Release Notes for Cisco Catalyst 9800 Series Wireless Controller, Cisco IOS XE Dublin 17.10.x

First Published: 2022-11-30

Release Notes for Cisco Catalyst 9800 Series Wireless Controller, Cisco IOS XE Dublin 17.10.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 Dublin 17.10.1

Table 1: New and Modified Software Features

Feature Name	Description and Documentation Link
Application Performance Monitoring (Includes FlexConnect and Fabric Modes)	This feature collects and exports assurance-related metrics (per application) of the flows forwarded through the corresponding AP to the Cisco DNA Centre Assurance application. For more information, see the Chapter Application Performance Monitoring.
AP Power Distribution	The AP Power Distribution feature helps APs such as the Cisco Catalyst 9130 Series APs and Cisco Catalyst 9136 Series APs, to operate as 4x4 + 4x4 + USB on PoE+. The APs can reallocate the extra AP power to different radios while operating on PoE+ (30W). For example, to balance the power budget across 2.4-GHz, 5-GHz, and 6-GHz, disable 2.4-GHz to allow optimal 6-GHz operation. This feature has been enhanced to support the following: • Radio spatial streams • Flexible PoE profiles The following command is introduced: • **radio spatial-stream** For more information, see the Chapter AP Power Save.

Feature Name	Description and Documentation Link
Cisco DNA Center Client Event and SSID Telemetry Filter	This feature filters out telemetry data for a configured SSID on the controller and the corresponding AP. The following command is introduced: • **icap subscription client exclude telemetry-data wlan** For more information, see the Chapter Streaming Telemetry.
CleanAir Support for 6 GHz	From this release, CleanAir is supported in the 6-GHz band radio of the corresponding AP. For more information, see the Chapter Cisco CleanAir.
Device Classifier Dynamic XML Support	This feature enables better device classification without upgrading the device to a new release. For more information, see the Chapter Device Classifier Dynamic XML Support.
Device Ecosystem Data	This feature sends the device analytics data that is present in the RADIUS accounting request to Cisco ISE in order to profile endpoints. The following command is introduced: • **dot11-tlv-accounting** For more information, see the Chapter RADIUS Accounting.

Feature Name	Description and Documentation Link
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. See Cisco Catalyst 9800 Series Wireless Controller Command Reference → **pae**. Additional information on this feature can be found here .
DNS or DHCP or AAA Server Reachability Through IPSLA and Failure Reasons for DHCP	This feature introduces additional parameters to capture the DHCP server failures in client events and send them to Cisco DNA Center for meaningful insights into the network and to take proactive actions on network issues to improve reliability, high availability, and performance.
Downloadable ACL (Central Switching Only)	The Downloadable ACL (dACL) feature defines and updates ACLs in one place (Cisco ISE) and allows ACL download to all the applicable controllers. For more information, see the Chapter Downloadable ACL (dACL).

Feature Name	Description and Documentation Link
Factory Reset (with Data Wipe)	Factory reset will not only erase the configuration but also removes all the customer-specific data that has been added to the device since the time of its shipping. The erased data covers configurations, log files, boot variables, core files, and credentials such as FIPS-related keys. For more information, see the Hardware Installation Guides of the Cisco Catalyst 9800 Series Wireless Controllers.
New SFP Support on Cisco Catalyst 9800-80 Wireless Controllers	The following SFPs are supported from this release: • COLORCHIP-C040-Q020-CWDM4-03B • FINISAR-FTL4C1QL2L • FINISAR-FTL4C1QE1C • QSFP-40G-CSR-S • QSFP-40G-SR-BD • QSFP-H40G-ACU7M • QSFP-H40G-ACU10M
Site Load Balancing	The Load Balancing feature is enhanced to specify a site load for better load balancing. The following command is introduced: • **load** For more information, see the Chapter Enhanced Site Tag-Based Load Balancing.
Support for 4 FNF Monitors	From Cisco IOS XE Dublin 17.10.1, you can configure up to four flow monitors (from the earlier limit of two flow monitors) in a policy profile per direction (input and output) in local mode. The additional flow monitors help to collect DNS traffic statistics and send them to Cisco DNA Center to analyse and take corrective actions.
Upgrade YANG Models to YANG 1.1	Cisco-defined YANG models are in YANG Version 1.1 in Cisco IOS XE Dublin 17.10.1 and later releases.
Workgroup Bridge Mode on Cisco Catalyst 9124 and 9130 Series Access Points	Workgroup Bridge Mode mode is supported on the following APs: • Cisco Catalyst 9124 Series Access Points • Cisco Catalyst 9130 Series Access Points

Table 2: New and Modified GUI Features

Feature Name	GUI Path
AP Power Save	• **Configuration > Tags & Profiles > Power Profile**
CleanAir Support for 6 GHz	• **Monitoring >Wireless > CleanAir Statistics** • **Configuration > Radio Configurations > CleanAir**

MIBs

The following MIB is newly added or modified:

- CISCO-LWAPP-AP-MIB
- CISCO-LWAPP-SI-MIB

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 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.
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.
C9800-40-K9	Four 1/10-Gigabit Ethernet SFP or SFP+ ports and two power supply slots.
C9800-L-C-K9	• 4x2.5/1-Gigabit ports • 2x10/5/2.5/1-Gigabit ports
C9800-L-F-K9	• 4x2.5/1-Gigabit ports • 2x10/1-Gigabit ports

The following table lists the supported SFP models.

Table 6: 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	—	—	—
QSFP-40G-ER4	Supported	—	—	—
QSFP-40G-LR4	Supported	—	—	—
QSFP-40G-LR4-S	Supported	—	—	—

SFP Name	C9800-80-K9	C9800-40-K9	C9800-L-C-K9	C9800-L-F-K9
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-H10GB-CU1M	Supported	Supported	—	Supported
SFP-H10GB-CU2.5M	Supported	Supported	—	Supported
SFP-H10GB-CU2M	Supported	Supported	—	Supported

SFP Name	C9800-80-K9	C9800-40-K9	C9800-L-C-K9	C9800-L-F-K9
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/c/en/us/support/interfaces-modules/transceiver-modules/products-device-support-tables-list.html

Network Protocols and Port Matrix

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

Source	Destination	Protocol	Destination Port	Source Port	Description
Any	Cisco Catalyst 9800 Series Wireless Controller	TCP	22	Any	SSH
Any	Cisco Catalyst 9800 Series Wireless Controller	TCP	23	Any	Telnet
Any	Cisco Catalyst 9800 Series Wireless Controller	TCP	80	Any	HTTP
Any	Cisco Catalyst 9800 Series Wireless Controller	TCP	443	Any	HTTPS
Any	Cisco Catalyst 9800 Series Wireless Controller	UDP	161	Any	SNMP Agent
Any	Any	UDP	5353	5353	mDNS

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

Source	Destination	Protocol	Destination Port	Source Port	Description
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
Cisco Catalyst Center	Cisco Catalyst 9800 Series Wireless Controller	TCP	32222	Any	Device Discovery
Cisco Catalyst Center	Cisco Catalyst 9800 Series Wireless Controller	TCP	25103	Any	Telemetry Subscriptions

Important Notes

- To migrate public IP address from 16.12.x to 17.x. ensure that you configure the **service internal** command. If you do not configure the **service internal** command, the IP address does not carry forward.
- The Cisco Aironet 2800 and 3800 APs do not reset an interface (to clear any Ethernet interface physical layer issues) if the Dynamic Host Configuration Protocol (DHCP) does not resolve the IP address within a certain duration.

Supported APs

The following Cisco APs are supported in this release.

Indoor Access Points

- Cisco Catalyst 9105AX (I/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) Series Access Points
- Cisco Aironet 1815 (I/W), 1830 (I), 1840 (I), and 1850 (I/E) Access Points
- Cisco Aironet 2800 (I/E) Series Access Points
- Cisco Aironet 3800 (I/E/P) Series Access Points
- Cisco Aironet 4800 Series Access Points

Outdoor Access Points

- Cisco Aironet 1540 Series Access Points
- Cisco Aironet 1560 Series Access Points
- Cisco 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 Industrial Wireless 9167 (E) Heavy Duty Access Point

Integrated Access Points

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

Network Sensor

- Cisco Aironet 1800s Active Sensor

Pluggable Modules

- 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 8: Compatibility Information

Cisco Catalyst 9800 Series Wireless Controller Software	Cisco Identity Services Engine	Cisco Prime Infrastructure	Cisco AireOS-IRCM Interoperability	Cisco Catalyst Center	Cisco CMX
Dublin 17.10.1	3.0 2.7 2.6 2.4	3.10.2	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	11.0 10.6.3

GUI System Requirements

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

Table 9: Hardware Requirements

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

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

Software Requirements

Operating Systems:

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

Browsers:

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

Note Firefox Version 63.x is not supported.

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

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

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

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

Before You Upgrade

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

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

  Workaround:

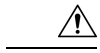
  - Upgrade using the CLI commands, or,
  - Upgrade to a fixed release first, and then upgrade to 17.15.x.

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

  Workaround:

  - Reboot the impacted APs through the power cycle.

  For more information, see CSCwm08044



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

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

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

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

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

Note

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

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

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

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

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

     ```
     Device# capwap ap restart
     ```

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

- If the *Cisco-IOS-XE-wireless-access-point-oper* shows country operator as **ZZ**, the information is specific for countries supporting multiple regulatory domains. These records should only be accessed and referred to by such countries. For country-specific information, refer to the respective record using the country code.

- The following Remote Procedure Calls (RPCs) should be used for Cisco Catalyst 9800 Series Wireless Controller and Cisco Embedded Wireless Controller:
  - Cisco Catalyst 9800 Series Wireless Controller: Use **ewlc-wncd-stats** within *Cisco-IOS-XE-wireless-ap-global-oper*.
  - Cisco Embedded Wireless Controller: Use **ewlc-wncd-stats** within *Cisco-IOS-XE-wireless-access-point-oper*.
- 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).
- 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 was deprecated in Cisco IOS XE 17.10.x, but currently remains supported. However, support for CCKM will be removed in a future release. Therefore, we recommend that you migrate to Fast Transition (FT) with 802.1X authentication and validate the configuration with supported key caching mechanisms.
- To migrate public IP address from 16.12.x to 17.x. ensure that you configure the **service internal** command. If you do not configure the **service internal** command, the IP address does not get carried forward.
- RLAN support with Virtual Routing and Forwarding (VRF) is not available.
- When you encounter the SNMP error *SNMP_ERRORSTATUS_NOACCESS 6*, it means that the specified SNMP variable is not accessible.
- We recommend that you perform a controller reload whenever there is a change in the controller's clock time to reflect an earlier time.

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

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

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

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

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

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

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

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

Upgrade Path to Cisco IOS XE Dublin 17.10.x

Table 10: Upgrade Path to Cisco IOS XE Dublin 17.10.x

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

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

Upgrading the Controller Software

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

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 Dublin 17.10.x
- **Image Names (9800-80, 9800-40, and 9800-L)**:
  - C9800-80-universalk9_wlc.17.10.x.SPA.bin
  - C9800-40-universalk9_wlc.17.10.x.SPA.bin
  - C9800-L-universalk9_wlc.17.10.x.SPA.bin
- **Image Names (9800-CL)**:
  - **Cloud**: C9800-CL-universalk9.17.10.x.SPA.bin
  - **Hyper-V/ESXi/KVM**: C9800-CL-universalk9.17.10.x.iso, C9800-CL-universalk9.17.10.x.ova
  - **KVM**: C9800-CL-universalk9.17.10.x.qcow2
  - **NFVIS**: C9800-CL-universalk9.17.10.x.tar.gz

Software Installation Commands

Cisco IOS XE Dublin 17.10.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.

Cisco IOS XE Dublin 17.10.x	
add file tftp: *filename*	Copies the install file package from a remote location to a device, and performs a compatibility check for the platform and image versions.
activateauto-abort-timer]	Activates the file and reloads the device. The **auto-abort-timer** keyword automatically rolls back image activation.
commit	Makes changes that are persistent over reloads.
rollback to committed	Rolls back the update to the last committed version.
abort	Cancels file activation, and rolls back to the version that was running before the current installation procedure started.
remove	Deletes all unused and inactive software installation files.

Licensing

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

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

Interoperability with Clients

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

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

Table 11: Test Configuration for Interoperability

Hardware or Software Parameter	Hardware or Software Type
Release	Cisco IOS XE Dublin 17.10.x
Cisco Wireless Controller	See Supported Hardware, on page 7.
Access Points	See Supported APs, on page 14

Hardware or Software Parameter	Hardware or Software Type
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 15.
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
HP chromebook 11a	Chrome OS 76.0.3809.136
Samsung Chromebook 4+	Chrome OS 77.0.3865.105

Client Type and Name	Driver or Software Version
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
Apple iPad Mini 2 ME279LL/A	iOS 11.4.1
Apple iPad Mini 4 9.0.1 MK872LL/A	iOS 11.4.1

Client Type and Name	Driver or Software Version
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
Google Pixel 4	Android 11
Google Pixel 5	Android 11

Client Type and Name	Driver or Software Version
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
Vocera Badges B3000n	4.3.3.18
Vocera Smart Badges V5000	5.0.6.35
Zebra MC40	Android 4.4.4

Client Type and Name	Driver or Software Version
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 Dublin 17.10.1

Caveat ID	Description
CSCwb23886	Cisco AireOS 1810W AP: RLAN DHCP issues are observed.
CSCwb51757	High channel utilization is observed on 5GHz radio with 40MHz.
CSCwc32182	Cisco AireOS 1852 AP: Radio firmware crash is observed.
CSCwc54370	A controller in HA is not sending gratuitous ARPs (GARPs) after it rejojns HA pair from standalone due to no RP or uplink.
CSCwc74020	Allow more than eight IPv6 addresses, per wireless client.
CSCwc89183	Controller crash is observed (on libewlc_client_dpath_svc.so).
CSCwc97199	Re-association request processing is delayed between the driver and wcp.
CSCwc99359	Rogue rule delete classification configuration is not working.
CSCwd02898	Cisco Catalyst 9300 Series Switch is not flushing remote MAC address after roaming to a local AP.
CSCwd03803	Cisco AireOS 1815I AP is rebooting (PC is at edma_poll / LR is at dma_cache_maint_page).
CSCwd04025	APs associated with the controller are showing interface "*Half duplex*".
CSCwd04571	Memory leak is observed (in wncd process) when under load.

Caveat ID	Description
CSCwd05689	Cisco Catalyst 9124AXI AP: RSSI is 7-8dbm weaker at a distance compared to other AP models.
CSCwd06018	802.11r reauthentication failed due to '*Invalid PMKID*' while doing inter-WNCD roaming.
CSCwd06122	AP join issues are observed due to stale client entries.
CSCwd10570	Cisco Catalyst 9130 AP: Beacon is showing incorrect datarates - different rates for same slot on different BSSIDs.
CSCwd12120	Inject path crash on controller switch on IPv6 QoS.
CSCwd12754	CAPWAP wireless traffic is getting the same Security Group Tag (SGT) tag as the corresponding incoming wired traffic.
CSCwd21996	Cisco Catalyst 9120 AP: CleanAir sensor is crashing.
CSCwd23681	Controller fails to update AP config with error "*% Error: no ap_name exists*".
CSCwd25931	Wireless client is not receiving IPv6 RA from wired - FlexConnect Local DHCP.
CSCwd26693	N+1 HA for FlexConnect is not working as expected.
CSCwd30828	Cisco Catalyst 9120 AP: Kernel panic crash is observed.
CSCwd32107	Cisco AireOS 2700 AP: AP_LAN_CONFIG payload is having invalid RLAN port enable value.
CSCwd32900	AP is dropping Extensible Authentication Protocol over LAN (EAPOL) message 4 during 4-way handshake.
CSCwd33981	Kernel panic crash with PC (at cpuidle_not_available).
CSCwd34890	Clients are getting deauthenticated imediately after getting IP address in LWA + Local Switching + Central Authentication scenario.
CSCwd35577	Redundancy fails due to double bit error correction code (ECC).
CSCwd36552	Cisco Catalyst 9120 AP: Kernel panic crash is observed.
CSCwd37706	Cisco Catalyst 9130 AP doesn't respond to reassociation request during client roaming.
CSCwd39599	Cisco Catalyst 9117 AP reloads unexpectedly with PC (at dst_release+0x18/0x90).
CSCwd39606	Cisco Catalyst 9117 AP reloads unexpectedly due to kernel panic (at dp_rx_wbm_err_process).

Caveat ID	Description
CSCwd40731	AP reloads due to kernel panic.
CSCwd40914	Cisco Catalyst 9120 AP is not forwarding EAP packet downstream to client.
CSCwd41108	Cisco Catalyst 9130AXE AP: Dart connectors are stuck at channel 36.
CSCwd41463	Cisco AireOS 3800 and 4800 APs are not sending Internet Group Management Protocol (IGMP) membership report.
CSCwd45079	FlexConnect AP performs Extensible Authentication Protocol (EAP) identity request after completing 4-way handshake.
CSCwd45536	AP is sending ARP broadcast to wireless clients when P2P blocking action is enabled.
CSCwd46091	Cisco Catalyst 9105AXI AP is requesting 30 watts of power, instead of 15.4 watts.
CSCwd46252	Controller shows AP as having no neighbors. This issue is caused when power level is set to maximum.
CSCwd46721	IP theft is observed due to client stale entry in Object Document Mapping (ODM) database.
CSCwd46815	EAP-TLS is failing for the wired clients behind MAP for the 2800/3800/4800/1562/6300 series APs.
CSCwd47286	Capability annotation is missing for some xpaths in yaml files.
CSCwd47741	Controller is failing to update Dynamic Channel Assignment (DCA) channels.
CSCwd49166	Cisco AireOS 3800 AP is consistently reporting high QoS Basic Set Service (QBSS) load.
CSCwd49686	AP doesnt not save syslog message before crash.
CSCwd49861	AIRESPACE-WIRELESS-MIB: bsnAPIfType OID documentation is incomplete.
CSCwd51523	Cisco Catalyst 9120 AP: Numerous power supply module (PSM) watchdog crashes are observed.
CSCwd52938	Wired clients behind a workgroup bridge (WGB) are not getting IP address in anchor WLAN.
CSCwd53025	Cisco Catalyst 9800-CL controller Self-signed Certificate (SSC) configuration command fails.
CSCwm95849	Cisco Catalyst 9136 AP does not receive the 6e SSID

Resolved Caveats for Cisco IOS XE Dublin 17.10.1

Caveat ID	Description
CSCwa79968	SNMP MIB is not fetching all that data or no data at all for SNMP walk with high client count.
CSCwb37457	Standby controller crashes when it is configured in RMI+RP HA mode with wired guest feature.
CSCwb43548	Disable ip proxy-arp by default.
CSCwb47040	Controller is not updating RFID location properly.
CSCwb52755	Apple and Android fast transition capable client is unable to authenticate with Identity Preshared Key (iPSK) profile.
CSCwb58100	Unable to map SSID with spaces in it on an attribute list.
CSCwb64761	Controller is discarding location updates from RFID tags.
CSCwb67450	Add **show process cpu platform sorted** command is needed in **show tech wireless** command group.
CSCwb69531	Controller initiates Extensible Authentication Protocol over LAN (EAPOL) retries for the client in RUN state.
CSCwb73461	Radio Resource Management (RRM) core generated @ group_dpc_compute_6GHz.
CSCwb78191	AAA VLAN override is not working in iPSK authentication + anchor WLAN configuration.
CSCwb87440	Open Virtualization Format (OVF) template allows to change serial number to any value.
CSCwb93067	Cisco Catalyst 9800-CL Controller: WNCd crash is observed during switch integrated security features (SISF) routines.
CSCwb93513	Stale client entries are not deleted and is stuck on device-tracking database.
CSCwc01644	CoS AP is using native VLAN instead of VLAN used in the policy profile.
CSCwc04197	Secondary controller crashes during redundancy switchover.
CSCwc05366	Wireless AAA dynamic VLAN assignment: Wireless clients cannot reach each other.
CSCwc14629	Web UI is taking long time to show initial page.
CSCwc15533	Continuous wncmgrd CPU HOG traceback is observed with scale Flexible NetFlow (FNF) mapping to policy profile.

Caveat ID	Description
CSCwc15944	Multicast data is not sent to clients; some APs are unable to join.
CSCwc17774	Few Object identifiers (OIDs) under CISCO-ENHANCED-MEMPOOL-MIB shows no instance after switchover.
CSCwc22468	Client traffic fails when client roams between APs with dot11r to dot11i transition.
CSCwc26105	Controller HA split brain due to multiple secondary addresses on the interface.
CSCwc26819	Controller is not sending Logical Link Control (LLC) or eXchange IDentifier (XID) spoofed frames after a mobility event.
CSCwc28408	WNCD crash on co_fetch_mbssid_from_rbssid.
CSCwc32226	Zebra RF guns gets deleted from controller randomly due to reason: CO_CLIENT_DELETE_REASON_ZONE_CHANGE.
CSCwc36910	cEdge device pushes wrong config syntax (config wlan broadcase-ssid disable 2).
CSCwc38828	Invalid TDL pointers caused WNCd crash.
CSCwc41358	MAC filtering: WLAN profile column displays the WLAN name + description.
CSCwc41903	Syslog needs to be enhanced.
CSCwc42784	Client fails to connect when protocol based QoS is configured.
CSCwc55982	Stale entry is observed in the show wireless device tracking database ip command output after client deletion.
CSCwc57227	Wireless Network Control Daemon (WNCd) crash is observed.
CSCwc57312	Layer2 VXLAN network identifier (VNID) number in CLI and GUI are different.
CSCwc57836	Restore configuration by HTTP mode does not work on Cisco Embedded Wireless Controller.
CSCwc59518	Cisco Catalyst 9800-80 controller crashes with the reason: Critical process wncd fault on rp_0_3 (rc=134).
CSCwc72047	APs are operating on disabled RF profile channels.
CSCwc75247	Packets destined for Layer 2 socket application gets delivered to Layer 3 socket application.
CSCwc76905	SISF crash is observed when handling DHCP messages.

Caveat ID	Description
CSCwc79394	WNCd is going high upto 99% on tbl(WNCD_DB/tbl_client_wsa_info).
CSCwd00711	When Wi-Fi Protected Access (WPA) 3 and Opportunistic Wireless Encryption (OWE) transition are enabled, non-WPA3 clients are getting network access in webauth-pending state.
CSCwd17349	Active chassis get stuck during SSO failover.

Troubleshooting

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

Related Documentation

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

Cisco Wireless Controller

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

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

The installation guide for your controller is available at:

- Hardware Installation Guides

All Cisco Wireless Controller software-related documentation

Cisco Catalyst 9800 Series 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.