Release Notes for Cisco Embedded Wireless Controller on Catalyst Access Points, Cisco IOS XE Cupertino 17.9.x

First Published: 2022-08-01

Last Modified: 2025-09-25

Release Notes for Cisco Embedded Wireless Controller on Catalyst Access Points, Cisco IOS XE Cupertino 17.9.x

Introduction to Cisco Embedded Wireless Controller on Catalyst Access Points



Caution

Problem Description: Authentication fails when attempting to upgrade software using the "CCO mode" in Cisco Embedded Wireless Controller (EWC) on a Cisco Catalyst Access Point (EWC-AP). This issue occurs when attempting to upgrade from a software release prior to one of the following releases: 17.3.x, 17.6.x, 17.9.5, 17.12.3, and 17.14.1.

Background: From May 1, 2024, onwards, Cisco Connection Online (CCO, known as cisco.com) will use a new authentication system for EWC-AP. This system is not backward compatible with the earlier EWC-AP software releases. EWC-AP software developed after January 31, 2024, will be able to authenticate with Cisco.com, before and after May 1, 2024. The releases include: 17.9.5 and later, 17.12.3 and later, and 17.14.1 and later.

Workaround: Download the desired EWC-AP image and load it into the EWC-AP over TFTP, SFTP, or (Desktop) HTTP.

Upgrade to one of the following releases:

1. 17.9.5 or later
2. 17.12.3 or later
3. 17.14.1 or later

After the upgrade, the CCO method for upgrades will work.

For more information, see Field Notice: FN74124.

The Cisco Embedded Wireless Controller on Catalyst Access Points is a version of the Cisco IOS XE-based controller software on Catalyst access points (AP). In this solution, a Catalyst AP that is running the Cisco

Embedded Wireless Controller on Catalyst Access Points software, is designated as the primary AP. Other APs, referred to as subordinate APs, associate to this primary AP.

The Cisco Embedded Wireless Controller on Catalyst Access Points provides enterprise-level WLAN features while maintaining operational simplicity and affordability. This solution is targeted at small and medium-sized business (SMB) customers or distributed enterprises, and can be run at single site deployments.

- The controllers come with high availability (HA) and seamless software updates. This keeps your services on always, both during planned and unplanned events.
- The deployment can be managed using a mobile application, Cisco Catalyst Center, Netconf/Restconf, web-based GUI, or CLI.

What's New in Cisco Embedded Wireless Controller on Catalyst Access Points, Cisco IOS XE Cupertino 17.9.8

There are no new features in this release.

What's New in Cisco Embedded Wireless Controller on Catalyst Access Points, Cisco IOS XE Cupertino 17.9.7

There are no new features in this release.

What's New in Cisco Embedded Wireless Controller on Catalyst Access Points, Cisco IOS XE Cupertino 17.9.6

There are no new features in this release.

What's New in Cisco Embedded Wireless Controller on Catalyst Access Points, Cisco IOS XE Cupertino 17.9.5

There are no new features in this release.

What's New in Cisco Embedded Wireless Controller on Catalyst Access Points, Cisco IOS XE Cupertino 17.9.4a

There are no new features in this release. This release provides a fix for CSCwh87343: Cisco IOS XE Software Web UI Privilege Escalation Vulnerability. For more information, see Security Advisory: cisco-sa-iosxe-webui-privesc-j22SaA4z.

What's New in Cisco Embedded Wireless Controller on Catalyst Access Points, Cisco IOS XE Cupertino 17.9.4

There are no new features in this release.

What's New in Cisco Embedded Wireless Controller on Catalyst Access Points, Cisco IOS XE Cupertino 17.9.3

There are no new features in this release.

What's New in Cisco Embedded Wireless Controller on Catalyst Access Points, Cisco IOS XE Cupertino 17.9.2

There are no new features in this release.

What's New in Cisco Embedded Wireless Controller on Catalyst Access Points, Cisco IOS XE Cupertino 17.9.1

Table 1: New and Modified Software Features

Feature Name	Description and Documentation Link
Zero Wait Dynamic Frequency Selection	When an access point (AP) moves to Dynamic Frequency Selection (DFS) channel, a service outage can occur. This feature helps to avoid service outages in regulatory domains. As of now, the US and Europe are the only supported domains. For more information, see the chapter Zero Wait Dynamic Frequency Selection.
Mesh Backhaul RRM Support	From this release onwards, RRM DCA runs on mesh backhaul, in the auto mode, when you configure the **wireless mesh backhaul rrm auto-dca** command. For APs that do not have dedicated (RHL) radios, DCA is triggered by running commands in the privilege EXEC mode. Mesh RRM DCA runs in the background for RHL radio enabled APs. The following commands are introduced: • **ap dot11 {24ghz | 5ghz | 6ghz} rrm channel-update mesh** • **ap dot11 {24ghz | 5ghz | 6ghz} rrm channel-update mesh bridge-group** • **ap name** *Cisco-ap-name* **dot11 {24ghz | 5ghz | 6ghz} rrm channel update mesh** • **show wireless mesh rrm dca status** • **wireless mesh backhaul rrm auto-dca** For more information, see the chapter Mesh Access Points.

Feature Name	Description and Documentation Link
RUM Report Throttling	For all topologies where the product instance initiates communication, the minimum reporting frequency is throttled to one day. This means the product instance does not send more than one RUM report a day. The affected topologies are: *Connected Directly to CSSM*, *Connected to CSSM Through CSLU* (product instance-initiated communication), *CSLU Disconnected from CSSM* (product instance-initiated communication), and *SSM On-Prem Deployment* (product instance-initiated communication). This resolves the problem of too many RUM reports being generated and sent for certain licenses. It also resolves the memory-related issues and system slow-down that was caused by an excessive generation of RUM reports. You can override the reporting frequency throttling, by entering the **license smart sync** command in privileged EXEC mode. This triggers an on-demand synchronization with CSSM or CSLU, or SSM On-Prem, to send and receive any pending data. RUM report throttling also applies to the Cisco IOS XE Amsterdam 17.3.6 and later releases of the 17.3.x train, and Cisco IOS XE Bengaluru 17.6.4 and later releases of the 17.6.x train. From Cisco IOS XE Cupertino 17.9.1, RUM report throttling is applicable to *all* subsequent releases.

Behavior Change

- The EWC internal AP or EWC capable AP wired interface did not send packets to subnet 192.168.129.0/24. The AP did not send traffic to 192.168.129.0/24 from wired 0 interface as the static route for 192.168.129.0/24 was automatically configured. Only clients in the subnet 192.168.129.0/24 were affected.

  From Cisco IOS XE Cupertino 17.9.3 onwards, the unusable address range has been changed from 192.168.129.0/24 to 192.168.255.252/30. Now, if the wired or wireless clients are on subnet 192.168.255.252/30, the AP does not send packets from the AP interface to the clients.

Interactive help

Interactive help is a user interface feature that

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

Modes of starting the interactive Help

You can start the interactive help in the these ways.

- Hover over the blue flap at the right-hand corner of a window in the GUI and clicking **Interactive Help**.
- Click **Walk-me Thru** in the left pane of a window in the GUI.

- Click **Show me How** whenever displayed in the GUI. Clicking **Show me How** triggers a specific interactive help that is relevant to the context you are in.

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

Additional troubleshooting information

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

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

Supported Cisco Access Point Platforms

The following Cisco access points are supported in the Cisco Embedded Wireless Controller on Catalyst Access Points network. Note that the APs listed as primary APs can also function as subordinate APs.

Table 2: Cisco APs Supported in Cisco Embedded Wireless Controller on Catalyst Access Points

Primary AP	Subordinate AP
Cisco Catalyst 9115 Series	Cisco Aironet 1540 Series
Cisco Catalyst 9117 Series	Cisco Aironet 1560 Series
Cisco Catalyst 9120 Series	Cisco Aironet 1815i
Cisco Catalyst 9124AXE/I/D	Cisco Aironet 1815w
Cisco Catalyst 9130	Cisco Aironet 1830 Series
Cisco Catalyst 9105AXI	Cisco Aironet 1840 Series
	Cisco Aironet 1850 Series
	Cisco Aironet 2800 Series
	Cisco Aironet 3800 Series
	Cisco Aironet 4800 Series
	Cisco Catalyst 9115 Series
	Cisco Catalyst 9117 Series
	Cisco Catalyst 9120 Series
	Cisco Catalyst 9124AXE/I/D
	Cisco Catalyst 9130
	Cisco Catalyst 9105AXW
	Cisco Catalyst 9105AXI
	Cisco Catalyst Industrial Wireless 6300 Heavy Duty Series Access Points
	Cisco 6300 Series Embedded Services Access Points

Note The following APs are not supported:

- Cisco Catalyst 9136 Access Points
- Cisco Catalyst 9166 Series Access Points
- Cisco Catalyst 9164 Series Access Points
- Cisco Catalyst 9162 Series Access Points

Table 3: Image Types and Supported APs in Cisco Embedded Wireless Controller on Catalyst Access Points

Image Type	Supported APs
ap1g4	Cisco Aironet 1810 Series Cisco Aironet 1830 Series Cisco Aironet 1850 Series
ap1g5	Cisco Aironet 1815i Cisco Aironet 1815w Cisco Aironet 1540 Series Cisco Aironet 1850 Series
ap1g6	Cisco Catalyst 9117 Series
ap1g6a	Cisco Catalyst 9130 Cisco Catalyst 9124AXE/I/D
ap1g7	Cisco Catalyst 9115 Series Cisco Catalyst 9120 Series
ap1g8	Cisco Catalyst 9105 Series
ap3g3	Cisco Aironet 2800 Series Cisco Aironet 3800 Series Cisco Aironet 4800 Series Cisco Aironet 1560 Series Cisco Catalyst Industrial Wireless 6300 Heavy Duty Series Access Points Cisco 6300 Series Embedded Services Access Points

Maximum APs and Clients Supported

Table 4: Scale Supported in Cisco EWC Network

Primary AP Model	Maximum APs Supported	Maximum Clients Supported
Cisco Catalyst 9105 AWI	50	1000
Cisco Catalyst 9115 Series	50	1000
Cisco Catalyst 9117 Series	50	1000
Cisco Catalyst 9120 Series	100	2000

Primary AP Model	Maximum APs Supported	Maximum Clients Supported
Cisco Catalyst 9124AXE/I/D	100	2000
Cisco Catalyst 9130	100	2000

Note If 25 to 100 APs have joined the EWC network, the maximum clients on the EWC internal AP is limited to 20.

Compatibility Matrix

The following table provides software compatibility information:

Table 5: Compatibility Information

Cisco Embedded Wireless Controller on Catalyst Access Points	Cisco ISE	Cisco CMX	Cisco Catalyst Center
Cupertino 17.9.x	3.0 2.7 2.6 2.4	10.6.3 10.6.2 10.6 10.5.1	See Cisco Catalyst Center Compatibility Information

Supported Browsers and Operating Systems for Web UI

Note The following list of Supported Browsers and Operating Systems is not comprehensive at the time of writing this document and the behavior of various browser for accessing the GUI of the EWC is as listed below.

Table 6: Supported Browsers and Operating Systems

Browser	Version	Operating System	Status	Workaround
Google Chrome	77.0.3865.120	macOS Mojave Version 10.14.6	Works	Proceed through the browser warning.
Safari	13.0.2 (14608.2.40.1.3)	macOS Mojave Version 10.14.6	Works	Proceed through the browser warning.
Mozilla Firefox	69.0.1	macOS Mojave Version 10.14.6	Works only if exception is added.	Set the exception.

Browser	Version	Operating System	Status	Workaround
Mozilla Firefox	69.0.3	macOS Mojave Version 10.14.6	Works only if exception is added.	Set the exception.
Google Chrome	77.0.3865.90	Windows 10 Version 1903 (OS Build 18362.267)	Works	Proceed through the browser warning.
Microsoft Edge	44.18362.267.0	Windows 10 Version 1903 (OS Build 18362.267)	Works	Proceed through the browser warning.
Mozilla Firefox	68.0.2	Windows 10 Version 1903 (OS Build 18362.267)	Works	Proceed through the browser warning.
Mozilla Firefox	69.0.3	Windows 10 Version 1903 (OS Build 18362.267)	Works only if exception is added.	Set the exception.
Google Chrome	78.0.3904.108	macOS Catalina 10.15.1	Does not work	NA

Upgrading the Controller Software

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

Note Before converting from CAPWAP to embedded wireless controller (EWC), ensure that you upgrade the corresponding AP with the CAPWAP image in Cisco AireOS Release 8.10.105.0. If this upgrade is not performed, the conversion will fail.

Finding the Software Version

The following table lists the Cisco IOS XE 17.9.x software for Cisco Embedded Wireless Controller on Catalyst Access Points.

Choose the appropriate AP software based on the following:

- Cisco Embedded Wireless Controller on Catalyst Access Points software to be used for converting the AP from an unified wireless network CAPWAP lightweight AP to a Cisco Embedded Wireless Controller on Catalyst Access Points-capable AP (primary AP)
- AP software image bundle to be used either for upgrading the Cisco Embedded Wireless Controller on Catalyst Access Points software on the primary AP or for updating the software on the subordinate APs or both

Prior to ordering Cisco APs, see the corresponding ordering guide for your Catalyst or Aironet access point.

Table 7: Cisco Embedded Wireless Controller on Catalyst Access Points Software

Primary AP	AP Software for Conversion from CAPWAP to Cisco EWC	AP Software Image Bundle for Upgrade	AP Software in the Bundle
Cisco Catalyst 9115 Series	C9800-AP-universalk9.17.09.08.zip C9800-AP-universalk9.17.09.07.zip C9800-AP-universalk9.17.09.06.zip C9800-AP-universalk9.17.09.05.zip C9800-AP-universalk9.17.09.4a.zip C9800-AP-universalk9.17.09.04.zip C9800-AP-universalk9.17.09.03.zip C9800-AP-universalk9.17.09.02.zip C9800-AP-universalk9.17.09.01.zip	C9800-AP-universalk9.17.09.08.zip C9800-AP-universalk9.17.09.07.zip C9800-AP-universalk9.17.09.06.zip C9800-AP-universalk9.17.09.05.zip C9800-AP-universalk9.17.09.4a.zip C9800-AP-universalk9.17.09.04.zip C9800-AP-universalk9.17.09.03.zip C9800-AP-universalk9.17.09.02.zip C9800-AP-universalk9.17.09.01.zip	ap1g7
Cisco Catalyst 9117 Series	C9800-AP-universalk9.17.09.08.zip C9800-AP-universalk9.17.09.07.zip C9800-AP-universalk9.17.09.06.zip C9800-AP-universalk9.17.09.05.zip C9800-AP-universalk9.17.09.4a.zip C9800-AP-universalk9.17.09.04.zip C9800-AP-universalk9.17.09.03.zip C9800-AP-universalk9.17.09.02.zip C9800-AP-universalk9.17.09.01.zip	C9800-AP-universalk9.17.09.08.zip C9800-AP-universalk9.17.09.07.zip C9800-AP-universalk9.17.09.06.zip C9800-AP-universalk9.17.09.05.zip C9800-AP-universalk9.17.09.4a.zip C9800-AP-universalk9.17.09.04.zip C9800-AP-universalk9.17.09.03.zip C9800-AP-universalk9.17.09.02.zip C9800-AP-universalk9.17.09.01.zip	ap1g6
Cisco Catalyst 9120 Series	C9800-AP-universalk9.17.09.08.zip C9800-AP-universalk9.17.09.07.zip C9800-AP-universalk9.17.09.06.zip C9800-AP-universalk9.17.09.05.zip C9800-AP-universalk9.17.09.4a.zip C9800-AP-universalk9.17.09.04.zip C9800-AP-universalk9.17.09.03.zip C9800-AP-universalk9.17.09.02.zip C9800-AP-universalk9.17.09.01.zip	C9800-AP-universalk9.17.09.08.zip C9800-AP-universalk9.17.09.07.zip C9800-AP-universalk9.17.09.06.zip C9800-AP-universalk9.17.09.05.zip C9800-AP-universalk9.17.09.4a.zip C9800-AP-universalk9.17.09.04.zip C9800-AP-universalk9.17.09.03.zip C9800-AP-universalk9.17.09.02.zip C9800-AP-universalk9.17.09.01.zip	ap1g7

Primary AP	AP Software for Conversion from CAPWAP to Cisco EWC	AP Software Image Bundle for Upgrade	AP Software in the Bundle
Cisco Catalyst 9124AXE/I/D	C9800-AP-universalk9.17.09.08.zip C9800-AP-universalk9.17.09.07.zip C9800-AP-universalk9.17.09.06.zip C9800-AP-universalk9.17.09.05.zip C9800-AP-universalk9.17.09.4a.zip C9800-AP-universalk9.17.09.04.zip C9800-AP-universalk9.17.09.03.zip C9800-AP-universalk9.17.09.02.zip C9800-AP-universalk9.17.09.01.zip	C9800-AP-universalk9.17.09.08.zip C9800-AP-universalk9.17.09.07.zip C9800-AP-universalk9.17.09.06.zip C9800-AP-universalk9.17.09.05.zip C9800-AP-universalk9.17.09.4a.zip C9800-AP-universalk9.17.09.04.zip C9800-AP-universalk9.17.09.03.zip C9800-AP-universalk9.17.09.02.zip C9800-AP-universalk9.17.09.01.zip	ap1g6a
Cisco Catalyst 9130	C9800-AP-universalk9.17.09.08.zip C9800-AP-universalk9.17.09.07.zip C9800-AP-universalk9.17.09.06.zip C9800-AP-universalk9.17.09.05.zip C9800-AP-universalk9.17.09.4a.zip C9800-AP-universalk9.17.09.04.zip C9800-AP-universalk9.17.09.03.zip C9800-AP-universalk9.17.09.02.zip C9800-AP-universalk9.17.09.01.zip	C9800-AP-universalk9.17.09.08.zip C9800-AP-universalk9.17.09.07.zip C9800-AP-universalk9.17.09.06.zip C9800-AP-universalk9.17.09.05.zip C9800-AP-universalk9.17.09.4a.zip C9800-AP-universalk9.17.09.04.zip C9800-AP-universalk9.17.09.03.zip C9800-AP-universalk9.17.09.02.zip C9800-AP-universalk9.17.09.01.zip	ap1g6a

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.

Guidelines and Restrictions

Internet Group Management Protocol (IGMP)v3 is not supported on Cisco Aironet Wave 2 APs.

Embedded Wireless Controller SNMP configuration is supported in Cisco Catalyst Center.

High memory usage on AP running Embedded Wireless Controller. Enabling **crash kernel** on the AP consumes additional memory on the AP. Hence, if **crash kernel** is enabled, the overall memory usage of the device will increase and will impact the scale numbers. On Cisco Catalyst 9130 Access Points, the memory consumption is a high of 128 MB.

During the EWC HA pair selection, after a power outage, the standby AP fails to come up in the new EWC HA pair. Another EWC capable AP becomes the standby AP and fails to come up as well. To avoid this situation, ensure that the same IP address is enforced on the active or standby APs during HA pair selection.

Interoperability with Clients

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

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

Table 8: Test Configuration for Interoperability

Hardware or Software Parameter	Hardware or Software Type
Release	Cisco IOS XE Cupertino 17.9.x

Access Points	• Cisco Aironet Series Access Points
	  • 1540
	  • 1560
	  • 1815i
	  • 1815w
	  • 1830
	  • 1840
	  • 1850
	  • 2800
	  • 3800
	  • 4800
	• Cisco Catalyst 9105AX Access Points
	• Cisco Catalyst 9115AX Access Points
	• Cisco Catalyst 9117AX Access Points
	• Cisco Catalyst 9120AX Access Points
	• Cisco Catalyst 9124AXE/I/D Access Points
	• Cisco Catalyst 9130AX Access Points

Hardware or Software Parameter	Hardware or Software Type
Radio	• 802.11ax • 802.11ac • 802.11a • 802.11g • 802.11n (2.4 GHz or 5 GHz)
Security	Open, PSK (WPA2-AES), 802.1X (WPA2-AES) (EAP-FAST, EAP-TLS), WPA3.
Cisco ISE	See Compatibility Matrix, on page 8.
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 9: Client Types

Client Type and Name	Driver / Software Version
Wi-Fi 6 Devices (Mobile Phone and Laptop)	
Apple iPhone 11	iOS 14.1
Apple iPhone SE 2020	iOS 14.1
Dell Intel AX1650w	Windows 10 (21.90.2.1)
DELL LATITUDE 5491 (Intel AX200)	Windows 10 Pro (21.40.2)
Samsung S20	Android 10
Samsung S10 (SM-G973U1)	Android 9.0 (One UI 1.1)
Samsung S10e (SM-G970U1)	Android 9.0 (One UI 1.1)
Samsung Galaxy S10+	Android 9.0
Samsung Galaxy Fold 2	Android 10
Samsung Galaxy Flip Z	Android 10
Samsung Note 20	Android 10
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 Catalina 10.15.4

Client Type and Name	Driver / Software Version
Apple Macbook Air 13 inch	OS High Sierra 10.13.4
Macbook Pro Retina	OS Mojave 10.14.3
Macbook Pro Retina 13 inch early 2015	OS Mojave 10.14.3
Dell Inspiron 2020 Chromebook	Chrome OS 75.0.3770.129
Google Pixelbook Go	Chrome OS 84.0.4147.136
HP chromebook 11a	Chrome OS 76.0.3809.136
Samsung Chromebook 4+	Chrome OS 77.0.3865.105
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 (18.32.0.5)
DELL Latitude E5540 (Intel Dual Band Wireless AC7260)	Windows 7 Professional (21.10.1)
DELL XPS 12 v9250 (Intel Dual Band Wireless AC 8260)	Windows 10 (19.50.1.6)
DELL Latitude 5491 (Intel AX200)	Windows 10 Pro (21.40.2)
DELL XPS Latitude12 9250 (Intel Dual Band Wireless AC 8260)	Windows 10 Home (21.40.0)
Lenovo Yoga C630 Snapdragon 850 (Qualcomm AC 2x2 Svc)	Windows 10(1.0.10440.0)
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 you to update to the latest Intel wireless drivers if advertised SSIDs are not visible.	
Tablets	
Apple iPad Pro	iOS 13.5
Apple iPad Air2 MGLW2LL/A	iOS 12.4.1
Apple iPad Mini 4 9.0.1 MK872LL/A	iOS 11.4.1
Apple iPad Mini 2 ME279LL/A	iOS 12.0
Microsoft Surface Pro 3 – 11ac	Qualcomm Atheros QCA61x4A
Microsoft Surface Pro 3 – 11ax	Intel AX201 chipset. Driver v21.40.1.3
Microsoft Surface Pro 7 – 11ax	Intel Wi-Fi chip (HarrisonPeak AX201) (11ax, WPA3)

Client Type and Name	Driver / Software Version
Microsoft Surface Pro X – 11ac & WPA3	WCN3998 Wi-Fi Chip (11ac, WPA3)
Mobile Phones	
Apple iPhone 5	iOS 12.4.1
Apple iPhone 6s	iOS 13.5
Apple iPhone 8	iOS 13.5
Apple iPhone X MQA52LL/A	iOS 13.5
Apple iPhone 11	iOS 14.1
Apple iPhone SE MLY12LL/A	iOS 11.3
ASCOM SH1 Myco2	Build 2.1
ASCOM SH1 Myco2	Build 4.5
ASCOM Myco 3 v1.2.3	Android 8.1
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 2	Android 10
Google Pixel 3	Android 11
Google Pixel 3a	Android 11
Google Pixel 4	Android 11
Huawei Mate 20 pro	Android 9.0
Huawei P20 Pro	Android 9.0
Huawei P40	Android 10
LG v40 ThinQ	Android 9.0
One Plus 8	Android 10
Oppo Find X2	Android 10
Redmi K20 Pro	Android 10
Samsung Galaxy S7	Andriod 6.0.1
Samsung Galaxy S7 SM - G930F	Android 8.0
Samsung Galaxy S8	Android 8.0
Samsung Galaxy S9+ - G965U1	Android 9.0
Samsung Galaxy SM - G950U	Android 7.0

Client Type and Name	Driver / Software Version
Sony Experia 1 ii	Android 10
Sony Experia xz3	Android 9.0
Xiaomi Mi10	Android 10
Spectralink 8744	Android 5.1.1
Spectralink Versity Phones 9540	Android 8.1
Vocera Badges B3000n	4.3.2.5
Vocera Smart Badges V5000	5.0.4.30
Zebra MC40	Android 5.0
Zebra MC40N0	Android Ver: 4.1.1
Zebra MC92N0	Android Ver: 4.4.4
Zebra TC51	Android 7.1.2
Zebra TC52	Android 8.1.0
Zebra TC55	Android 8.1.0
Zebra TC57	Android 8.1.0
Zebra TC70	Android 6.1
Zebra TC75	Android 6.1.1
Printers	
Zebra QLn320 Printer	LINK OS 6.3
Zebra ZT230 Printer	LINK OS 6.3
Zebra ZQ310 Printer	LINK OS 6.3
Zebra ZD410 Printer	LINK OS 6.3
Zebra ZT410 Printer	LINK OS 6.3
Zebra ZQ610 Printer	LINK OS 6.3
Zebra ZQ620 Printer	LINK OS 6.3
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

Issues

Issues describe unexpected behavior in Cisco IOS releases. 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 will cover 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 a caveat, click the corresponding identifier.

Open Caveats for Cisco IOS XE 17.9.8

Caveat ID	Description
CSCwm73020	Controller relays unicast DHCP requests
CSCwn81268	Due to switch reload when AP boots up, IOX-APP is starting before USB is detected
CSCwn89252	AP running 17.15.2 not possible to install Solum IOX APP
CSCwj88851	Yang/CLI length mismatch for AP location description
CSCwm98000	Catalyst 9105 AP display Short Preamble \"Allowed\" but then rejects association with SP \"Not Allowed\"
CSCwn31021	Controller fails to represent the correct format of AP Name and VLAN ID in option 82

Open Caveats for Cisco IOS XE 17.9.7

There are no open caveats for this relesae.

Open Caveats for Cisco IOS XE 17.9.6

Identifier	Headline
CSCwj08558	The Cisco Catlalyst 9124 APs are not assigning correct channels on the 2.4-GHz radio
CSCwk82907	The controller AP join issues due to CPP stale entries, caused by qos-template-bind childless objects
CSCwk84121	Local software clients are assigned to zone ID 0 when IP overlap and Flex vlan-central-sw is configured

Identifier	Headline
CSCwk90493	The interface VRRP MAC flaps between active and standby Embedded Wireless Controller (EWC)
CSCwm09148	The rogue Syslog messages do not appear in EWC and in the Syslog server
CSCwm09738	Memory leak in Cisco Catalyst 9120 APs, on 17.9.5

Open Caveats for Cisco IOS XE 17.9.5

Identifier	Headline
CSCwh18613	The encrypted mesh pre-shared key changes when the **password encryption aes** command is applied.
CSCwh63050	The controller sends Internet Group Management Protocol (IGMP) queries with an IP address not present in the controller and a controller MAC address.
CSCwi04855	The Cisco Catalyst 9115 AP disjoins the controller repeatedly, with traceback.
CSCwi16509	APs disjoin the contoller displaying the "Invalid radio slot id" error message. Few APs do not join back the controller.
CSCwi27380	The media stream feature does not work.
CSCwi28382	The controller experiences an unexpected reset.
CSCwi29636	The controller crashes due to WNCD process fault.
CSCwi42112	The MAC addresses of wired clients are being learnt from the Cisco Catalyst 9124 MAP port.
CSCwi51025	Cisco Catalyst 9130 AP crashes due to kernel panic.
CSCwi53481	Cisco Catalyst 9300 Series Switches running on the controller loses the SUDI MIC trustpoint during an upgrade.
CSCwi55714	The controller reboots unexpectedly due to a Network Mobility Service Protocol (NMSP) process failure.
CSCwi56780	MAC Authentication Bypass (MAB) is not initiated unless the device is deauthenticated.
CSCwi60173	Security Group Tag (SGT) is not applied to the wireless client in the Software-Defined Access (SDA) fabric.
CSCwi62934	Cisco Catalyst 9120 AP drops large packets towards clients, resulting in poor browsing experience.
CSCwi66133	Cisco Catalyst 9130 AP crashes due to kernel panic.

Open Caveats for Cisco IOS XE 17.9.4a

For the list of open caveats, click here.

Open Caveats for Cisco IOS XE 17.9.4

For the list of open caveats, click here.

Open Caveats for Cisco IOS XE 17.9.3

Identifier	Headline
CSCwd69780	Controller crash is observed due to netflow watchdog and observed CPU HOG in wncmgrd due to scale netflow.
CSCwa67566	Cisco Catalyst 9800 Series Controller/AireOS parity: Rejects clients with wrong PMKID when changing AKM from FT to dot1x to FT again.
CSCwd96484	Controller reloads unexpectedly after generating "wncd" core files.
CSCwe16892	Traceback and reload occurs after detecting a bad magic number in chunk header.
CSCwe18012	Standby controller crashes while saving tbl QoS table.
CSCwe38431	Controller is re-marking SIP packets from CS3 to CS0 in upstream/downstream when voice cac is configured.
CSCwe49267	Controller is not sending GTK M5 packet to 8821 after FT roaming between wncds.
CSCwd56391	Controller is not providing RSSI location data for some of the RFID tags in database.
CSCwd86288	Load average warning is displayed even when Cisco Catalyst 9800-80 Series Controller is healthy.
CSCwd96376	Unable to login to controller GUI/CLI with the user created by Day 0 Wizard.
CSCwd98332	Controller reloads after failing to match the interface ID in the anchor message.
CSCwe12057	QoS Page is not loading when ACL has double quote special character in the name.
CSCwe25610	Client delete initiated. Reason: CO_CLIENT_DELETE_REASON_REMOTE_MOBILITY_DELETE - Mobility Local.
CSCwe31270	Clients stop passing traffic when there is a missing bandwidth limit AAA attribute on the controller.
CSCwe39039	Traceback is observed after provisioning controller from Cisco DNA Center.
CSCwe42211	EWC time offset is not updated on GUI.
CSCwc72194	Cisco Catalyst 9120 AP: Radio core dump: wl0: wlc_check_assert_type HAMMERING.
CSCwd46815	EAP-TLS is failing for the wired clients behind MAP for Cisco 2800, 3800, 4800, 1562, 6300 series APs.

Identifier	Headline
CSCwd79502	Controller is tracking stale entry due to anchored client getting IPv4 and IPv6 in different VLANs.
CSCwd90742	Cisco Catalyst 9120AX AP kernel crash - PC is at rhb_del_interface+0xc.
CSCwd90907	Cisco Catalyst 9164 AP: Crash is observed on radio 1.
CSCwd91054	COS-APs are not encrypting EAP_ID_REQ after M1-M4 and not updating PMKID for dot1x OKC.
CSCwe00248	Poor reassociation behavior observed between Spectralink 84xx series phones and Cisco Catalyst 9136 APs.
CSCwe04602	Cisco Catalyst 9120 AP fails to forward traffic to wireless client for about 60 seconds.
CSCwe07802	Cisco APs such as 2800, 3800, 4800, and 1562 are dropping upstream EAP packets.
CSCwe11747	Cisco Catalyst AX Series APs are decoding EAP request ID incorrectly.
CSCwe22861	AID leak is observed in Flex Cisco Wave 2 APs.
CSCwe30473	Radio firmware crash is observed due to a frozen rc queue.
CSCwe31030	Cisco Catalyst 9105AXW AP is crashing.
CSCwe32005	Cisco Catalyst 9130 AP: Packet loss is observed on Digital Signage device.
CSCwe42604	Cisco Catalyst 9120 AP is dropping 2 bytes from EAP TLS packet causing clients not to join dot1x SSID.
CSCwe43294	Cisco Catalyst 9105AXW AP and Cisco Aironet 1815W Flex RLAN AP does not apply VLAN in the ethernet port after AAA vlan override.
CSCwe44216	AP crash is observed due to kernel panic (PC is at vfp_reload_hw+0x30/0x44).
CSCwe44991	Cisco Catalyst 9105AX AP: Kernel panic crash is observed.
CSCwe45300	Cisco Catalyst 9120 AP: Sending Msg:2 in mode:2 to hostapd failed.
CSCwe45894	AP are not forwarding IGMPv3 query to wireless clients.
CSCwe45970	APs are stuck in UBOOT.
CSCwe50033	Cisco Catalyst 9120AX AP: Clients are continuously disconnecting if more than 10 clients are using MS TEAMS.

Open Caveats for Cisco IOS XE 17.9.2

Caveat ID	Description
CSCwc49992	Timeout during Direct Memory Access (DMA) transaction causes kernel panic in Access Point
CSCwd05213	Kernel panic crash observed when gRPC server process is executed.

Caveat ID	Description
CSCwd05689	Cisco Catalyst 9124 Access Point AXI RSSI is 7 dBm to 8 dBm weaker at a distance compa models.
CSCwd10570	Cisco Catalyst 9130 Access Point displays different beacon data-rates for different Basic Se (BSSIDs).
CSCwd22017	Apple iOS devices are deleted due to IP Learn timeout.
CSCwd30828	Cisco Catalyst 9120 Access Point crashes and reloads due to kernel panic.
CSCwd32215	Clients are stuck in "S_CO_L2_AUTH_IN_PROGRESS" loop when completing authentica
CSCwd33981	Kernel panic crash is observed when PC is at "cpuidle_not_available".
CSCwc64201	Cisco Catalyst 9105 Access Point experiences communication gaps when working as a wor
CSCwc87688	Cisco Catalyst 9120 Access Point randomly displays high noise level in 5-GHz radio.
CSCwd21996	Cisco Catalyst 9120 Access Point experiences CleanAir sensor crash.
CSCwd22430	Access Points fail to view the backup image after running the "archive download-sw" comr
CSCwd25931	Wireless client does not receive IPv6 RA from wired FlexConnect local Dynamic Host Config
CSCwd28109	Cisco Catalyst 9130 Access Point experiences high latency or packet drops during TFTP.
CSCwd34908	Dynamic Channel Allocation (DCA) debug in the controller does not display Slot 2 when tl uses channel 36.

Open Caveats for Cisco IOS XE 17.9.1

There are no open caveats for this release.

Resolved Caveats for Cisco IOS XE 17.9.8

Caveat ID	Description
CSCwj60401	Catalyst AP is not requesting not more than 30 Watts
CSCwp93430	Cisco Catalyst 9130 AP stuck in crash loop after upgrade to 17.9.7
CSCwq71415	AP1852 sends excessive BAR flood due to Client not responding to data
CSCwk81946	Controller experiences kernel unresponsiveness due to tdl memory corruption
CSCwo62157	Controller with CAPWAP enabled display memory leak in tdl_mac_addr object
CSCwp86129	Client connected to local mac-auth PSK or MPSK SSIDs get disconnected and do not remain connected to the controller
CSCwo96182	SWEET32 Vulnerability on Cisco Catalyst 9120 APs

Resolved Caveats for Cisco IOS XE 17.9.7

Identifier	Headline
CSCwn04959	Internal AP does not join the EWC controller in the Site Survey mode

Resolved Caveats for Cisco IOS XE 17.9.6

Identifier	Headline
CSCwi21444	AP traps are not getting update to DNAC when AP joins the controller with misconfigured state
CSCwi54064	APs in the same controller classify each other as Rogue and alert as "AP Impersonation" threat
CSCwi55714	The controller reboots when handling the NMSP TLS connection
CSCwi88967	Cisco Catalyst 9120 APs crash and reload due to PSM microcode watchdog CS00012333933
CSCwi99296	Cisco Catalyst 9120 kernel panic observed with PC at wlc_bmac_suspend_mac_and_wait+0x3c/0x488 CS00012321648/CS00012332197
CSCwj10697	Cisco Catalyst 9124 AP: EWC image upgrade fails
CSCwj25187	Redundancy details not populated in the GUI for EWC
CSCwj31356	The controller reboots due to RRM process fault
CSCwj79545	The controller unexpectedly reboots: WNCD process reboots due to assertion failed with invalid BSSID
CSCwj97748	Cisco Catalyst 9130 AP: Kernel Panic with PC at _raw_spin_locK/LR wlan_objmgr_peer_try_get_ref (SF 07221295/07229313)
CSCwi69042	Cisco Aironet 1562 mesh AP not able to join through the root AP using EAP and flex-bridge site tag
CSCwi94248	AP crashes on dump mutx command
CSCwj83935	The controller **show tech X** is empty if the previous **show tech X** term length stop did not complete before SSH close
CSCwj96666	Syntax errors in CISCO-LWAPP-DOT11-MIB

Resolved Caveats for Cisco IOS XE 17.9.5

Identifier	Headline
CSCwf92148	The Cisco Catalyst 9120 AP dual 5-GHz radio does not disable High Efficiency (HE) in slot 0, when 11AX and slot 1 HE are disabled in all the configured WLANs.

Identifier	Headline
CSCwf13804	Cisco Catalyst 9120 AP fails to onboard new client associations.
CSCwf52815	Cisco Wave 2 APs do not reach the Maximum Transmission Unit (MTU) value of the Internet Control Message Protocol (ICMP).
CSCwf53520	Cisco Aironet 1815 AP encounters a kernel panic crash.
CSCwf59348	The maximum transmit power level for Cisco Catalyst 9105 AP, Cisco Catalyst 9115 AP, and Cisco Catalyst 9120 AP for Ireland (IE) is set at -128 dBm.
CSCwf62051	Cisco Aironet 1815W AP in FlexConnect mode encounters kernel panic, even with mDNS enabled.
CSCwf63818	Cisco Aironet 1832 AP encounters a kernel panic crash while in local mode.
CSCwf93992	Cisco Aironet 2800 Flex AP do not process EAP-TLS fragmented packets if the delay is more than 50ms.
CSCwf99932	Cisco Catalyst 9120 AP Radio1 crashes.
CSCwh08625	Cisco Catalyst 9120 AP experiences a kernel panic crash with specific PC and LR stack trace.
CSCwh09879	Cisco Wave 2 APs in FlexConnect mode sends assoc-resp failure after changing country code.
CSCwh17592	Cisco Catalyst 9130AXI AP slot 1 does not announce HT/VHT/HE capabilities when dual radio is enabled.
CSCwh20306	When aWIPS is enabled in Cisco Wave 2 APs, hyperlocation breaks.
CSCwh20934	Cisco Catalyst 9120 AP and Cisco Aironet 2800 AP crashes when joining the controller.
CSCwh33190	Cisco Catalyst 9115 AP (Local Mode) crashes due to a kernel panic.
CSCwh54762	Cisco Catalyst 9120 AP kernel panic does not synchronise.
CSCwh61011	Cisco Catalyst 9120 AP and Cisco Catalyst 9115 AP unexpectedly disjoin the controller, not establishing DTLS.
CSCwh74663	Cisco Aironet 2800, or 3800, or 4800, or 1560 AP, or Cisco Catalyst 6300 APs do not send QoS data frames downstream.
CSCwe24263	Cisco Catalyst 9130 AP encounters client-side issues due to inconsistent Tx power levels.
CSCwf10839	VRRP traffic causes the switch port to be down due to **storm-control action** config on Switch port side.
CSCwf13107	Cisco Catalyst 9105 AP encounters radio crash during longevity test.
CSCwf22246	Cisco Catalyst 9130 AP standardize calculation of mgmt frame count across AP chipsets.
CSCwf65794	Cisco Aironet 1852 AP reloads unexpectedly due to radio failure.

Identifier	Headline
CSCwf81866	Radio 0 Workgroup Bridge (WGB) configuration is not backed up correctly during a Trivial File Transfer Protocol (TFTP) backup of the configuration.
CSCwf83292	Cisco Catalyst 9130 AP does not send DHCP Offer and Acknowledgement (ACK) Over the Air (OTA) through the radio interface to the client.
CSCwf83515	Inconsistent Tx power levels advertised in country information of 802.11 beacon frame.
CSCwh20944	Cisco Catalyst 9120 AP crashed due to kernel panic.
CSCwh27425	Cisco Catalyst 9115AX AP does not forward a part of CAPWAP data packets to the uplink direction.
CSCwh29924	Cisco Catalyst 9105 AP, Cisco Catalyst 9115 AP, Cisco Catalyst 9120 AP WGB antenna-A does not function properly if the configuration is AB-antenna.
CSCwh35072	Cisco Aironet 3800 AP reloads unexpectedly due to FIQ/NMI reset.
CSCwh45418	Cisco Catalyst 9124 AP sends incorrect duplex information through Cisco Discovery Protocol (CDP).
CSCwh50681	A newly created SSID is broadcasted after a wireless upgrade.
CSCwh87343	Cisco IOS XE Software Web UI Privilege Escalation Vulnerability.
CSCwf40430	Cisco Catalyst 9130 AP and Cisco Catalyst 9800 AP encounter issues where mobile devices cannot prompt "incorrect password".
CSCwf76119	Clients are denied wireless access after profiling through **Access-Reject**. After a Change of Authorization (CoA), clients get network access using PMK cache.
CSCwf83132	The controller and later branches do not send 11r mobility payload.
CSCwf86242	The controller encounters a crash under the Wireless Network Control Daemon (WNCD) process.
CSCwf87281	The controller encounters a segmentation fault due to NULL timer.
CSCwh31966	The controller crashes on the WNCD process during DB abort.
CSCwh44793	Cisco Catalyst 9130 AP fails to join back after changing the AP site tag from the controller on 17.3.6.
CSCwh56836	Cisco Catalyst 9120 AP running Cisco Embedded Wireless Controller (EWC) crashes causing a constant active failover.
CSCwh58099	The controller disconnects a client from Identity Service Engine (ISE), causing a Change of Authorization (CoA) terminate and successful reconnect.
CSCwh59109	The controller encounters an unexpected reload with the reload reason RIF.
CSCwh61007	The controller crashes constantly whenever it provisions multiple APs.

Identifier	Headline
CSCwh63050	The Cisco Catalyst 9800-40 Wireless Controller sends Internet Group Management Protocol (IGMP) queries using client VLAN gateway IP address.
CSCwh82872	The controller encounters an association request drop due to an AP issue with the Cisco Catalyst 9115 AP model in Flex mode SSIDs.
CSCwi04855	The Cisco Catalyst 9115 AP repeatedly joins and disjoins using Catalyst 9800 traceback.
CSCwi16104	The controller encounters an unexpected DBM reset during VLAN list retrieval.
CSCvx90714	The **show interface status** function displays the maximum link speed (2500) on the auto-negotiation port.
CSCwd68141	The commands **show wireless wps rogue AP detail** and **show wireless wps rogue client detail** do not display the containment details for AP types.
CSCwe81775	Apple devices are not deleted properly after sending EAP logoff messages resulting in client elapsing more than 60 seconds for connectivity.
CSCwf04815	The Tx power reduces on AP slots 0 and 1 by one level due to incorrect coverage hole detection.
CSCwf13879	Cisco Catalyst 9800-CL Wireless Controller crashes unexpectedly when users are unable to connect to WiFi and access the controller's GUI.
CSCwf30516	The attribute positions in the **show wireless ewc-ap ap image predownload status** output should remain fixed regardless of the string size.
CSCwf50558	The controller still runs DCA Aggressive even after disabling the same with command.
CSCwf54827	Controller sends and stops accounts with high session time on AVP **Acct-Session-Time**.
CSCwf60519	Client struggles to connect to the controller's AP due to an invalid PMKID.
CSCwf84639	Cisco Catalyst 9120 AP XOR mode status is not updated, with the radio mode status still being monitored on the Prime Infrastructure (PI).
CSCwf88890	Cisco Catalyst 9800-L AP GUI encounters a display issue where it is stuck loading in **Monitoring > Wireless > AP Statistics > General** for a specific AP 3802.
CSCwf96138	The customer (CU) encounters roaming failure in flex mode local switch central authentication case for the iPhone SE 3rd edition.
CSCwh08892	The controller GUI displays a blank page after the user login page due to a malformed **user pref json.**
CSCwh12481	Cisco Catalyst 9130AXI-E AP does not join the controller with the Tanzania (TZ) country code.
CSCwh14232	The controller does not send Logical Link Control (LLC) or Exchange of Identification (XID) spoofed frames after a mobility event.

Identifier	Headline
CSCwh20334	The controller Change of Authorization (CoA) server key appears blank when entering a new AAA server configuration via Graphical User Interface (GUI).
CSCwh33056	Policy tag description disappears after deleting Wireless Local Area Network (WLAN) location entries in the Cisco Catalyst C9800-80 wireless model.
CSCwh57076	The controller does not forward broadcast ARP requests to the wireless client.
CSCwh70511	The controller Redundancy Management Interface (RMI) flaps with "Closed transport communication channel" messages are observed.
CSCwh71608	Cisco Catalyst 9800-L Mesh AP (MAP) is unable to join through the Root AP (RAP) using Extensible Authentication Protocol (EAP) and flex-bridge site tag.
CSCwh88246	URL Filter not applied after invalid configuration.
CSCwh93462	The controller displays a negative value for APs joined or discovered in the **show wireless stats ap loadbalance summary** feature.
CSCwi02479	Cisco Catalyst C9800-80 AP unexpectedly reloads due to a corrupted value in a stack, leading to a stack overflow.
CSCwi04642	Cisco Catalyst 9800-80 AP does not save the webauth portal IPV4 address.
CSCwi07401	Cisco IOS-XE controller AP encounters an unexpected reboot while collecting wireless client stats using an EEM script.
CSCwi08147	The controller Graphical User Interface (GUI) does not allow modifying QoS policies without automatically setting the **QoS SSID policy** on the policy profile.
CSCwh30078	Cisco Wave 2 APs have multiple processes that crashed while running throughput test.
CSCwh59543	Cisco Catalyst 9120 APs experience a Radio FW_1 crash.
CSCwh63270	Cisco Catalyst 9130AXI APs constantly crash on the Cisco Catalyst 9800-L due to radio failure.
CSCwh68360	Cisco Catalyst 9120 AP encounters a kernel panic crash.
CSCwh81332	Cisco Catalyst 9130 AP encounters kernel panic crash.
CSCwh87903	Cisco Catalyst 9120 AP sends **auth_resp** failures for specific client mac addresses due to **suppressed by MAC filter**.
CSCwh88100	Cisco Aironet 3800 AP encounters kernel panic crash.
CSCwh92425	Cisco Catalyst 9130 AP and Cisco Catalyst 9136 AP are not respecting client Power Save mode.
CSCwi03442	Cisco Catalyst 9130 AP do not forward RTP packets downstream to the client.
CSCwi07094	Apple clients are unable to connect to Flex **WPA2+WPA3 SSID** with Secure Agile Exchange (SAE) enabled and Opportunistic Key Caching (OKC) disabled.

Identifier	Headline
CSCwf79175	Pairwise Master Key ID (PMKID) mismatch between flex central-auth Cisco Wave 2 APs and controller.
CSCwh49406	Cisco Catalyst 9130 AP are spamming syslog controllers with thousands of logs per second.
CSCwh62342	AP FlexConnect fails to respond to a client's mDNS query for airplay service.
CSCwh75431	Cisco Aironet 1815 AP and Cisco Aironet 1830 AP report performance issues across the 5GHz band.
CSCwh93655	Cisco Catalyst 9120 AP displays an unexpected antenna stream of 2x2 in radio at 2.4/5 GHz.
CSCwi08442	The APs are unable to join when Controller-Based Application Recognition (CBAR) is enabled on the controller.
CSCwd63620	The WNCD core encounters a controller crash while modifying rf tag mapping.
CSCwe42200	The controller configured with the radius server **address fqdn**, does not add the second IP resolved by DNS if the addresses are updated.
CSCwh02698	Cisco Catalyst 9800-40 controller sends incomplete Security Group Tag (SGT) to Identity Service Engine (ISE) 3.1 patch 3.
CSCwh59048	The -A domain access point does not join or have radios down when connected to the controller configured for Guatemala (GT).
CSCwh68219	Cisco Catalyst 91xx AP, connected to the controller, does not process the EAP-TLS server Hello.
CSCwh92459	The controller switches experience frequent reloads and system reports. Despite removing redundancy, both switches still crash.
CSCwi10656	The controller encounters high CPU usage due to a WNCD process running out of session IDs.
CSCwe81775	The controller fails to completely delete Apple devices (macOS 13.2.1 and 12.6.0) after sending Extensible Authentication Protocol (EAP) logoff messages.
CSCwh09642	Zone ID was not created or populated for some of the site tags, resulting in IP theft.
CSCwh89539	The controller displays logging output indicating CAPWAP messages are queued.
CSCwi22895	The controller encounters a crash within RRM service.
CSCwh37783	The Lobby Admin page of the controller GUI does not load.
CSCwh22981	WNCD process crashes.
CSCwf68612	The controller reloads unexpectedly due to segmentation fault in the WNCD process.

Identifier	Headline
CSCwf30701	Cisco Aironet 2800 AP and Cisco Catalyst 9120 AP as supplicants do not initate the EAP process until the static IP address is assigned.

Resolved Caveats for Cisco IOS XE 17.9.4a

Identifier	Headline
CSCwh87343	Cisco IOS XE Software Web UI Privilege Escalation Vulnerability. For more information, see Security Advisory: cisco-sa-iosxe-webui-privesc-j22SaA4z.

Resolved Caveats for Cisco IOS XE 17.9.4

CSCwe01579	The WNCD process reloads unexpectedly while creating an RRM client coverage.
CSCwd46815	Cisco Aironet 2800/3800/4800, Cisco Aironet 1562 Series Outdoor APs, Cisco Catalyst IW6300 Series Heavy Duty APs: EAP-TLS fails for the wired clients behind mesh AP.
CSCwd60034	Cisco Aironet 3800 AP radio reloads unexpectedly and displays the 'Beacon Stuck' message.
CSCwd79502	The controller tracks stale entries due to the anchored client receiving IPv4 and IPv6 in different VLANs.
CSCwd91054	Cisco Wave 2 APs do not encrypt EAP_ID_REQ after M1-M4 and do not update PMKID for dot1x OKC.
CSCwe04602	Cisco Wave 2 APs fail to forward traffic to wireless clients for about 60 seconds in the SDA Fabric WLANs.
CSCwe07802	Cisco Aironet 2800/3800/4800, and Cisco Aironet 1562 Series Outdoor APs drop upstream EAP packets.
CSCwe11213	Cisco Catalyst 9130 AP crashes due to radio failure.
CSCwe14729	The controller reboots due to memory corruption when processing DHCP Reply Option82.
CSCwe17593	Cisco Catalyst 9115 AP workgroup bridge (WGB) stops sending traffic to the root AP after about 60 seconds from its initial connection.
CSCwe18012	The standby controller crashes while saving the QoS table.
CSCwe25446	Unexpected reboot experienced due to the WNCD process.
CSCwe27839	Kernel panic observed on Cisco Catalyst 9120 AP during longevity test.
CSCwe30473	The Cisco Wave 2 APs radio firmware reloads unexpectedly because of the RC queue being stuck.

CSCwe38431	The controller re-marks SIP packets from CS3 to CS0 during upstream or downstream when voice CAC is configured.
CSCwe39888	The RRM process crashes while running the Dynamic Channel Assignment (DCA) algorithm.
CSCwe49267	The controller does not send GTK M5 packet to Cisco Wireless IP Phone 8821 after FT roaming between WNCDs.
CSCwe55390	Cisco Aironet 3802 AP experiences buffering when UP6 or voice traffic less than 500ms after Spectralink phone roam causes audio issues.
CSCwe56266	RRM crash observed on the controller during bootup.
CSCwe62694	The WNCD process goes into an infinite loop on customer network with 382 APs.
CSCwe66730	DCA assigned wrong channels after Dynamic Frequency Selection (DFS) events.
CSCwe67580	No CAPWAP data tunnel formed between OEAP and the controller after changing the public IP address.
CSCwe67810	The Cisco Wave 2 APs in FlexConnect standalone mode disconnects clients on DHCP renewal every 18 minutes.
CSCwe70970	Need an option to prioritize KeepAlives in the redundancy port for High Availability SSO deployment.
CSCwe73403	DHCP Option 82 is not added in WLAN with EoGRE tunnel when SVI interface is down.
CSCwe73758	Cisco Catalyst 9115AX AP unable to send beacons stuck on 5-GHz.
CSCwe74653	AP does not send the delete reasons to the controller resulting in stale entries.
CSCwe74874	Cisco Catalyst 9120 AP randomly crashes due to kernel panic.
CSCwe76818	Cisco Catalyst 9800-80 Wireless Controller: Syslog configuration does not reflect in the AP.
CSCwe81552	Transmit Power Control (TPC) does not work as expected in the secondary radio operating in the 5-GHz band.
CSCwe82892	Client connected to FlexConnect AP with profile policy is assigned to VLAN 1 instead of a native VLAN.
CSCwe85742	The controller needs to clear PMKID when it fails to ressurect client entry upon N+1 AP failover.
CSCwe87973	Cisco Aironet 3800 AP reloads unexpectedly due to FIQ or NMI reset.
CSCwe91394	AeroScout T15e tags do not report the temperature data due to extra bytes.
CSCwe99957	The controller does not respond to keepalive from AP after an AP disconnect.
CSCwf04748	AP reloads unexpectedly due to CALLBACK FULL Reset Radio.

CSCwf07264	The WNCD process crashes when accessing the Crimson database.
CSCwf07605	Cisco Catalyst 9105AXW AP and Cisco Aironet 1815W AP: The MAC device cannot get an IP address in the Ethernet port after AAA VLAN override.
CSCwf15582	AP radio reloads unexpectedly as the beacon is stuck.
CSCwf29742	Cisco Catalyst 9120 AP: Firmware crashes when multicast and longevity is run with more than 80 clients.
CSCwf34100	When Samsung device (Galaxy Tab S6 Lite - P610K) tries to associate with a Cisco AP, AP sends association rejected with status code 40.
CSCwf42824	Cisco Catalyst 9105AXW APs do not recover after an upgrade.
CSCwf44027	Usernames go missing randomly for wireless 802.1x clients on the controller GUI or console.
CSCwf44483	The Cisco Catalyst 9120AXI AP: 5-GHz radio remains operationally down when -A domain AP joins the controller for country Panama (PA).
CSCwf50177	Cisco Catalyst 9105AXW AP detects a large number of bad blocks.
CSCwf54714	The controller reloads unexpectedly.
CSCwf55303	Active controller reboots when RP link comes up.
CSCwf67316	The Cisco Aironet 2800/3800/4800 Series APs, Cisco Aironet 1560 Series Outdoor APs, and Cisco Catalyst IW6300 Heavy Duty Series APs may not detect radar on the required levels after CAC time.
CSCwf71255	Client traffic fails after AP N+1 failover and policy update.
CSCwf71906	The controller does not plumb the IPv4 address in IP Source Guard (IPSG) datapath on Central Web Authentication (CWA) SSIDs for clients having single IPv4 address.
CSCwb51757	High channel utilization on 5-GHz radio when channel bonding is set to 40 MHz.
CSCwc49970	Channel 165 on 5-GHz is not allowed on Cisco Aironet 2800, 3800, 4800 APs.
CSCwd08068	Cisco Aironet 1815W AP crashes due to Out-of-Memory (OOM) issues when the WCPD process consumes memory.
CSCwd41463	Cisco Wave 2 APs intermittently stop sending IGMP membership report.
CSCwd56391	The controller does not provide RSSI location data for some of the RFID tags in the database.
CSCwd68141	Rogue containment LRAD is not displayed in the **show wireless wps rogue ap detail** command output.
CSCwd72847	Cisco Catalyst 9115 AP stops transmitting multicast traffic downstream.
CSCwd78416	Cisco Embedded Wireless Controller sends bursts of Virtual Router Redundancy Protocol (VRRP) traffic.

CSCwd86288	Load average warning is displayed even when Cisco Catalyst 9800-80 Series Wireless Controller is healthy.
CSCwd98332	The controller reloads after failing to match the interface ID in the anchor message.
CSCwe00848	Cisco Catalyst 9105 Series APs reload unexpectedly due to kernel panic.
CSCwe06561	It is not possible to delete the EWC core system report files when AP is changed to CAPWAP mode.
CSCwe07297	Cisco Catalyst 9120 AP reloads unexpectedly due to radio firmware crash.
CSCwe15338	Cisco Catalyst 9120 AP: TX is stuck and AP does not respond to the client's probe or authentication.
CSCwe17920	Cisco Catalyst 9124 AP does not forward traffic to workgroup bridge (WGB) after a session timeout.
CSCwe18185	The day 0 factory image for the new out-of-the-box Cisco Catalyst 9130 AP (VID03) does not contain iox.tar.gz.
CSCwe19858	Cisco Catalyst 9130 AP advertises incorrect local power constraint value in the management frames.
CSCwe30429	Cisco Catalyst 9800-L Series Wireless Controllers display the last reload reason as 'reload' instead of 'Critical process wncd fault'.
CSCwe30572	Cisco Wave 2 AP leaks Network Address Translation (NAT) IP from iOX app.
CSCwe32853	Cisco Catalyst 9124AXI AP does not forward Remote LAN (RLAN) traffic to the upstream network.
CSCwe35285	The controller deletes client. This could be triggered by the CSCwd91054 fix.
CSCwe42211	EWC Time Offset is not updated on the GUI.
CSCwe42302	The Inter-Release Controller Mobility (IRCM) client is deleted silently after a profile name mismatch.
CSCwe45553	Reword the error message displayed during one-shot AP Service Pack (APSP) installation to enhance clarity.
CSCwe53639	The controller sends high volume of messages matching 'brain: +(awk|sed)'.
CSCwe63089	The LEDs on the APs sporadically turn white.
CSCwe71081	macOS Setup Assistant: Guest issue is observed.
CSCwe74895	The controller crashes when running the AP packet capture.
CSCwe76817	CAPWAP Maximum Transmission Unit (MTU) discovery issue is reported on the APs.
CSCwe80617	Wireless clients are unable to connect to Cisco Aironet 1830 AP after input or output error messages are displayed.

CSCwe82287	AP prevents a Protected Management Frame (PMF) Wi-Fi Protected Access Version 3 (WPA3) client from associating after the client initiates self-deauthentication.
CSCwe84267	Cisco Wave 2 AP in flex N+1 failover mode does not transmit first CAPWAP data keepalive.
CSCwe88776	EWC capable mesh AP waits three minutes in CAPWAP init.
CSCwe91264	AP reloads unexpectedly when PC is at get_partial_node.isra
CSCwe92462	Client Data Rate chart is skewed by management rate rather than data rate.
CSCwe95127	The controller provides incorrect data for certain APs in response to the SNMP query bsnAPIfDot11BSSID.
CSCwf09008	Cisco Catalyst 9800-CL Wireless Controller crashes sporadically due to WNCD process fault.
CSCwf09259	The AP LED flash automatically switches on after reboot.
CSCwf11117	Cisco Catalyst 9120 AP: Root AP deauthenticates workgroup bridge (WGB) continuously after a roam.
CSCwf14803	The controller web UI menu displays cryptic feature names after upgrade.
CSCwf22225	Cisco Catalyst 9120 APs: Standardize calculation of management frame count across AP chipsets.
CSCwf22788	The **show wireless client summary detail** command output does not display all the IPv6 addresses.
CSCwf42629	VLAN group support for static IP clients when dot1x SSID have SGT through AAA override.
CSCwf45495	Cisco Catalyst 9130 APs fail to start CAPWAP due to interface reset every 52s during the DHCP process.
CSCwf57471	The controller GUI does not respond when enabling Application Visibility and Control (AVC) on wireless policy profiles with special characters.
CSCwf88588	The AP manager crashes during ISSU upgrade to 17.9.3 and causes the controller to go into boot loop.

Resolved Caveats for Cisco IOS XE 17.9.3

Identifier	Headline
CSCwd40731	AP reloads due to kernel panic - not syncing: softlockup: hung tasks.
CSCwd80290	IOS AP image validation certificate failed/expired, causing AP join issues.
CSCvx32806	COS-APs are stuck in bootloop due to image checksum verification failure.
CSCwc10696	Regular ASR support field is disabled for supporting clients.

Identifier	Headline
CSCwc24994	Cisco Aironet 3800 series AP crashes due to kernel panic (PC is at vfp_reload_hw+0x30/0x44).
CSCwc32182	Cisco Catalyst AP 1852: Radio firmware crash is observed.
CSCwc55632	Cisco Catalyst 9124 MAP fails to connect to Cisco Aironet 1562 RAP after first reload of MAP.
CSCwc75732	Cisco Aironet 4800 AP: Firmware radio crash is observed.
CSCwc89183	Controller crash is observed on libewlc_client_dpath_svc.so.
CSCwd02898	Cisco Catalyst 9300 Series Switch is not flushing remote MAC address after roaming to a local AP.
CSCwd04571	Memory leak is observed in wncd process when under load.
CSCwd06122	AP Join issues reported due to stale client entries.
CSCwd08678	Timer is not running state client not deleted by controller.
CSCwd10570	Cisco Catalyst 9130 AP: Beacon with incorrect datarates - different rates for same slot on different BSSIDs.
CSCwd12120	Inject path crash is observed on controller switch on IPv6_qos.
CSCwd26693	N+1 HA for FlexConnect is not working.
CSCwd30828	Cisco Catalyst 9120 AP: Kernel panic crash is observed.
CSCwd35577	Redundancy fails during double bit ECC error
CSCwd39605	Cisco Catalyst 9117 AP reloads unexpectedly due to kernel panic at console_unlock+0x320/0x3ac.
CSCwd41108	Cisco Catalyst 9130AXE AP with Dart connectors are stuck at channel 36.
CSCwd46721	IP Theft occurs due to stale client entries in the ODM database.
CSCwd47741	Controller is failing to update dynamic channel assignment (DCA) channels in radio resource management (RRM) are stuck.
CSCwd52745	Cisco Aironet 3802 AP: Kernel crash is observed.
CSCwd55757	Wave 2 APs: Systemd critical process crash - dnsmasq-host.service failed.
CSCwd56621	Controller GUI logging buffer size display is incorrect.
CSCwd63516	Cisco Catalyst 9120 AP fails EAP-TLS port authentication after Plug and Play (PnP) configuration is pushed.
CSCwd63665	Cisco Catalyst 9800-80 Series Wireless Controller shows high CPU utilization in wncd with 200 APS due to WSA.

Identifier	Headline
CSCwd63861	SIGSEGV crash is observed when incrementing roaming statistics.
CSCwd69780	Controller crashes due to netflow watchdog and observed CPU HOG in wncmgrd due to scale netflow.
CSCwd77823	Cisco Catalyst 9130 AP: Radio firmware crash is observed.
CSCwd79178	Cisco Aironet 1840 OEAP: Crash is observed due to radio failure.
CSCwd81523	Cisco Catalyst 9130 AP is not sending EAP_ID_RESP next assoc-req after PMF client tx deauth in middle of EAP handshake.
CSCwd90472	Adding static IP MAC binding to device tracking fails.
CSCwd90907	Cisco Catalyst 9164 AP: Crash is observed on Radio 1.
CSCwd90909	Cisco Catalyst 9115 AP: Crash is observed on Radio 1.
CSCwd93773	Controller should not enable 2nd 5Ghz radio for 9124E with PoE+ (30W).
CSCwe00248	Poor reassociation behavior is observed between Spectralink 84xx series phones and Cisco Catalyst 9136 APs.
CSCwe08688	EWC: Mesh AP factory reset mode cannot be set to EWC after converting it to CAPWAP and factory-reset.
CSCwb72924	FlexConnect client is intermittently unable to reconnect to an AP.
CSCwc35049	Cisco Catalyst 9136 AP and Cisco Catalyst 9166 AP: AP CLI displays continuous logs printing 'Starting CAF Health check service'.
CSCwc58794	The accounting start messages are not sent when the client username is changed.
CSCwc59814	Disable burst beacon by default, for 11AC Cisco Wave 2 QCA APs.
CSCwc81656	Flash file system corruption is observed on AIR-CAP2702E-K-K9.
CSCwc87688	Cisco Catalyst 9120 AP shows very high noise level on 5-GHz radio.
CSCwd00979	The output of the **show wlan all** command has incorrect WLAN radio policy information.
CSCwd03803	Cisco Aironet 1815I AP reboot: PC is at edma_poll / LR is at dma_cache_maint_page.
CSCwd04025	PI 3.10.1: Associated APs with controller is showing interface "Half duplex".
CSCwd06018	802.11r re-auth failed due to invalid Pairwise Master Key ID (PMKID) while doing inter-WNCD roaming.
CSCwd12754	CAPWAP wireless traffic is getting the same Security Group Tag (SGT) as the corresponding incoming wired traffic.
CSCwd19631	Cisco Catalyst 9120 AP cannot operate in mGig when EEE is enabled on switchport.

Identifier	Headline
CSCwd21996	Cisco Catalyst 9120 AP: CleanAir sensor is crashing.
CSCwd23681	Controller fails to update AP config with error "% Error: no ap_name exists".
CSCwd32107	Cisco Aironet 2700 AP: Ignore CAPWAP_PAYLOAD: AP_LAN_CONFIG payload having invalid RLAN port enable value.
CSCwd34535	Cisco Catalyst 9124 AP does not send dual DFS statistics to the controller.
CSCwd34890	Clients are getting deauth immediately after getting IP address in LWA+LocalSW+CentralAuth.
CSCwd34908	Controller is not following the Dynamic Channel Assignment (DCA) sensitivity threshold.
CSCwd35393	Wireless load balancing affinity incorrectly shows AP site tag as default-site.
CSCwd46091	Cisco Catalyst 9105AXI AP is requesting 30 watts instead of 15.4 watts.
CSCwd46770	License: Remove reporting interval (fixed 8 hours) and change Sync report to a user action.
CSCwd49166	Cisco Aironet 3800 AP is consistently reporting high QoS Basic Set Service (QBSS) load.
CSCwd49861	AIRESPACE-WIRELESS-MIB: bsnAPIfType OID documentation incomplete.
CSCwd52385	AP is not initiating gRPC connection to Cisco DNA Center correctly after token expiry.
CSCwd52938	Wired clients behind workgroup bridge (WGB) are not getting IP address in anchor WLAN.
CSCwd59921	Cisco Catalyst 9130 AP is dropping EAP-TLS frames.
CSCwd60376	Cisco Catalyst 9120 AP: Kernel panic is observed with PC is at pci_generic_config_read+0x34/0xa8.
CSCwd74123	Cisco Catalyst 9105 OEAP: Personal SSID is not advertising HE IE in beacon.
CSCwd74571	Wcpd crashes after reusing freed packets.
CSCwd77188	Profile mismatch counter is not increasing.
CSCwd77188	Cisco Aironet 3802 AP: Broadcasts different power values in beacon country IE.
CSCwd79645	Wireless client are unable to communicate after session timeout when AP dropped once during the session.
CSCwd83840	Cisco Aironet 1830 AP: Wireless clients are unable to connect - "writing to fd 27 failed!".
CSCwd83841	EWC: AP is not sending packets from wired interface to subnet 192.168.129.0/24.

Identifier	Headline
CSCwd95618	The reachability timer of the **device-tracking binding reachable-lifetime** command does not work properly.
CSCwd96376	Unable to login to controller GUI or CLI with the user created by Day 0 Wizard.
CSCwd96489	Tracebacks observed on Cisco Wave 1 AP while writing tags.
CSCwd99656	The **snmp-server host** command is not filtering characters properly (Fails when name is e.g.TEST\).
CSCwe06752	Controller GUI cannot configure HA/SSO if wireless mgmt interface is not configured.
CSCwe11547	Crash is seen on "Critical process rrm fault on rp_0_0 (rc=139)".
CSCwe12057	QoS Page is not loading when access control list (ACL) has double quote special character in the name.
CSCwe13286	On reload, the EWC capable MAP blocklists RAP for CAPWAP timeout
CSCwe18524	AP filter error in the controller GUI when add operation follows edit/view.
CSCwe26846	Console Flood- check_dot1x_feature_status: config change or tams_init_not_done.

Resolved Caveats for Cisco IOS XE 17.9.2

Caveat ID	Description
CSCwa42620	Cisco Catalyst 9130 Access Point drops packets on-air for Phoenix WinNonlin application.
CSCwc09461	Cisco Catalyst 9120 Access Points send Authentication response frames to clients after long de
CSCwc75102	Conversion of Mobility Express Access Points from ME to CAPWAP mode using DHCP optio
CSCwc78435	Cisco Catalyst 9130 Access Point sends incorrect channel list in out-of-band DFS event causin issues.
CSCwd08259	Cisco Catalyst 9120, 9115, and 9105 Access Points experience radio firmware crash with Cisco releases.
CSCvx80422	An access point fails to forward packets when using 10.128.128.127 or 10.128.128.128 address
CSCvz66623	EAP-TLS clients behind the Mesh Access Point (MAP) experience authentication failure.
CSCwb08291	Cisco Catalyst 9105AXW Access Point introduces latency when clients use RLAN ports.
CSCwc05350	Cisco Wave 2 Access Points: CAPWAP MTU flapping occurs due to asymmetric MTU betwee controller and vice-versa.
CSCwc10621	CleanAir statistics are not visible in Cisco Catalyst 9130 Access Points when joined to EWC.
CSCwc38912	Changing an Access Point site or policy tag to a Flex local switching set intermittently causes c failure to local web auth WLANs.

Caveat ID	Description
CSCwc51894	Cisco Catalyst 9117 Access Point reloads unexpectedly due to kernel panic with "dp_print_
CSCwc71198	CAPWAP flapping is observed when VRRPv3 is present in the network.
CSCwc73462	Backslash "\" in the end of the RADIUS servers' shared secret is not allowed for FlexConne
CSCwc81341	Cisco Catalyst 9130 Access Point experiences kernel panic crash in Local mode when full c enabled.
CSCwc05366	Wireless clients cannot reach each other as ARP resolution fails when performing dynamic AAA with SSID.
CSCwc15533	Continuous wncmgrd CPUHOG traceback with scale Flexible NetFlow (FNF) mapping to p 100% wncd utilization.
CSCwc15944	Multicast data is not sent to clients and few Access Points are unable to join the controller.
CSCwc22468	Client traffic fails when client roams between access points with a transition between dot11
CSCwc42784	Client fails to connect when protocol based Quality of Service (QoS) is configured.
CSCwc57227	Controller experiences an unexpected reset resulting in a system report containing a wncd c
CSCwc59518	Cisco Catalyst 9800-80 Wireless Controller crashes when using WLAN profile with 32 char Channel Availability Check (CAC).
CSCwb47040	Controller does not update Radio Frequency Identification (RFID) location properly.
CSCwc26819	Controller does not send LLC or XID spoofed frames after a mobility event.
CSCwc36125	Radio Resource Management (RRM) startup mode gets triggered on every reboot as the cont of the last state.
CSCwc41358	Controller MAC filtering: WLAN profile column displays the WLAN name and description
CSCwc57836	Restore configuration by HTTP mode does not work in EWC.
CSCwc62824	Controller does not send LLC or XID spoofed frames after a mobility event.
CSCwc72047	Access Points operate in disabled RF profile channels in Cisco IOS-XE 17.6.2 release versi
CSCwc76905	Switch Integrated Security Features (SISF) crash is observed when handling the DHCP mes

Resolved Caveats for Cisco IOS XE 17.9.1

Caveat ID	Description
CSCwa38847	Upgrade from CCO profile fails when a guest account (non-Cisco account) is used.
CSCwb22347	Support for special characters in the Image Download profile in EWC.

Troubleshooting

For the most up-to-date, detailed troubleshooting information, visit the Cisco TAC website at:

https://www.cisco.com/en/US/support/index.html

Go to **Product Support** and select your product from the list, or enter the name of your product. Look under **Troubleshoot and Alerts** to find information about the problem that you are experiencing.

Related Documentation

Information about Cisco IOS XE is available at:

https://www.cisco.com/c/en/us/products/ios-nx-os-software/ios-xe/index.html

All the support documentation for Cisco Catalyst 9100 Access Points are available at: https://www.cisco.com/c/en/us/support/wireless/catalyst-9100ax-access-points/tsd-products-support-series-home.html

Cisco Validated Designs documents are available at:

https://www.cisco.com/go/designzone

Cisco Embedded Wireless Controller on Catalyst Access Points

For support information, see the following documents:

- Cisco Wireless Solutions Software Compatibility Matrix
- Cisco Embedded Wireless Controller on Catalyst Access Points Software Configuration Guide
- Cisco Embedded Wireless Controller on Catalyst Access Points Command Reference Guide
- Cisco Embedded Wireless Controller on Catalyst Access Points Online Help

Installation guides for Catalyst Access Points are available at:

https://www.cisco.com/c/en/us/support/wireless/catalyst-9100ax-access-points/products-installation-guides-list.html

For all Cisco Wireless Controller software-related documentation, see:

https://www.cisco.com/c/en/us/support/wireless/catalyst-9800-series-wireless-controllers/tsd-products-support-series-home.html

Wireless Products Comparison

- Use this tool to compare the specifications of Cisco wireless APs and controllers:

  https://www.cisco.com/c/en/us/products/wireless/wireless-lan-controller/product-comparison.html

- Product Approval Status:

  https://prdapp.cloudapps.cisco.com/cse/prdapp/jsp/externalsearch.do?action=externalsearch&page=EXTERNAL_SEARCH

- Wireless LAN Compliance Lookup:

https://www.cisco.com/c/dam/assets/prod/wireless/wireless-compliance-tool/index.html

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 Cisco Trust Portal at https://trustportal.cisco.com/c/r/ctp/trust-portal.html#/.

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

Cisco Connected Mobile Experiences

Cisco Connected Mobile Experiences Documentation

Cisco Catalyst Center

Cisco Catalyst Center Documentation

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business results you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco 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 web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.

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

© 2022 Cisco Systems, Inc. All rights reserved.