Release Notes for Cisco Embedded Wireless Controller on Catalyst Access Points, Cisco IOS XE 17.14.x

First Published: 2024-04-05

Release Notes for Cisco Embedded Wireless Controller on Catalyst Access Points, Cisco IOS XE 17.14.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 IOS XE 17.14.1

Table 1: New and Modified Software Features

Feature Name	Description and Documentation Link
CAPWAP Message Aggregation	This feature aggregates the CAPWAP control messages of the same type waiting in the queue to be transmitted to the AP. The following command is introduced: • **capwap aggregation** For more information, see CAPWAP Message Aggregation.
Kernel Minidump and Trustzone Upgrade	From this release, the Kernel Minidump and Trustzone Upgrade feature offers a more effective method for diagnosing kernel issues. The following command is introduced: • **core-dump kernel type** For more information, see Kernel Minidump and Trustzone Upgrade
Radio Resource Management (RRM) Dynamic Channel Assignment (DCA) Support on Mesh Backhaul	Until the Cisco IOS XE 17.13.1 release, the RRM DCA optimized the root AP (RAP) backhaul radio channel of a mesh subtree by considering the noise, interference, load, and the RF parameter measurements only from the RAP. From this release, the RRM DCA on Mesh Backhaul feature enables DCA to make better channel assignments for a mesh subtree, by having continuous measurements and inputs from the whole mesh tree required to run DCA. The following command is introduced: • **show wireless mesh rrm dca changed** For more information, see Mesh Access Points.
YANG RPC Support for **clear aaa counters** and **clear radius statistics** Commands.	From this release, YANG RPC is supported for the **clear aaa counters** and **clear radius statistics** commands so that they can clear all counters, or specified RADIUS server ID counters to the device.

Interactive help

Interactive help is a user interface feature that

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

Modes of starting the interactive Help

You can start the interactive help in the these ways.

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

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

Additional troubleshooting information

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

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

Important Notes

- EWC GUI slowness is observed after upgrading from Cisco IOS XE 17.9 to 17.12, 17.15, or later, as a result of security API changes in webserver session management. For more information, see CSCwq65843.

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 Catalyst 9117 Series Cisco Catalyst 9120 Series Cisco Catalyst 9124AXE/I/D Cisco Catalyst 9130 Cisco Catalyst 9105AXI	Cisco Aironet 1540 Series Cisco Aironet 1560 Series Cisco Aironet 1815i Cisco Aironet 1815w Cisco Aironet 1830 Series 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

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

Image Type	Supported APs
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	50	1000
Cisco Catalyst 9124AXE/I/D	50	1000
Cisco Catalyst 9130	50	1000

Note

- If 25 to 50 APs have joined the EWC network, the maximum clients on the EWC internal AP is limited to 20.
- From Cisco IOS XE Dublin 17.12.1 onwards, the maximum supported scale in Cisco Catalyst 9120AX Series APs, Cisco Catalyst 9124AX Series APs, and Cisco Catalyst 9130AX Series APs, is reduced to 50 APs from 100 APs and 1000 clients from 2000 clients.

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
Cisco IOS XE 17.14.x	3.2 3.1 3.0 2.7	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.
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.

Browser	Version	Operating System	Status	Workaround
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

Before You Upgrade

- (#CSCwn29592) EWC running the Cisco IOS XE 17.12.x image on Cisco Catalyst 9124AX APs or 9130AX APs is sometimes unable to load Cisco IOS XE 17.15.2 image due to space constraints.

  Workaround:

  - Downgrade first to Cisco IOS XE Cupetino 17.9.6 and then upgrade to Cisco IOS XE 17.15.2.

- The following Remote Procedure Call (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*.

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 17.14.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-universalk9.17.14.01.zip	C9800-AP-universalk9.17.14.01.zip	ap1g7
Cisco Catalyst 9117 Series	C9800-AP-universalk9.17.14.01.zip	C9800-AP-universalk9.17.14.01.zip	ap1g6
Cisco Catalyst 9120 Series	C9800-AP-universalk9.17.14.01.zip	C9800-AP-universalk9.17.14.01.zip	ap1g7
Cisco Catalyst 9124AXE/I/D	C9800-AP-universalk9.17.14.01.zip	C9800-AP-universalk9.17.14.01.zip	ap1g6a
Cisco Catalyst 9130	C9800-AP-universalk9.17.14.01.zip	C9800-AP-universalk9.17.14.01.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 Dublin 17.14.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

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.

Hardware or Software Parameter	Hardware or Software Type
Cisco ISE	See Compatibility Matrix, on page 6.
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
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

Client Type and Name	Driver / Software Version
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)
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

Client Type and Name	Driver / Software Version
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
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

Client Type and Name	Driver / Software Version
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 Issues for Cisco IOS XE 17.14.1

Identifier	Headline
CSCwj02903	Controller CAPWAP Mobility Control and Data Path goes down as it fails to handle Path Maximum Transmission Unit (PMTU) acknowledgement.
CSCwj12705	Virtual Routing and Forwarding (VRF) mismatch between the Cisco 5520 Series Wireless Controller as anchor controller and the Cisco Catalyst 9800-80 Wireless Controller as foreign causes user connection failure.
CSCwi53570	Cisco Catalyst 9800-L Wireless Controller interface connecting to TenGigabitEthernet0/1/0 encounters input/overrun errors.
CSCwj04177	AP undergoing Extensible Authentication Protocol (EAP) fails if the password is more than 31 characters.
CSCwi39752	Cisco Catalyst 9800-40 Wireless Standby Controller unexpectedly becomes unresponsive with the last reload reason 'Critical software exception'.
CSCwj13944	AAA override VLAN is not applied upon roaming in local authentication as the user is placed back in the default VLAN.
CSCwj03060	Cisco Aironet 1815w AP encounters kernel unresponsiveness on image version 17.9.4.205.
CSCwi96176	Cisco Catalyst 9130 and 9166 APs show high channel utilization with one single client connected.
CSCwi99566	Cisco Catalyst 9124AXI-E AP becomes unresponsive due to channel 36 not being supported in the Jordan regulatory domain.
CSCwj00465	Active controller becomes ActiveRecovery when the redundancy port link is down.
CSCwj16668	Wired clients behind a WGB lose network connectivity when doing IRCM roaming from Cisco Catalyst 9800 Wireless Controller to Cisco 5520 Wireless Controller.
CSCwi53998	Cisco Aironet 1815 APs report 0 dBm as the Received Signal Strength Indicator (RSSI) for neighboring APs.
CSCwi99296	Cisco Catalyst 9120 AP encounters kernel unresponsiveness with the PC due to wlc_bmac_suspend_mac_and_wait.
CSCwj08558	Cisco Catalyst 9124 APs do not assign the correct channels where 2.4 GHz is set for clients.
CSCwj25187	Controller does not display the redundancy details on the Web-UI, only on the Command Line Interface (CLI).
CSCwj13842	Controller causes IP theft and client deletion via Address Resolution Protocol (ARP) with DHCP required enabled.

Identifier	Headline
CSCwj29389	Controller encounters memory leak at the CAPWAP control message fragmentation issue.
CSCwj13190	Inventory app shows "Internal Error" for controller that was in Catalyst Center for several releases.
CSCwi83037	Cisco Aironet 4800 AP: Radio Core data files generated Radio 1 During the Longevity testing.
CSCwi04855	Cisco Catalyst 9115 APs disjoin repeatedly with controller traceback.
CSCwj14376	Cisco Catalyst 9800-40 Wireless Controller's mobility tunnels go down after upgrading via In-Service Software Upgrade (ISSU).
CSCwj03495	Cisco Aironet 1562 as Mesh AP (MAP) recognizes Cisco Catalyst 9124 Root AP (RAP) as a parent and completes authentication, but fails in the CAPWAP join because Mesh Adjacency messages are undetected by the RAP.
CSCwj11366	Cisco Wave 2 APs in FlexConnect do not decrypt traffic after Opportunistic Key Caching (OKC) fast roaming is enabled.
CSCwh52553	Cisco Catalyst 9105 AP encounters high utilization and performance issues due to high mDNS traffic.
CSCwj26196	Controller running the IOS XE software encounters an unexpected reset while trying to validate the MAC address with the EWLC_APP_INFRA_ID_MAGIC.
CSCwj34379	Cisco Catalyst 9800-80 Wireless Controller encounters Wireless Network Control daemon (WNCd) issues when accessing Crimson Database.
CSCwj35579	Clients require IP DHCP smart-relay support for controller.
CSCwj42441	Memory leak under the Smand process.
CSCwj34753	Mesh AP reflects back client unicast traffic on the wired port.

Resolved Issues for Cisco IOS XE 17.14.1

Identifier	Headline
CSCwh88320	Cisco Catalyst 9800-40 Wireless Controller encounters false jammer alerts.
CSCwf30701	Cisco Aironet 2800 and Cisco Catalyst 9120 APs as supplicants do not initiate the Extensible Authentication Protocol (EAP) process until a static IP address is assigned.
CSCwf99932	Cisco Catalyst 9120 AP Radio1 becomes unresponsive.
CSCwh57076	Controller does not forward broadcast Address Resolution Protocol (ARP) request to the wireless client.
CSCwh63270	Cisco Catalyst 9130AXI APs unexpectedly become unresponsive due to radio failure.

Identifier	Headline
CSCwf79175	Pairwise Master Key Identification (PMKID) mismatch between FlexConnect central authentication Wave 2 AP and controller for 802.11X-SHA256 on roaming clients.
CSCwf92148	Cisco Catalyst 9120 AP dual 5 GHz allow clients to connect to slot 0 as High Efficiency (HE) clients when 802.11ax is disabled in all WLANs and to slot 1 with the same WLANs HE disabled.
CSCwf13107	Cisco Catalyst 9105 AP becomes unresponsive during longevity test because of Single Client Bridge (SCB) mismatch.
CSCwf10839	Cisco Embedded Wireless Controller sends bursts of Virtual Router Redundancy Protocol (VRRP) traffic, causing the switch port to be down due to the storm-control action configuration on the switch port side.
CSCwh81332	Cisco Catalyst 9130APs encounter kernel unresponsiveness after upgrading to 17.6.6.
CSCwh68219	Cisco Catalyst 91xx AP does not process the Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) server Hello.
CSCwh09642	IP Theft observed due to the zone ID being 0x00000000.
CSCwi64010	Controller accepts the reserved IPv6 multicast address to be configured as a mobility multicast IPv6 address.
CSCwf83278	Controller client traffic fails in N+1 mode when AP sends CLIENT_DEL_STOP_REASSOC.
CSCwi96508	Cisco Wave 2 APs allowing SKC roam cause client deletion with the reason as INVALID_PMKID.
CSCwf53520	Cisco Aironet 1815 AP encounters kernel unresponsiveness.
CSCwi18057	Controller encounters a 4-way handshake failure and a missing M3 packet.
CSCwf68131	Cisco Catalyst 9105AXW APs detect bad block monitoring and repair.
CSCwi20933	FlexConnect client is unable to perform Secure Agile Exchange (SAE) authentication due to the controller rejecting assoc-req with a Pairwise Master Key Identification (PMKID) mismatch.
CSCwh92425	Cisco Catalyst 9130 and 9136 APs do not honor power saving mode.
CSCwh54762	Cisco Catalyst 9120 AP encounters kernel unresponsiveness due to not syncing: assert:"0" failed: file "wlc_fifo.c:960".
CSCwh20306	Cisco Wave 2 APs hyperlocation is broken if aWIPS is enabled.
CSCwi22895	Controller becomes unresponsive within Radio Resource Management (RRM) service due to ReloadReason=Critical process rrm fault on rp_0_0 (rc=134).
CSCwi64652	802.11ax APs running IoT application do not reset the BLE interface after 100 attempts.

Identifier	Headline
CSCwi08147	Controller's GUI does not allow modifying QoS policies without having the "QoS Service Set Identifier (SSID) policy" automatically set on the policy profile.
CSCwf07384	Wired clients behind the Cisco Catalyst 9105 AP RLAN face limited connectivity and can't pass any traffic.
CSCwf65794	Cisco Aironet 1852 AP reloads unexpectedly due to radio failure.
CSCwh74663	Cisco Aironet 2800, 3800, 4800, 1560 APs and Cisco Catalyst IW6300 AP do not send QoS data frames downstream.
CSCwh29924	Cisco Catalyst 9105, 9115, and 9120 AP WGB Antenna-a encounters a malfunction if the configuration is ab-antenna.
CSCwf52815	Cisco Wave 2 APs improve the PMTU Discovery mechanism to be able to honor the ICMP unreachable MTU value and recalculate the AP PMTU.
CSCwf72320	Cisco Catalyst IW916x APs and Cisco Catalyst 9105, 9130, and 9136 APs become unresponsive with the reason LED_APP or sxpd.
CSCwi48980	Controller local password policy does not take effect on GUI login as expected.
CSCwi04705	Controller does not send the broadcast Gratuitous Address Resolution Protocol (gARP) on behalf of the client on inter-controller roaming events.
CSCwh89539	Controller queues CAPWAP messages for longer than x seconds with client throttling turned on.
CSCwh30996	PDU type in the transmit (Tx) packet for iBeacon in dual mode needs to be changed to adv_non_connectable_ind.
CSCwh59543	Cisco Catalyst 9120 AP becomes unresponsive leading to a Capwapd Crash during Scale Longevity.
CSCwf91557	Cisco Wave 2 APs stop the PMTU Discovery mechanism after reaching the maximum hardcoded value.
CSCwi35946	Cisco Catalyst 9120 AP encounters kernel unresponsiveness.
CSCwf12301	Watchdog Reset (wcpd) Transmit (Tx) retry number is not MAC Service Data Unit (MSDU)-based.
CSCwh74415	FlexConnect local switching APs per client rate limit do not work.
CSCwi88967	Cisco Catalyst 9120 APs disconnect due to Port Status Monitor (PSM) microcode watchdog CS00012333933.
CSCwf78066	APs managed by the controller display the "No radios in the selected band" message in the Cisco Catalyst Center heat map.
CSCwf13804	APs fail to onboard new client associations with ‘No buffer space available’ messages.

Identifier	Headline
CSCwh56147	Controller is missing Simple Network Management Protocol (SNMP) Object ID (OID) for AP Location Tag.
CSCwh92459	Controller unexpectedly becomes unresponsive with ReloadReason "Critical process wncd fault on rp_0_0".
CSCwh20944	Cisco Catalyst 9120 AP encounters kernel unresponsiveness - not syncing: assert:"done" failed: file "phy_ac_radio.c:6141.
CSCwi34051	Cisco Aironet 2800 AP encounters FIQ/NMI reset due to PC at wl_get_staid_info.
CSCwi95945	Cisco Catalyst 9130 APs stop forwarding router advertisements for FlexConnect Local Switching/Local Authentication after 4-6 hours of uptime.
CSCwe52756	Cisco Catalyst 9120 AP sends Ready to Send (RTS) with 6 Mbps when this rate is configured as unsupported (CS00012284859).
CSCwi07401	Controller encounters an unexpected reboot while collecting wireless client stats with the Embedded Event Manager (EEM) script.
CSCwh49810	Audit session ID changes and client loses network access after inter- Wireless Network Control Daemon (WNCD) roam.
CSCwh82872	Cisco Catalyst 9115AXI-S AP association request dropped on the Cisco Catalyst 9800-80 Wireless Controller.
CSCwh87903	Cisco Catalyst 9120 AP sends authorization response failures for specific MAC addresses due to "suppressed by MAC filter".
CSCwi69251	Cisco Catalyst 9800-40 Wireless Controller becomes unresponsive on Critical process Radio Resource Management (RRM) fault on rp_0_0.
CSCwf95868	Single Band Broadcom (BCM) WGB Radio 0 Transmit (Tx) power decreased by nearly 20 dBm while configuring antenna number.
CSCwf83292	Cisco Catalyst 9130 AP does not send DHCP Offer and Acknowledgement (ACK) Over the Air (OTA) through the radio interface to the client.
CSCwj10697	Cisco Catalyst 9124AX AP experiences image upgrade failure.
CSCwi67013	Cisco Aironet 2800 AP on Taiwan domain is unable to send Wi-Fi signals on channels 52, 120, 124 and 128.
CSCwi69093	Controller GUI shows incorrect number of clients connected to the AP.
CSCwi19804	Cisco Catalyst 9105, 9115, 9120 APs experience radio misconfiguration after AP reloads in admin state down.
CSCwh75431	Cisco Aironet 1830, 1850 APs report false high channel utilization, which causes performance isues on 5 GHz band.
CSCwi52692	Cisco Catalyst 9130 AP moves Universal PoE spare pair to turn off over CDP.

Identifier	Headline
CSCwh27366	Cisco Aironet 3800 AP radio firmware becomes nonoperational with reset code 2.
CSCwh62342	mDNS gateway does not respond correctly when Location Specefic Services filter is enabled in the 5-GHz band on FlexConnect AP.
CSCwf50177	Cisco Catalyst 9105AXW AP experiences large count of bad physical eraseblocks.
CSCwh31966	Controller becomes nonoperational on WNCd process during database termination.
CSCwh18613	Encrypted wireless mesh pre-shared key changes when "password encryption aes" is in use.
CSCwi28174	Layer 3 multicast packets are sent on native VLAN when VLAN ID 1 is selected on policy profile with AAA override.
CSCwf93992	Cisco Aironet 2800 FlexConnect APs are unable to process EAP-TLS fragmented packets if delay is more than 50ms.
CSCwi28172	Cisco Catalyst 9120 AP experiences kernel panic with PC at wlc_bmac_suspend_mac_and_wait+0x3c/0x488 [wl] CS00012321648.
CSCwf81866	Radio 0 WGB configuration is not backed up correctly when doing a TFTP backup of the configuration.
CSCwf63818	Cisco Aironet 1832 AP running on release IOS XE Cupertino 17.9.2 experiences kernel panic.
CSCwh58099	Controller allows client reconnection after client deletion and Change of Authorization (CoA) termination.
CSCwf83132	Controller does not send 802.11r mobility payload on mobility group name change to FlexConnect AP causing MDID mismatch.
CSCwi35699	Cisco Catalyst 9120 AP detects its BSSID as malicious after channel resets.
CSCwi47294	Per client rate limit with FlexConnect AP is not functioning.
CSCwf40553	Cisco Catalyst 9115, 9120AX APs do not allow channel 165 for -Z domain.
CSCwh81071	Slot 2 is down for GB country after performing factory reset.
CSCwi08442	APs are unable to join when CBAR is configured on controller.
CSCwj01446	Personal Identity Verification (PIV) authentication requires an additional backslash in the redirection URL to work successfully.
CSCwi07094	Apple clients are unable to connect to FlexConnect AP when WPA3 is enabled.
CSCwi06785	Controller does not send IPv4 GARPs or IPv6 NA for wireless clients in RUN state after a switchover.
CSCwf59348	Cisco Catalyst 9105, 9115, and 9120 APs set the maximum transmit power level to -128 dBm in Country IE.

Identifier	Headline
CSCwh09879	Cisco Wave 2 APs in FlexConnect mode do not allow clients to connect and sends association-response failure after changing country code.
CSCwh30078	Cisco Wave 2 APs become nonoperational repeatedly in throughput testing.
CSCwh88100	Cisco Aironet 3800 AP becomes nonoperational due to kernel panic with PC at skb_unlink+0x40/0x54.
CSCwe24263	Cisco Catalyst 9130 experiences inconsistent transmission power levels advertised in the country information of beacon frame causing client-side issues.
CSCwf94863	Cisco Catalyst 9115 AP becomes nonoperational due to kernel panic with PC/LR is at drop_pagecache_sb+0x78/0x110.
CSCwh88246	AP does not allow to apply URL filter after invalid configuration.
CSCwi72191	VLAN change on the AP port results in unsuccessful update of IPv6 routes on Wave 2 AP.
CSCwf91445	Controller shares accounting information for PSK local authentication WLANs.
CSCwi75759	Controller reloads due to critical process WNCd fault.
CSCwi11182	Memory leak occurs when no RADIUS server is reachable.
CSCwh27425	Cisco Catalyst 9115AX AP does not forward a part of the CAPWAP data packets to the uplink direction.
CSCwi42112	MAC address of wired clients are being learned from the Cisco Catalyst 9124 MAP.
CSCwi08073	Controller receives false notifications for reaching maximum client limit.
CSCwh59048	APs in the 5-GHz band remains in down state for -A domain access points in Guatemala.
CSCwi19481	Cisco Catalyst 9130 APs stop forwarding router advertisements after 4-6 hours of operation.
CSCwi83124	Pop-ups are not displayed correctly in dark mode in the controller.
CSCwh37783	Controller is unable to load lobby admin page.
CSCwf62051	Access point unexpectedly reloads due to kernel panic with mDNS enabled.
CSCwi11038	Cisco Catalyst 9115 OEAP experiences kernel unresponsiveness.
CSCwh35072	Cisco Aironet 3800 AP reloads unexpectedly due to FIQ/NMI reset.
CSCwh99036	Controller experiences WNCd abnormalities when processing the AP supported channels.
CSCwh42002	Controller becomes nonoperational with WNCd core while processing CAPWAP data.
CSCwh61011	Cisco Catalyst 9120 and 9115 APs unexpectedly disjoin from the controller and do not establish DTLS again.

Identifier	Headline
CSCwf42824	Cisco Catalyst 9105AXW APs do not recover after upgrade.
CSCwh68360	Cisco Catalyst 9120 AP experiences kernel panic due to wlc_key_set_data in 17.9.4 CS00012316343.
CSCwi96089	Cisco Wave 2 APs do not plumb keys after session timeout reauthentication.
CSCwh50681	New SSID arp0v0 is broadcast only after a Cisco IOS-XE Cupertino 17.9.3 wireless upgrade.
CSCwf67316	Cisco Aironet 2800, 3800, 4800, 1560, IW6300 APs may not detect radar on the required levels after CAC time.
CSCwe81775	Apple devices are not deleted after sending EAP messages.
CSCwf69377	Controller might become nonoperational within IOSd during an update to SPAN source ports.
CSCwh68768	Controller displays public cloud 17.9.3 error while configuring basic wireless setup.
CSCwi03442	Cisco Catalyst 9130 AP does not honor U-APSD trigger frame resulting in RTP stream disruption.
CSCwh08625	Cisco Catalyst 9105, 9115, 9120 APs experience kernel panic with PC at _raw_spin_unlock CS00012303664.
CSCwi50732	VLAN Group Support for DHCP and Static IP Clients feature does not work on FlexConnect Central Switching mode.
CSCwh91254	Monitoring PHY Health check on Broadcom APs
CSCwh20334	Change of Authorization (CoA) server key appears blank on the controller GUI.
CSCwh49406	Cisco Catalyst 9130 AP generates excessive CleanAir syslogs.
CSCwh33190	Cisco Catalyst 9115 AP in local mode becomes nonoperatioanl due to kernel panic.
CSCwh61007	Controller becomes nonoperational when provisioning multiple APs.
CSCwh33056	Policy tag description disappears after deleting WLAN location entries.
CSCwf83515	Inconsistent transmission power levels advertised in Country information of beacon frame causes client-side issue.
CSCwf45495	Cisco Catalyst 9130 APs do not start CAPWAP due to interface reset while waiting for IP address from DHCP.
CSCwi92439	Cisco Aironet 1815 APs report high channel utilization in the 5-Ghz band.
CSCwi55714	Controller unexpectedly reboots when handling NMSP TLS connection.
CSCwi28382	Controller experiences unexpected resets with the following message: Log message: %PMAN-3-PROCHOLDDOWN: R0/7: wncd: The process wncd has been helddown (rc 134)

Identifier	Headline
CSCwf64009	Cisco Aironet 1815 AP leaks RLAN VLAN traffic with looped port.
CSCwi54064	APs in same controller classify each other as rogue and sends "AP Impersonation" alert.
CSCwh76420	Controller becomes nonoperational while performing ISSU upgrade.
CSCwi81972	Cisco Wave 2 APs should check CAPWAP payload sanity before deleting it.
CSCwj04904	Cisco Catalyst 9300LM switch is not compatible with Cisco Aironet 1815 AP when it is connected on a port with Cisco Unified IP Phone 7945G.
CSCwh44793	Cisco Catalyst 9130 AP on IOS XE Amsterdam 17.3.6 fails to join with error to set FT data in BSSID after site-tag is changed on controller.
CSCwi22270	Cisco Catalyst 9120 AP experiences radio unresponsiveness during longevity run test on IOS XE 17.13.
CSCwh20934	Cisco Catalyst 9120 AP and Cisco Aironet 2800 AP reboot repeatedly due to Systemd critical process unresponsiveness when joining controller that runs on IOS XE Amsterdam 17.9.3.
CSCwi05672	Wireless Driver is unable to decrypt ICAP packets in Cisco Catalyst 9130 AP.
CSCwh01589	Cisco Catalyst 9120AXE AP remains at u-boot and with multiple failure messages.
CSCwi66582	Controller returns with error while uploading backup file with FTP on GUI.
CSCwi22847	Controller becomes nonoperational after receiving analytics from AP.

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

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)

© 2024 Cisco Systems, Inc. All rights reserved.