Release Notes for Cisco Embedded Wireless Controller on Catalyst Access Points, Cisco IOS XE 17.13.x

First Published: 2023-12-08

Release Notes for Cisco Embedded Wireless Controller on Catalyst Access Points, Cisco IOS XE 17.13.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 17.13.1

Table 1: New and Modified Software Features

Feature Name	Description and Documentation Link
Cisco Aironet Wave 2 and Catalyst Access Point Image Management	A new command is introduced to display a brief information about the AP image details: • **show ap image details** The **show ap config general** command has been enhanced to view the general configuration information of all Cisco APs.

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
Dublin 17.13.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*.

Upgrade Path to Cisco IOS XE 17.13.x

Table 7: Upgrade Path to Cisco IOS XE 17.13.x

Current Software	Upgrade Path for Deployments with 9130 or 9124	Upgrade Path for Deployments Without 9130 or 9124
16.10.x	—	Upgrade first to 16.12.5 or 17.3.x and then to 17.13.x.
16.11.x	—	Upgrade first to 16.12.5 or 17.3.x and then to 17.13.x.
16.12.x	Upgrade first to 17.3.5 or 17.6.x or later and then to 17.13.x.	Upgrade first to 17.3.5 or 17.6.x or later and then to 17.13.x.
17.1.x	Upgrade first to 17.3.5 or 17.6.x or later and then to 17.13.x.	Upgrade first to 17.3.5 or 17.6.x or later and then to 17.13.x.
17.2.x	Upgrade first to 17.3.5 or 17.6.x or later and then to 17.13.x.	Upgrade first to 17.3.5 or 17.6.x or later and then to 17.13.x.

Current Software	Upgrade Path for Deployments with 9130 or 9124	Upgrade Path for Deployments Without 9130 or 9124
17.3.1 to 17.3.4	Upgrade first to 17.3.5 or 17.6.x or later and then to 17.13.x.	Upgrade first to 17.3.5 or 17.6.x or later and then to 17.13.x.
17.3.4c or later	Upgrade directly to 17.13.x.	Upgrade directly to 17.13.x.
17.4.x	Upgrade first to 17.6.x and then to 17.13.x.	Upgrade first to 17.6.x and then to 17.13.x.
17.5.x	Upgrade first to 17.6.x and then to 17.13.x.	Upgrade first to 17.6.x and then to 17.13.x.
17.6.x	Upgrade directly to 17.13.x.	Upgrade directly to 17.13.x.
17.7.x	Upgrade directly to 17.13.x.	Upgrade directly to 17.13.x.
17.8.x	Upgrade directly to 17.13.x.	Upgrade directly to 17.13.x.
17.9.x	Upgrade directly to 17.13.x.	Upgrade directly to 17.13.x.
17.10.x	Upgrade directly to 17.13.x.	Upgrade directly to 17.13.x.
17.11.x	Upgrade directly to 17.13.x.	Upgrade directly to 17.13.x.
17.12.x	Upgrade directly to 17.13.x.	Upgrade directly to 17.13.x.

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 17.13.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 8: 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-universalk9.17.13.01.zip	C9800-AP-universalk9.17.13.01.zip	ap1g7
Cisco Catalyst 9117 Series	C9800-AP-universalk9.17.13.01.zip	C9800-AP-universalk9.17.13.01.zip	ap1g6
Cisco Catalyst 9120 Series	C9800-AP-universalk9.17.13.01.zip	C9800-AP-universalk9.17.13.01.zip	ap1g7
Cisco Catalyst 9124AXE/I/D	C9800-AP-universalk9.17.13.01.zip	C9800-AP-universalk9.17.13.01.zip	ap1g6a
Cisco Catalyst 9130	C9800-AP-universalk9.17.13.01.zip	C9800-AP-universalk9.17.13.01.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 9: Test Configuration for Interoperability

Hardware or Software Parameter	Hardware or Software Type
Release	Cisco IOS XE Dublin 17.13.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.
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 10: 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
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)

Client Type and Name	Driver / Software Version
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
ASCOM SH1 Myco2	Build 2.1
ASCOM SH1 Myco2	Build 4.5
ASCOM Myco 3 v1.2.3	Android 8.1

Client Type and Name	Driver / Software Version
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
Zebra MC40N0	Android Ver: 4.1.1
Zebra MC92N0	Android Ver: 4.4.4
Zebra TC51	Android 7.1.2

Client Type and Name	Driver / Software Version
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 17.13.1

Identifier	Headline
CSCwe81775	Apple devices are not deleted after sending Extensible Authentication Protocol (EAP) logoff messages.
CSCwh57076	Controller is not forwarding broadcast address resolution protocol (ARP) request to wireless client.
CSCwh63050	Controller is sending Internet Group Management Protocol (IGMP) queries using client VLAN gateway ip address that is not present in the controller and with controller macaddress.
CSCwh66453	Run state client (after successful webauth) is not able to pass traffic.
CSCwh68219	Cisco Catalyst 9100 Series AP is not processing Extensible Authentication Protocol (EAP)-Transport Layer Security (TLS) server Hello.
CSCwh74415	Per client rate limit with FlexConnect local switching APs is not working.
CSCwh88246	URL filter is not applied after invalid configuration.
CSCwh92425	Cisco Catalyst 9130 and 9136 APs do not consider power save mode.
CSCwi06785	Controller is not sending IPv4 Gratuitous ARP (GARP) or IPv6 NA for wireless client in RUN state after switchover.
CSCwi07094	Apple client is not able to connect to flex Wi-Fi Protected Access (WPA) 2 + WPA3 SSID with Simultaneous Authentication of Equals (SAE) enabled and Opportunistic Key Caching (OKC) disabled.
CSCwi16104	A dbm crash is observed at VLAN list retrieval.
CSCwi18057	4-way handshake failure, missing M3 packet.
CSCwi22847	Cisco Catalyst 9800-80 Controller crashes after receiving analytics from AP.
CSCwf95319	AP Radio 0 experiences a crash caused by a stuck beacon on the AP.
CSCwd71613	AP detects its own BSSID as malicious after a channel reset.
CSCwf90946	Cisco Catalyst 9130 AP doesnt forward 802.1x "Identity Request" with wireless phones.
CSCwh73374	Cisco Catalyst 9800-80 Controller crashes due to puntinject keepalive process.
CSCwi21444	AP traps are not getting updated to Cisco DNA Centre when AP joins the controller with misconfigured state.

Resolved Caveats for Cisco IOS XE 17.13.1

Identifier	Headline
CSCwh42002	Controller crashes with wireless network control deamons (WNCD) core while processing CAPWAP data.
CSCwh06834	Using special characters in the password while generating trustpoint generates an invalid trustpoint.
CSCwf86242	Controller reloads unexpectedly with CAPWAP window size set to 0.
CSCwh61007	Controller is crashing constantly whenever it provisions multiple APs.
CSCwh76420	Controller crashes while performing In-Service Software Upgrade (ISSU) upgrade.
CSCwf78066	Cisco DNA Center 2.3.3.7: "No radios in the selected band" message on the floor map.
CSCwh18613	Encrypted mesh pre-shared key changes each time "password encryption aes" is applied.
CSCwh56147	SNMP OID for AP location tag is missing on the controller.
CSCwh58099	After client deletion and Change of Authorization (CoA) terminiate, controller allows client reconnect.
CSCwh92459	Controller reloads unexpectedly with WNCD fault on rp_0_0.
CSCwh49810	Audit session ID changes after inter-WNCD roam.
CSCwh89539	CAPWAP messages are queued for longer than x seconds when client throttling is turned on.
CSCwh59420	Cisco Catalyst 9136 AP is crashing.
CSCwf68612	Controller reloads unexpectedly due to segmentation fault in WNCD process.
CSCwf99932	Cisco Catalyst 9120 AP: Radio1 is crashing.
CSCwf12301	WCPD tx retry count is always 0.
CSCwh87343	Cisco IOS XE Software Web UI privilege escalation vulnerability.
CSCwf36752	Terminal Access Controller Access-Control System (TACACS) failed to encrypt the secret key if we use fully qualified domain name (FQDN) as TACACS+ address when configured for first time.
CSCwf13804	Cisco Catalyst 9120 APs are randomly failing to onboard new client associations.
CSCwf99906	Network time protocol (NTP) authentication that is removed after a reload is using more than 16 bytes.
CSCwf21390	Duplicate Access-Request messages with CTS client username is seen when multiple RADIUS servers are configured.
CSCwf66661	The sm_device_count_list takes too long to populate leading to websocket termination.

Identifier	Headline
CSCwh27366	AP radio firmware crashes with reset code 2.
CSCwe11213	Cisco Catalyst 9130 AP crashes due to radio recovery failure.
CSCwf13107	Cisco Catalyst 9105 AP: Radio crash is observed.
CSCwh09879	Cisco Wave 2 APs in FlexConnect mode is sending assoc-resp failure with status code 12 and AID 0 after changing country code.
CSCwh33190	Cisco Catalyst 9115 AP (Local Mode) crashes due to kernel panic.
CSCwh20306	Cisco Wave 2 AP: Cisco Hyperlocation feature is broken when Advanced Wireless Intrusion Prevention System (aWIPS) is enabled.
CSCwf59348	Cisco Catalyst 9105/9115/9120 AP: The beacon is set to Max Transmit Power Level of 128 dBm for Ireland.
CSCwf61881	Cisco Catalyst 9166D1 AP changes country code to UX domain and prevents setting it to standard power.
CSCwh74663	Cisco Aironet 3800 AP is not sending Quality of Service (QoS) data frames downstream due to RadarDetected flag as TRUE.
CSCwf83278	Client traffic fails with N+1 when AP sends CLIENT_DEL_STOP_REASSOC.
CSCwh08625	AP kernel panic crash is observed (at _raw_spin_unlock).
CSCwe24263	Cisco Catalyst 9130 AP: Inconsistent Tx power levels are advertised in beacons.
CSCwf53520	Cisco Aironet 1815 AP: Kernel panic crash is observed.
CSCwf94863	Cisco Catalyst 9115 AP: Kernel panic crash is observed (at drop_pagecache_sb+0x78/0x110).
CSCwh50681	New SSID arp0v0 is being broadcasted after an upgrade.
CSCwf60151	Memory leak with pubd on controller due telemetry connection flap.
CSCwf91445	Controller pushes accounting information for preshared key (PSK) local authentication WLANs.
CSCwf29742	Cisco Catalyst 9120 AP: Firmware crash is observed while running multicast and longeivity with more than 80 clients.
CSCwf64009	Cisco Aironet 1815 AP is leaking Remote LAN (RLAN)-VLAN traffic with looped port.
CSCwf95868	The Tx power of single- band BCM workgroup bridge (WGB) radio 0 is decreased by nearly 20 dBm after configuring antenna number.
CSCwh11858	Cisco Switch running IOS-XE software crashes when removing Fully Qualified Domain Name (FQDN) Access Control List (ACL).
CSCwf83292	Cisco Catalyst 9130 AP is not sending DHCP offer and ACK over the air to clients.

Identifier	Headline
CSCwh27425	Cisco Catalyst 9115AX AP is not forwarding a part of CAPWAP data packets to the uplink direction.
CSCwf68131	Cisco Catalyst 9105AXW AP: Large number of bad blocks are detected.
CSCwh54762	A kernel panic occurs as a result of failure to synchronize (assert:"0" failed: file "wlc_fifo.c:960").
CSCwf10839	Bursts of Virtual Router Redundancy Protocol (VRRP) traffic sent from the Cisco Embedded Wireless Controller on Cisco Catalyst Access Points and Switch port get down due to storm-control action.
CSCwf07384	Wired client behind Cisco Catalyst 9105 RLAN is not able to pass traffic.
CSCwf65794	Cisco Aironet 1852 AP reloads unexpectedly due to radio failure (radio recovery failed).
CSCwf62051	Cisco Aironet 1815W AP crashes due to kernel panic.
CSCwh29924	Cisco Catalyst 9105/9115/9120 AP WGB: Antenna-a couldn't function properly if configuration is ab-antenna.
CSCwf52815	Cisco Wave 2 AP: Improve Path Maximum Transmission Unit (PMTU) discovery mechanism to be able to honor the Internet Control Message Protocol (ICMP) unreachable maximum transmission unit (MTU) value.
CSCwh20934	CiscoWave 2 APs are reloading due to Systemd critical process crash.
CSCwh35072	Cisco Aironet 3800 AP reloads unexpectedly due to Fast Interrupt Request (FIQ)/Non-Maskable Interrupt (NMI) reset.
CSCwf93992	Cisco Aironet 2800 APs in FlexConnect mode are not processing Extensible Authentication Protocol (EAP)-Transport Layer Security (TLS) fragmented packets if delay is more than 50 ms.
CSCwf81866	Radio 0 WGB configuration is not backed up correctly when doing a TFTP backup of the configuration.
CSCwf63818	Cisco Aironet 1832 AP: Kernal panic crash is observed.
CSCwh61011	Cisco Catalyst 9120 and 9115 APs unexpectedly disjoins from the controller and is not able to establish Datagram Transport Layer Security (DTLS again.

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)

© 2023 Cisco Systems, Inc. All rights reserved.