025	The transmission power in Cisco Catalyst 9166-ROW GB decreases when there is a channel change.
CSCwh06834	Using special characters in the password while generating TP generates an invalid TP.
CSCwh08625	AP is unresponsive due to kernel panic with low PC and LR values.
CSCwh18759	Cisco Aironet 1815 Series AP unresponsive due to system memory running low and kernel panic; not syncing.
CSCwf13804	netlink_socket_receive multicast_group 1 return failure: No buffer space available errors are seen.
CSCwf52815	Cisco AP should improve Path Maximum Transmission Unit (PMTU) to be able to honor the ICMP unreachable MTU value.
CSCwf62051	Cisco Aironet 1815w AP unresponsive due to kernel panic.

Caveat ID	Description
CSCwf90014	Issues with Cisco Intelligent Capture (iCAP) on IPv6 cluster.
CSCwf44321	Interferers on Connected Mobile Experiences won't be displayed, although they are shown on the controller for 2.4 and 5 GHz.
CSCwf61881	AP is randomly moving from US -> UX domain and unable to set it to standard power.
CSCwf86242	Cisco 9800 Wireless Controller unexpectedly reloads with CAPWAP window size set to 0.
CSCwh61007	Controller constantly being unresponsive whenever it provisions multiple APs.
CSCwf29742	Cisco Catalyst 9120 AP: Firmware unresponsive while running multicast & longeivity with 80+ clients
CSCwh33190	Cisco Catalyst 9115 Series Wi-Fi 6 AP unresponsive due to kernel panic.
CSCwf07384	Wired client behind Cisco Catalyst 9105 Series RLAN is not able to pass traffic.
CSCwf68131	The Cisco Catalyst Series 9105AXW AP faces bad block monitoring after upgrading the software.
CSCwf95868	Single Band BCM WGB Radio 0 Tx power decreases by nearly 20 dBm while configuring antenna number.
CSCwh13494	Cisco Catalyst 9136 Series APs in -F regulatory domain are beaconing at a lower power.
CSCwf83292	Cisco Catalyst 9130 Series AP receives DHCP offer and ACK at the wired Ethernet port, but does not send it over the radio interface to the client.
CSCwf90114	Stale entries remain for APs no longer connected to system.
CSCwh59420	Cisco Catalyst 9136 Series APs unresponsive on Cisco IOS XE Cupertino 17.9.x
CSCwh76420	A controller may get unresponsive within WNCd service when performing an ISSU upgrade from Cisco IOS XE Bengaluru 17.6.xreleases to Cisco IOS XE Cupertino 17.9.x releases.
CSCwf81866	Radio 0 WGB configuration is not backed up correctly when doing a TFTP backup of the configuration.
CSCwf65794	Cisco 1852 AP reloads unexpectedly due to radio failure.
CSCwf78066	Cisco Catalyst Center users might see a "No radios in the selected band" message on the floor maps and the AP icons might start showing up as white circles instead of the normal AP icons.
CSCwh29924	Cisco Catalyst 9105 APs, Cisco Catalyst 9115 APs, or Cisco Catalyst 9120 APs WGB: Antenna-a couldn't function properly if configuration is ab-antenna.
CSCwf12301	The retries number is always 0 for [QCA 12.0] WCPD TX.

Caveat ID	Description
CSCwf10839	A large amount of Virtual Router Redundancy Protocol (VRRP) traffic causes the switch port to be down due to storm-control action configuration.
CSCwe24263	Cisco Catalyst 9130 Series AP: Inconsistent Tx power levels advertised in beacons.
CSCwh30996	The Bluetooth Low Energy Power Distribution Unit used in dual mode for iBeacon with PDU type is adv_discover_ind vs the one used in tx only mode for vibeacon is adv_non_connectable_ind.
CSCwf91445	Controller pushes accounting information for pre-shared key (PSK) Local Auth WLANs.
CSCwf94863	Cisco Catalyst 9115 Series Wi-Fi 6 AP unexpectedly reboots due to kernel panic.
CSCwf64009	Cisco Aironet 1815 Series AP leaking RLAN VLAN traffic with looped port.
CSCwf98534	Geolocation reported by Global Navigation Satellite System(GNSS) module does not take into account external GPS antenna cable length in the computation of the ellipse uncertainty region.
CSCwh09676	Wireless Control Protocol (WCP) Dynamic Memory Allocation unfree logs missing and dmalloc files not updated periodically.
CSCwh27366	AP radio firmware failure reset code 2 with failure signature GDP.
CSCwh27425	Cisco Catalyst 9115AX Series AP does not forward a part of CAPWAP data packets to the uplink direction.
CSCwf13107	Radio being unresponsive during longevity test with Cisco Catalyst 9105 Series AP.
CSCwh35072	Cisco Aironet 3800 Series AP reloads unexpectedly due to FIQ/NMI reset.
CSCwh45418	Cisco Catalyst 9124 Series AP is sending incorrect duplex information via Cisco Discovery Protocol (CDP).
CSCwh50681	New SSID arp0v0 being broadcast after Cisco IOS XE Cupertino 17.9.3 wireless upgrade.
CSCwf68612	Controller may reload unexpectedly, generating a system-report containing a core file for the WNCd process.
CSCwf99906	Network Time Protocol (NTP) authentication removed after reload using more than 16 bytes.
CSCwh11858	When removing an Fully qualified domain name (FQDN) ACL from the switch, the device unexpectedly reloads, the ACL is not deleted after the reload.
CSCwf21390	Duplicate Access-Request messages with Cisco Trusted Security (CTS) client username when more than one RADIUS server is configured.
CSCwf36752	Using template from Cisco Catalyst Center or using copy-paste with a specific configuration for first time, the TACACS+ encryption fails.

Caveat ID	Description
CSCwf66661	Web UI page renders the page slowly while accessing device_type contents.

Resolved Caveats for Cisco IOS XE Dublin 17.12.1

From this release, the list of caveats is displayed using BST tool. When you click the BST link, it opens a separate window and lists the bugs sorted by severity. You can filter it further using the options in the tool.

Click on the following link to view the Resolved Caveats: BST Link

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 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 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.