Release Notes for Cisco Embedded Wireless Controller on Catalyst Access Points, Cisco IOS XE Dublin 17.12.x

First Published: 2023-07-28

Last Modified: 2024-03-22

Release Notes for Cisco Embedded Wireless Controller on Catalyst Access Points, Cisco IOS XE Dublin 17.12.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. 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 Dublin 17.12.3

There are no new features in this release.

What's New in Cisco Embedded Wireless Controller on Catalyst Access Points, Cisco IOS XE Dublin 17.12.2

There are no new features in this release.

This release provides a fix for CSCwh87343: Cisco IOS XE Software Web UI Privilege Escalation Vulnerability. For more information, see Security Advisory: cisco-sa-iosxe-webui-privesc-j22SaA4z.

What's New in Cisco Embedded Wireless Controller on Catalyst Access Points, Cisco IOS XE Dublin 17.12.1

Table 1: New and Modified Software Features

Feature Name	Description and Documentation Link
Archive less than 1 day	The **request platform software trace archive last** command has been enhanced to archive all the trace logs relevant to all the processes running on a system.

Feature Name	Description and Documentation Link
FIPS 140-3 Compliance	This release enables all COS APs to achieve FIPS 140-3 compliance, ensuring adherence to security standards. The Cisco Catalyst 9800 controllers, however, are FIPS 140-2 compliant. **Caution** Downgrading to versions below 17.12.1 can have a negative impact on COS APs in the following scenarios: • When FIPS or WLANCC security modes are enabled. • When the ECDHE-RSA-AES128-GCM-SHA256 cipher suite is not selected for AP DTLS (by default it is selected). **Note** There is no impact on the Cisco IOS AP models. The **show wireless certification config** command has been introduced to verify whether downgrade is impacted or not. For more information, see the chapter FIPS.
Improve Crash Data Collection, Kernel Panics, Out of Memory	A new command is introduced to limit the number of kernel core dumps collected on the AP: • **core-dump kernel limit**

Feature Name	Description and Documentation Link
Intelligent Capture (iCAP) Hardening	This feature aims at making troubleshooting for wireless clients and APs easier. In this release, the following enhancements are made to the iCAP feature: • Anomaly Detection • RF Statistics The following commands are introduced: • **icap subscription client anomaly-detection report-individual enable** • **icap subscription client anomaly-detection report-individual per-client throttle** • **icap subscription client anomaly-detection report-individual per-type throttle** • **ap name icap subscription client anomaly-detection report-individual enable** • **ap name icap subscription client anomaly-detection report-individual per-client throttle** • **ap name icap subscription client anomaly-detection report-individual per-type throttle** For more information, see the chapter Intelligent Capture Hardening.
MacBook Analytics	This feature is supported on the controller when the MacBook device sends 11k action frames along with the model information. For more information, see the chapter Device Analytics.
Mesh Support in Cisco Catalyst 9130AX Series Access Points	From this release, mesh support is included in the Cisco Catalyst 9130AX Series Access Points. All traditional capabilities of mesh are included in the Cisco Catalyst 9130AX Series APs operating in Cisco IOS XE Dublin 17.12.1. For more information, see the chapter Mesh Access Points.

Feature Name	Description and Documentation Link
Modified Trustpoints for Secure Unique Device Identity (SUDI) Certificates	

Feature Name	Description and Documentation Link

	From Cisco IOS XE Dublin 17.12.1 onwards, the following changes have been introduced for trustpoints:
	• Trustpoint names for existing SUDI certificates
	If your device supports Cisco Manufacturing CA III certificate and is not disabled, the trustpoint names are as follows:
	• For *Cisco Manufacturing CA III* certificate, the trustpoint name has changed from CISCO_IDEVID_SUDI to CISCO_IDEVID_CMCA3_SUDI
	• For *Cisco Manufacturing CA SHA2* certificate, the trustpoint name has changed from CISCO_IDEVID_SUDI_LEGACY to CISCO_IDEVID_CMCA2_SUDI
	If your device does not support Cisco Manufacturing CA III certificate or if the certificate is disabled using **no platform sudi cmca3** command, the trustpoint names are as follows:
	• For *Cisco Manufacturing CA SHA2* certificate, the trustpoint name has changed from CISCO_IDEVID_SUDI to CISCO_IDEVID_CMCA2_SUDI
	• For *Cisco Manufacturing CA* certificate, the trustpoint name has changed from CISCO_IDEVID_SUDI_LEGACY to CISCO_IDEVID_CMCA_SUDI
	• **show wireless management trustpoint** command output
	If Cisco Catalyst 9300 Series Switch is used with a Cisco Catalyst 9800 Series Wireless Controller for wireless deployments, the trustpoint name in the output of **show wireless management trustpoint** command is updated to the modified trustpoint name as mentioned previously.
	The following example shows a sample output of **show wireless management trustpoint** command. Note that if your device does not support Cisco Manufacturing CA III certificate or if the certificate is disabled, the Trustpoint Name in the following output displays CISCO_IDEVID_CMCA2_SUDI.
	`Device# show wireless management trustpoint`
	`Trustpoint Name : CISCO_IDEVID_CMCA3_SUDI`
	`Certificate Info : Available`
	`Certificate Type : MIC`
	`Certificate Hash : <SHA1 - hash>`
	`Private key Info : Available`
	`FIPS suitability : Not Applicable`
	• **show ip http server status** command output

Feature Name	Description and Documentation Link

	If you configure the trustpoint for the HTTP server as CISCO_IDEVID_SUDI, the output of **show ip http server status** command displays the operating trustpoint along with the configured trustpoint.
	The following example shows a sample output of **show ip http server status** command with both the configured and the operating trustpoint names. Note that if your device does not support Cisco Manufacturing CA III certificate or if the certificate is disabled, the operating trustpoint in the following output displays CISCO_IDEVID_CMCA2_SUDI.
	`Device# show ip http server status`
	`…`
	`HTTP secure server trustpoint: CISCO_IDEVID_SUDI`
	`HTTP secure server operating trustpoint: CISCO_IDEVID_CMCA3_SUDI`

Rogue Channel Width	From this release, you can specify the channel width and the band for rogue detection. The following command is introduced: • **condition chan-width** For more information, see the chapter Radio Resource Management.
Rogue PMF	From this release, the controller will contain rogue APs with 802.11w Protected Management Frame (PMF) on centrally switched WLANs. The following commands are introduced: • **rogue detection containment pmf-denial** • **pmf-deauth** For more information, see the chapter Radio Resource Management.
Software Entropy Enhancement for FIPS 140-3	From Cisco IOS XE Dublin 17.12.1 onwards, Federal Information Processing Standard (FIPS) 140-3 is supported as a security standard to validate cryptographic modules.

Table 2: New and Modified GUI Features

Feature Name	GUI Path
Rogue Channel Width	• **Configuration > Security >Wireless Protection Policies > Rogue AP Rules**

Behavior Change

From Cisco IOS XE Dublin 17.12.1 onwards, EWC supports a reduced scale of APs and clients for the following APs:

EWC AP	Current Scale (Maximum APs Supported / Maximum Clients Supported)	New Scale (Maximum APs Supported / Maximum Clients Supported)
Cisco Catalyst 9120AX Series Access Points	100 APs/2000 clients	50 APs/1000 clients
Cisco Catalyst 9124AX Series Access Points	100 APs/2000 clients	50 APs/1000 clients
Cisco Catalyst 9130AX Series Access Points	100 APs/2000 clients	50 APs/1000 clients

Note Starting 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, has been reduced to 50 APs from 100 APs and 1000 clients from 2000 clients.

Interactive Help

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

You can start the interactive help in the following ways:

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

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

The following features have an associated interactive help:

- Configuring AAA
- Configuring FlexConnect Authentication
- Configuring 802.1x Authentication
- Configuring Local Web Authentication

- Configuring OpenRoaming
- Configuring Mesh APs

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

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

Supported 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 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 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
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 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	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.

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
Dublin 17.12.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.
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

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 Dublin 17.12.x

Table 8: Upgrade Path to Cisco IOS XE Dublin 17.12.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 17.12.x.
16.11.x	—	Upgrade first to 16.12.5 or 17.3.x and then to 17.12.x.
16.12.x	Upgrade first to 17.3.5 or 17.6.x or later and then to 17.12.x.	Upgrade first to 17.3.5 or 17.6.x or later and then to 17.12.x.
17.1.x	Upgrade first to 17.3.5 or 17.6.x or later and then to 17.12.x.	Upgrade first to 17.3.5 or 17.6.x or later and then to 17.2.x.
17.2.x	Upgrade first to 17.3.5 or 17.6.x or later and then to 17.12.x.	Upgrade first to 17.3.5 or 17.6.x or later and then to 17.12.x.
17.3.1 to 17.3.4	Upgrade first to 17.3.5 or 17.6.x or later and then to 17.12.x.	Upgrade first to 17.3.5 or 17.6.x or later and then to 17.12.x.
17.3.4c or later	Upgrade directly to 17.12.x.	Upgrade directly to 17.12.x.
17.4.x	Upgrade first to 17.6.x and then to 17.12.x.	Upgrade first to 17.6.x and then to 17.12.x.

Current Software	Upgrade Path for Deployments with 9130 or 9124	Upgrade Path for Deployments Without 9130 or 9124
17.5.x	Upgrade first to 17.6.x and then to 17.12.x.	Upgrade first to 17.6.x and then to 17.12.x.
17.6.x	Upgrade directly to 17.12.x.	Upgrade directly to 17.12.x.
17.7.x	Upgrade directly to 17.12.x.	Upgrade directly to 17.12.x.
17.8.x	Upgrade directly to 17.12.x.	Upgrade directly to 17.12.x.
17.9.x	Upgrade directly to 17.12.x.	Upgrade directly to 17.12.x.
17.10.x	Upgrade directly to 17.12.x.	Upgrade directly to 17.12.x.
17.11.x	Upgrade directly to 17.12.x.	Upgrade directly to 17.12.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 17.12.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 9: 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-universalk9.17.12.03.zip C9800-AP-universalk9.17.12.02.zip C9800-AP-universalk9.17.12.01.zip	C9800-AP-universalk9.17.12.03.zip C9800-AP-universalk9.17.12.02.zip C9800-AP-universalk9.17.12.01.zip	ap1g7
Cisco Catalyst 9117 Series	C9800-AP-universalk9.17.12.03.zip C9800-AP-universalk9.17.12.02.zip C9800-AP-universalk9.17.12.01.zip	C9800-AP-universalk9.17.12.03.zip C9800-AP-universalk9.17.12.02.zip C9800-AP-universalk9.17.12.01.zip	ap1g6
Cisco Catalyst 9120 Series	C9800-AP-universalk9.17.12.03.zip C9800-AP-universalk9.17.12.02.zip C9800-AP-universalk9.17.12.01.zip	C9800-AP-universalk9.17.12.03.zip C9800-AP-universalk9.17.12.02.zip C9800-AP-universalk9.17.12.01.zip	ap1g7
Cisco Catalyst 9124AXE/I/D	C9800-AP-universalk9.17.12.03.zip C9800-AP-universalk9.17.12.02.zip C9800-AP-universalk9.17.12.01.zip	C9800-AP-universalk9.17.12.03.zip C9800-AP-universalk9.17.12.02.zip C9800-AP-universalk9.17.12.01.zip	ap1g6a
Cisco Catalyst 9130	C9800-AP-universalk9.17.12.03.zip C9800-AP-universalk9.17.12.02.zip C9800-AP-universalk9.17.12.01.zip	C9800-AP-universalk9.17.12.03.zip C9800-AP-universalk9.17.12.02.zip C9800-AP-universalk9.17.12.01.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 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 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 10: Test Configuration for Interoperability

Hardware or Software Parameter	Hardware or Software Type
Release	Cisco IOS XE Dublin 17.12.x

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

Hardware or Software Parameter	Hardware or Software Type
Radio	• 802.11ax • 802.11ac • 802.11a • 802.11g • 802.11n (2.4 GHz or 5 GHz)
Security	Open, PSK (WPA2-AES), 802.1X (WPA2-AES) (EAP-FAST, EAP-TLS), WPA3.
Cisco ISE	See Compatibility Matrix, on page 12.
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.

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 17.12.3

Identifier	Headline
CSCwj03495	Cisco Aironet 1562 mesh AP cannot join Cisco Catalyst 9124 root AP due to a missing mesh adjacency message.
CSCwj05365	Cisco Catalyst 9115 AP experiences kernel panic crash.
CSCwi99437	Clients are unable to connect to Cisco Aironet 1850 AP FlexConnect Simultaneous Authentication of Equals (SAE) SSID.

Identifier	Headline
CSCwi99296	Cisco Catalyst 9120 AP experiences kernel panic crash.
CSCwi96508	Cisco Wave 2 APs allow Sticky Key Caching (SKC) roam causing client deletion with INVALID_PMKID as the reason.
CSCwi96176	Cisco Catalyst 9130 APs and Cisco Catalyst 9166 APs show High Channel Utilization with one single client connected.
CSCwi95945	No plumbing takes place from Group Temporal Key (GTK) to the driver when GTK rekeys.
CSCwi69696	Cisco Aironet 1815 Series APs experiences random drops in traffic going towards wireless clients.
CSCwi92439	Cisco Catalyst 1815 APs are reporting high channel utilization in the 5-GHz band.
CSCwi40659	Clients in the same remote LAN (RLAN) with different OfficeExtend Access Point (OEAP) cannot communicate between each other.
CSCwi16509	APs disjoin with the "Invalid radio slot id" error and do not rejoin the controller.
CSCwh52553	High mDNS traffic causes Cisco Catalyst 9105 AP to have high utilization and performance issues.

Open Caveats for Cisco IOS XE 17.12.2

Identifier	Headline
CSCwf29762	The controller running the mDNS feature crashes due to a NULL check missing in the code.
CSCwf93063	Intel AX210 client connection fails after a few minutes of traffic with Cisco Aironet 1815 Series APs.
CSCwh18613	The encrypted mesh pre-shared key changes each time **password encryption aes** command is run.
CSCwh20239	The wcpd process restarts on the Cisco Catalyst 9105 AP generating core but with no AP reload.
CSCwh56836	The Cisco Embedded Wireless Controller (EWC) AP crashes and causes constant active failover.
CSCwh58099	After client deletion and COA termination, the controller allows the deleted client to reconnect.
CSCwh59543	Radio FW 1 and CAPWAP crashed during scale longevity test.
CSCwh63050	Controller sends Internet Group Management Protocol (IGMP) queries with non-controller IP address and controller MAC address.

Identifier	Headline
CSCwh67349	Cisco Aironet 3802 Series AP crashes continuously during the capwapd and cleanaird processes.
CSCwh68219	Cisco Catalyst 9100 Series APs are not processing the EAP-TLS server.
CSCwh80060	Cisco Wave 2 APs connected to the controller lose Flex WLAN - VLAN mapping intermittently.
CSCwh92459	Controller crashes due to wncd process fault.
CSCwh88100	Cisco Aironet 3800 Series APs experience kernel panic crash.
CSCwe93421	Cisco Catalyst 9115 APs intermittently stop transmitting multicast traffic downstream.
CSCwh29442	Cisco Catalyst 9800-40 Wireless Controller crashes after ISSU upgrade.
CSCwh46368	Cisco Catalyst 9800-40 Wireless Controller device tracking binds BSSID MAC to wired IP address causing reachability issues.
CSCwh49467	Cisco Catalyst 9130AXI AP leaks multicast traffic to the wrong BSSID.
CSCwh49810	Audit session ID changes after inter-WNCD roaming.
CSCwh62342	AP FlexConnect as an mDNS gateway does not respond correctly when Location Specific Services (LSS) filter is enabled in the 5-GHz band.
CSCwh67342	Cisco Catalyst 9130 APs are not able to join when Controller Based Application Recognition (CBAR) is enabled on the controller.
CSCwh74415	Per client rate limit with FlexConnect local switching APs do not work.
CSCwh75431	Cisco Aironet 1800 Series APs report false channel utilization affecting performance across the 5-GHz band.
CSCwh82580	Cisco Catalyst 9120 Series APs crash when Prime Infrastructure shuts down one of the SSIDs through the Schedule SSID Availability feature.
CSCwh89539	CAPWAP messages are queued for longer than 'x' seconds with client throttling being switched on.
CSCwh49406	Excessive CleanAir syslogs are generated from Cisco Catalyst 9130 Series APs.
CSCwh67285	The controller is unable to get telemetry data due to the unexpected reload and failure of the pubd process.
CSCwh68360	Cisco Catalyst 9120 AP crashes due to kernel panic.
CSCwh63270	Cisco Catalyst 9130AXI APs crash due to radio failure.
CSCwh87903	Cisco Catalyst 9120 APs sending auth_resp failures for specific client MAC addresses.
CSCwh81332	Cisco Catalyst 9130 Series APs experience kernel panic crash.

Open Caveats for Cisco IOS XE 17.12.1

For the list of open caveats, click here.

Resolved Caveats for Cisco IOS XE 17.12.3

Identifier	Headline
CSCvy50798	Cisco Catalyst 9124 Series APs are not displayed in the controller GUI after it is registered.
CSCwh58054	Cisco Embedded Wireless Controller-AP: Users will experience authentication failures when using CCO mode for software upgrades, after April 30, 2024.
CSCwj10697	EWC on Cisco Catalyst 9124 AP image upgrade fails.

Resolved Caveats for Cisco IOS XE 17.12.2

Identifier	Headline
CSCwh87343	Cisco IOS XE Software Web UI Privilege Escalation Vulnerability. For more information, see Security Advisory: cisco-sa-iosxe-webui-privesc-j22SaA4z.
CSCwf60151	The controller experiences a memory leak at the kernel level with the pubd process.
CSCwe11213	Cisco Catalyst 9130 AP crashes due to radio recovery failure.
CSCwf79458	11AX WGB 2.4-GHz radio does not roam when 11r is enabled.
CSCwh20306	Cisco Wave 2 APs: Hyperlocation is broken if aWIPS is enabled.
CSCwf83278	Client traffic fails with N+1 when AP sends CLIENT_DEL_STOP_REASSOC.
CSCwh08532	The DSCP marking on Cisco Wave 2 APs for QoS metal policies is not happening in the slow and fast path.
CSCwh20301	There is no telemetry data sent from the controller to Cisco DNA Center.
CSCwf53520	Kernel panic crash observed on Cisco Aironet 1815 Series AP.
CSCwh42002	Controller crashes with wncd core while processing CAPWAP data.
CSCwh61011	Cisco Catalyst 9120 APs and Cisco Catalyst 9115 APs unexpectedly disjoin from the controller and are not able to establish DTLS connection again.
CSCwf59348	Cisco Catalyst 9105 AP, Cisco Catalyst 9115 AP, and Cisco Catalyst 9120 AP beacons set the maximum transmit power level to 128 dBm in Ireland (Country IE).
CSCwf63818	Kernal panic crash observed on Cisco Aironet 1832 AP.
CSCwf93992	Cisco Aironet 2800 Flex APs do not process EAP-TLS fragmented packets if the delay is more than 50ms.

Identifier	Headline
CSCwf99932	Cisco Catalyst 9120 AP experiences a radio crash.
CSCwh09879	Clients are unable to connect to the Cisco Wave 2 AP FlexConnect after a country code change.
CSCwh20934	Cisco Wave 2 APs reload due to systemd critical process crash.
CSCwh54279	Kernel panic crash observed in Cisco Aironet 1815 OEAP.
CSCwh74663	Cisco Aironet 3800 AP does not send QoS data frames downstream as the RadarDetected flag is set to TRUE.
CSCwh81040	Cisco Catalyst 9120 AP with local mode crashes when Workgroup Bridge (WGB) associates with the SSID profile.
CSCwh54762	Cisco Catalyst 9120 AP crashes due to kernel panic.
CSCwf53331	Kernel panic crash observed in Cisco Catalyst 9124 AP in Bridge mode, after changing channels on the 5-GHz radio.
CSCwh06834	Using special characters in the password while generating trustpoint generates an invalid trustpoint.
CSCwh08625	Kernel panic crash observed in Cisco Catalyst 9120 AP.
CSCwh18759	Cisco Aironet 1815 AP crashed due to low system memory and kernel panic.
CSCwf13804	APs are randomly failing for new client associations. 'No buffer space available' error is reported.
CSCwf52815	Cisco Wave 2 APs to improve PMTU Discovery mechanism to honor the ICMP unreachable MTU value.
CSCwf62051	Cisco Aironet 1815W APs crash due to kernel panic.
CSCwf90014	Issues observed with Cisco Intelligent Capture on IPv6 cluster.
CSCwf44321	Controller does not report Interferers over the NMSP channel to the Cisco Spaces connector.
CSCwf86242	The controller unexpectedly reloads when the CAPWAP window size is set to 0.
CSCwh61007	Controller crashes whenever it provisions multiple APs.
CSCwf29742	Cisco Catalyst 9120 AP: Firmware crashed while running multicast and longevity test.
CSCwh33190	Cisco Catalyst 9115 AP (Local Mode) crashed due to kernel panic.
CSCwf07384	The wired client behind Cisco Catalyst 9105 AP RLAN is not able to pass traffic.
CSCwf68131	Bad blocks monitoring and repair in Cisco Catalyst 9105AXW Series APs.
CSCwf95868	WGB radio 0 TX power decreases by 20dBm while configuring the antenna number in a single band mode.

Identifier	Headline
CSCwf83292	Cisco Catalyst 9130 APs do not send DHCP Offer and ACK OTA to the client.
CSCwf90114	Stale AP entries remain after AP flap during SSO with scale SVI/VRF configuration.
CSCwh76420	Controller crashes while performing ISSU upgrade.
CSCwf81866	Radio 0 WGB configuration is not backed up correctly when doing a TFTP backup of the configuration.
CSCwf65794	Cisco Aironet 1852 AP reloads unexpectedly due to radio failure.
CSCwf78066	Cisco DNA Center displays the "No radios in the selected band" message on the floor maps.
CSCwh29924	Cisco Catalyst 9105/9115/9120 AP WGB: Antenna-A does not function properly if the configuration is an AB-antenna.
CSCwf12301	The wcpd TX retries count is not MSDU based.
CSCwf10839	A large volume of VRRP traffic sent from EWC and the switch port go down due to the storm-control action that is configured.
CSCwe24263	Inconsistent TX power levels advertised in beacons in Cisco Catalyst 9130 APs.
CSCwh30996	The Bluetooth Low Energy (BLE) PDU type in the TX packet for iBeacon in dual mode needs to be changed.
CSCwf91445	Controller pushes the accounting information for PSK Local Auth WLANs.
CSCwf94863	Cisco Catalyst 9115 AP unexpectedly reboots due to kernel panic.
CSCwf64009	Cisco Aironet 1815 AP experiences frequent drops in RLAN-VLAN traffic with looped ports.
CSCwf98534	Global Navigation Satellite System (GNSS) antenna cable length is not taken into account in uncertainty computation.
CSCwh09676	The Wireless Control Protocol (WCP) dmalloc unfree logs are missing and dmalloc files not updated periodically.
CSCwh27366	Cisco Aironet 3800 AP experiences radio firmware crash.
CSCwh27425	Cisco Catalyst 9115AX AP does not forward a part of the CAPWAP data packets to the uplink direction.
CSCwf13107	Radio crash is observed during longevity test in Cisco Catalyst 9105 AP.
CSCwh35072	Cisco Aironet 3800 AP reloads unexpectedly due to FIQ/NMI reset.
CSCwh45418	Cisco Catalyst 9124 AP sends incorrect duplex information through Cisco Discovery Protocol (CDP).
CSCwh50681	New SSID is being broadcasted after the 17.9.3 wireless upgrade.
CSCwf68612	Controller reloads unexpectedly due to segmentation fault in the wncd process.

Identifier	Headline
CSCwf99906	Network Time Protocol (NTP) authentication is removed after reloading.
CSCwh11858	The device unexpectedly reloads when removing an FQDN ACL from the switch.
CSCwf21390	Duplicate Access-Request messages with the CTS client username occurs when more than one RADIUS server is configured.
CSCwf36752	TACACS encryption fails if FQDN is used as the T+ address when it is configured for first time.
CSCwf66661	The controller GUI renders the page slowly while accessing the device type content, leading to WebSocket termination.

Resolved Caveats for Cisco IOS XE 17.12.1

For the list of resolved caveats, click here.

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 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.