Release Notes for Cisco Embedded Wireless Controller on Catalyst Access Points, Cisco IOS XE Cupertino 17.7.x

First Published: 2021-12-07

Release Notes for Cisco Embedded Wireless Controller on Catalyst Access Points, Cisco IOS XE Cupertino 17.7.x

Note The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

Introduction to Cisco Embedded Wireless Controller on Catalyst Access Points

The Cisco Embedded Wireless Controller on Catalyst Access Points is a version of the Cisco IOS XE-based controller software on Catalyst access points. In this solution, a Catalyst access point (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 Digital Network Architecture (DNA) Center, Netconf/Restconf, web-based GUI, or CLI.

What's New in Cisco Embedded Wireless Controller on Catalyst Access Points, Cisco IOS XE Cupertino 17.7.1

Table 1: New and Modified Software Features

Feature Name	Description and Documentation Link
Guest Anchor with Centralized EoGRE	The Guest Anchor with Centralized EoGRE feature for EWC allows you to provide internet services to wireless guest clients, with the help of the Guest Anchor with Centralized EoGRE feature. For more information, see the chapter Guest Anchor with Centralized EoGRE.
Fast Teardown for a Mesh Access Point	This feature detects the Root Access Point (RAP) uplink failure and addresses the fast teardown of a mesh network when an uplink failure occurs. The following commands are introduced: • **fast-teardown** • **wireless profile mesh** **Note** Fast Teardown for Mesh APs is not supported on Cisco Industrial Wireless (IW) 3702 Access Points. For more information, see the chapter Mesh Access Points .
Smart Licensing Using Policy: Factory-installed Trust Code	For new hardware orders, a trust code is now installed at the time of manufacturing. Note: You cannot use a factory-installed trust code to communicate with CSSM.
Smart Licensing Using Policy: Support for Trust Code in Additional Topologies	A trust code is automatically obtained in topologies where the product instance initiates the sending of data to *CSLU* and in topologies where the product instance is in an air-gapped network.
Smart Licensing Using Policy: RUM Report Optimization and Availability of Statistics	RUM report generation and related processes have been optimized. This includes a reduction in the time it takes to process RUM reports, better memory and disk space utilization, and visibility into the RUM reports on the product instance (how many there are, the processing state each one is in, if there are errors in any of them, and so on).

Feature Name	Description and Documentation Link
Smart Licensing Using Policy: Support to Collect Software Version Through Smart License Agent	If version privacy is disabled (**no license smart privacy version** global configuration command), the Cisco IOS-XE software version running on the product instance and Smart Agent version information is *included* in the RUM report.
Smart Licensing Using Policy: Account Information Included in the ACK and show command outputs	A RUM acknowledgement (ACK) includes the Smart Account and Virtual Account that was reported to, in CSSM. You can then display account information using various **show**commands. The account information that is displayed is always as per the latest available ACK on the product instance.
Smart Licensing Using Policy: CSLU Support for Linux	CSLU can now be deployed on a machine (laptop or desktop) running Linux.
Support for Federal Information Processing Standard (FIPS) Mode in Mesh Access Points	From this release onwards, FIPS mode is supported in Mesh Access Points.
Wi-Fi Protected Access 3 Hash-to-Element (H2E) Support for SAE Authentication	The Hash-to-Element (H2E) is new method for PWE (Password Element) generation which is used in the SAE protocol. It is a computationally efficient technique to mitigate side-channel attacks. The following are the supported PWE methods in the WLAN configuration: • h2e—Hash-to-Element only; disables HnP. • hnp—Hunting and Pecking only; disables H2E. • Both-h2e-hnp—Both Hash-to-Element and Hunting and Pecking support (Is the default option). The following command has been modified: • **security wpa akm sae pwe {h2e | hnp | both-h2e-hnp}** For more information, see the chapter Support for Hash-to-Element for Password Element in SAE Authentication.

Table 2: New and Modified GUI Features

Feature Name	GUI Path
Fast Teardown for a Mesh Access Point	• **Configuration** > **Wireless** > **Mesh** > **Profiles**
Guest Anchor with Centralized EoGRE	• **Configuration** > **Tags & Profiles** > **EoGRE**

Feature Name	GUI Path
Wi-Fi Protected Access 3 Hash-to-Element (H2E) Support for SAE Authentication	• **Configuration** > **Tags & Profiles** > **WLANs**

Note Cisco Catalyst 9136 series Access Points do not run Cisco Embedded Wireless Controllers (EWC) and does not join EWC on access points.

Interactive Help

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

You can start the interactive help in the following ways:

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

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

The following features have an associated interactive help:

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

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

- Navigate to **Preferences > Privacy**.
- On the **Website tracking** field, uncheck the checkbox to disable **Prevent cross-site tracking**.
- On the **Cookies and website data** field, uncheck the checkbox to disable **Block all cookies**.

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 3: 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 Series 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 Series Cisco Catalyst 9105AXW Cisco Catalyst 9105AXI Cisco Catalyst Industrial Wireless 6300 Heavy Duty Series Access Points Cisco 6300 Series Embedded Services Access Points

Table 4: 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

Image Type	Supported APs
ap1g5	Cisco Aironet 1815i Cisco Aironet 1815w Cisco Aironet 1540 Series Cisco Aironet 1850 Series
ap1g6	Cisco Catalyst 9117 Series
ap1g6a	Cisco Catalyst 9130 Series 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 5: 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
Cisco Catalyst 9124AXE/I/D	100	2000
Cisco Catalyst 9130 Series	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 6: Compatibility Information

Cisco Embedded Wireless Controller on Catalyst Access Points	Cisco ISE	Cisco CMX	Cisco DNA Center
Cupertino 17.7.x	3.0 2.7 2.6 2.4 2.3	10.6.3 10.6.2 10.6 10.5.1	See Cisco DNA 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 7: 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.

Browser	Version	Operating System	Status	Workaround
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 17.7.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-universalk9.17.07.01.zip	C9800-AP-universalk9.17.07.01.zip	ap1g7
Cisco Catalyst 9117 Series	C9800-AP-universalk9.17.07.01.zip	C9800-AP-universalk9.17.07.01.zip	ap1g6
Cisco Catalyst 9120 Series	C9800-AP-universalk9.17.07.01.zip	C9800-AP-universalk9.17.07.01.zip	ap1g7
Cisco Catalyst 9124AXE/I/D	C9800-AP-universalk9.17.07.01.zip	C9800-AP-universalk9.17.07.01.zip	ap1g6a
Cisco Catalyst 9130 Series	C9800-AP-universalk9.17.07.01.zip	C9800-AP-universalk9.17.07.01.zip	ap1g6a

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 DNAC.

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 Series 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 Cupertino 17.7.x

Hardware or Software Parameter	Hardware or Software Type
Access Points	• Cisco Aironet Series Access Points • 1540 • 1560 • 1815i • 1815w • 1830 • 1840 • 1850 • 2800 • 3800 • 4800 • 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 7.
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)
DELL Latitude E5540 (Intel Dual Band Wireless AC7260)	Windows 7 Professional (21.10.1)

Client Type and Name	Driver / Software Version
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
Drager Delta	VG9.0.2
Drager M300.3	VG2.4
Drager M300.4	VG2.4

Client Type and Name	Driver / Software Version
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
Zebra TC52	Android 8.1.0
Zebra TC55	Android 8.1.0
Zebra TC57	Android 8.1.0

Client Type and Name	Driver / Software Version
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

Caveats

Caveats describe unexpected behavior in Cisco IOS releases. Caveats 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 17.7.1

Caveat ID	Description
CSCvz89115	Flexconnect APs are not forwarding DHCP packets after change-of-authorization (CoA) with a change of VLAN using 802.1x encryption.

Caveat ID	Description
CSCvz94692	AP crash is observed due to radio failure (too many radio failures).
CSCwa12278	Cisco Catalyst 9115 AP is crashing due to kernel panic.
CSCwa14307	AP crash is observed due to kernel panic.

Resolved Caveats for Cisco IOS XE 17.7.1

Caveat ID	Description
CSCvv94885	The **show ap cdp neighbours** command displays the name of the switch instead of the domain name.
CSCvy01360	Cisco Catalyst 9115AX AP is reporting false radar detection on channels 100-112.
CSCvx71141	Cisco Catalyst 9800-80 Wireless Controller crashes due to a CPU hog in the radio resource management (RRM) process.
CSCvx81815	Controller does not send server hello packets to AP when enabling Datagram Transport Layer Security (DTLS) encryption.
CSCvy02120	Cisco Catalyst 9130AX AP fails to send reassociation response to roaming clients and deletes the client.
CSCvy11011	Controller displays a traceback similar to: EVENTLIB-3-CPUHOG - ewlc_client_location - remove_weakest_radio_measurement.
CSCvy11981	Controller reloads unexpectedly when AP name is more than 31 characters.
CSCvy25684	Different data rates are observed in CLI and RF profiles.
CSCvy36744	Controller stops forwarding broadcasts intermittently to clients.
CSCvy46043	Controller reloads unexpectedly for switch integrated security features (SISF) heap pointer to l2_socket_counter record.
CSCvy58934	Controller is not sending the CAPWAP restart payload when filter is applied and AP name is changed.
CSCvy72750	Unable to use the **wireless broadcast vlan** command.

Caveat ID	Description
CSCvy74904	AP authorization related RADIUS request does not include the calling station ID and NAS port type.
CSCvy76922	Switch stack with Cisco IOS XE 17.3.2a displays high memory alerts.
CSCvy89423	WNCMGRD process has crashed due to segmentation fault.
CSCvy90646	Controller drops the incoming CAPWAP keepalive for random APs.
CSCvy94284	Controller crashes after running **clear wlan id** command.
CSCvy99116	A crash is observed when a wireless client attempts to connect and the connection times out.
CSCvz14394	Custom-page in web authentication parameter map is not loaded into running configuration after a reload.
CSCvz15015	Cisco Catalyst 9130AX AP loses its WLAN configuration after moving between controllers.
CSCvz17623	Memory leak is observed in emulated database and AP join.
CSCvz28378	Memory leak is observed in WNCD process running 17.3.3 of around 200MB per day.
CSCvy25684	Client location probe displays error when probe request parsing fails.
CSCvz45488	Memory leak is observed in the OPERATIONAL_DB causing dbm crash.
CSCvz45576	Rogue telemetry updates need to be throttled as the controller sends lot of rogue reports to Cisco DNAC.
CSCvz51976	Include AP ethernet speed and duplex information in the output of **show ap config general** command.
CSCvz53408	Fast Transition IE is sent as 0 in M3 after session timeout.
CSCvz63742	Controller does not provide cLApAdminStatus information through SNMP when forensic Advanced Wireless Intrusion Prevention System (aWIPS) is configured.
CSCvz68857	Optimize bsnMobileData OID query to improve performance.

Caveat ID	Description
CSCvz80697	Controller does not remove old NMSP entries when new probes are received in a different slot.
CSCvz84691	Controller crashes due to WNCD process when learning an IP address for a client.
CSCvz89976	Controller running 17.3.4 crashes due to workgroup bridge (WGB).

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 16 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 Online Help
- 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 Connected Mobile Experiences

Cisco Connected Mobile Experiences Documentation

Cisco DNA Center

Cisco DNA Center Documentation

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you’re looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.
- 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.