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: 2026-08-05

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 (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 Dublin 17.12.8

There are no new features in this release.

What's New in Cisco Embedded Wireless Controller on Catalyst Access Points, Cisco IOS XE Dublin 17.12.7a

There are no new features in this release.

What's New in Cisco Embedded Wireless Controller on Catalyst Access Points, Cisco IOS XE Dublin 17.12.6a

There are no new features in this release.

What's New in Cisco Embedded Wireless Controller on Catalyst Access Points, Cisco IOS XE Dublin 17.12.5

There are no new features in this release.

What's New in Cisco Embedded Wireless Controller on Catalyst Access Points, Cisco IOS XE Dublin 17.12.4

There are no new features in this release.

What's New in Cisco Embedded Wireless Controller on Catalyst Access Points, Cisco IOS XE Dublin 17.12.3

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.
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.

Feature Name	Description and Documentation Link
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**
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.

Behavior Change for Cisco IOS XE 17.12.6a

- Controller displayed out-of-order packet issue with fragmented packets when Auto QoS was enabled. When a client tries to connect to an EAP-TLS-based SSID, during the certificate exchange, the client sends its device certificate. If the certificate is fragmented because it exceeds the MTU (1500), the fragments are observed to be sent out-of-order from the controller when Auto QoS is enabled.

  With the change in behavior, the fragments are classified and applied with default action. For workarounds, refer to CSCwo97886.

- The **ip proxy-arp** configuration is disabled by default under VLAN interfaces for the controller.
- For Cisco Aironet 1815T Series AP, from Cisco IOS XE 17.12.x, `.../storage/config.oeap` was created beforehand as long as the AP is in OEAP mode.

  With the change in behavior, once the AP boots in FlexConnect OEAP mode, it switches on the default OEAP DHCP server (dhcp0) as day 1 configuration.

- The maximum supported RFIDs per WNCD for any platform has been increased to greater than 9601 RFIDs. The new value of the maximum RFID is platform dependent.
- Authentication for AP with EAP fails if the password is more than 31 characters. With the change in behavior, password with more than 31 characters works successfully.
- When you apply an AP tag configuration, ensure that the number of APs associated with a non-default site tag does not exceed the platform limit. The system allows these configurations, but APs exceeding the limit cannot join the network.

The configuration validator now checks for this condition and when more APs than the platform limit are associated with the same site tag, the configuration is not rejected.

- Cisco Catalyst 9105 AP bridges the RLAN traffic to a wrong VLAN.

  To prevent this issue:

  - Delete any unused VLAN from the FlexConnect profile.
  - Run the **capwap ap erase all** command to clear the AP cache.

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

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

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 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 Catalyst Center
Dublin 17.12.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 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.

Browser	Version	Operating System	Status	Workaround
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

Before You Upgrade

- To ensure a smooth upgrade and prevent potential boot loop issues with APs, review the following Field Notice and technical documentation. It is critical to complete these actions prior to initiating your upgrade.
  - FN74383: Field Notice
  - Validate and Recover Catalyst APs on 17.12
- (#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 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.

Current Software	Upgrade Path for Deployments with 9130 or 9124	Upgrade Path for Deployments Without 9130 or 9124
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.
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 AP.

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-universalk9.17.12.08.zip C9800-AP-universalk9.17.12.7a.zip C9800-AP-universalk9.17.12.6a.zip C9800-AP-universalk9.17.12.05.zip C9800-AP-universalk9.17.12.04.zip C9800-AP-universalk9.17.12.03.zip C9800-AP-universalk9.17.12.02.zip C9800-AP-universalk9.17.12.01.zip	C9800-AP-universalk9.17.12.08.zip C9800-AP-universalk9.17.12.7a.zip C9800-AP-universalk9.17.12.6a.zip C9800-AP-universalk9.17.12.05.zip C9800-AP-universalk9.17.12.04.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-universalk9.17.12.08.zip C9800-AP-universalk9.17.12.7a.zip C9800-AP-universalk9.17.12.6a.zip C9800-AP-universalk9.17.12.05.zip C9800-AP-universalk9.17.12.04.zip C9800-AP-universalk9.17.12.03.zip C9800-AP-universalk9.17.12.02.zip C9800-AP-universalk9.17.12.01.zip	C9800-AP-universalk9.17.12.08.zip C9800-AP-universalk9.17.12.7a.zip C9800-AP-universalk9.17.12.6a.zip C9800-AP-universalk9.17.12.05.zip C9800-AP-universalk9.17.12.04.zip C9800-AP-universalk9.17.12.03.zip C9800-AP-universalk9.17.12.02.zip C9800-AP-universalk9.17.12.01.zip	ap1g6

Primary AP	AP Software for Conversion from CAPWAP to Cisco EWC	AP Software Image Bundle for Upgrade	AP Software in the Bundle
Cisco Catalyst 9120 Series	C9800-AP-universalk9.17.12.08.zip C9800-AP-universalk9.17.12.7a.zip C9800-AP-universalk9.17.12.6a.zip C9800-AP-universalk9.17.12.05.zip C9800-AP-universalk9.17.12.04.zip C9800-AP-universalk9.17.12.03.zip C9800-AP-universalk9.17.12.02.zip C9800-AP-universalk9.17.12.01.zip	C9800-AP-universalk9.17.12.08.zip C9800-AP-universalk9.17.12.7a.zip C9800-AP-universalk9.17.12.6a.zip C9800-AP-universalk9.17.12.05.zip C9800-AP-universalk9.17.12.04.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-universalk9.17.12.08.zip C9800-AP-universalk9.17.12.7a.zip C9800-AP-universalk9.17.12.6a.zip C9800-AP-universalk9.17.12.05.zip C9800-AP-universalk9.17.12.04.zip C9800-AP-universalk9.17.12.03.zip C9800-AP-universalk9.17.12.02.zip C9800-AP-universalk9.17.12.01.zip	C9800-AP-universalk9.17.12.08.zip C9800-AP-universalk9.17.12.7a.zip C9800-AP-universalk9.17.12.6a.zip C9800-AP-universalk9.17.12.05.zip C9800-AP-universalk9.17.12.04.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-universalk9.17.12.08.zip C9800-AP-universalk9.17.12.7a.zip C9800-AP-universalk9.17.12.6a.zip C9800-AP-universalk9.17.12.05.zip C9800-AP-universalk9.17.12.04.zip C9800-AP-universalk9.17.12.03.zip C9800-AP-universalk9.17.12.02.zip C9800-AP-universalk9.17.12.01.zip	C9800-AP-universalk9.17.12.08.zip C9800-AP-universalk9.17.12.7a.zip C9800-AP-universalk9.17.12.6a.zip C9800-AP-universalk9.17.12.05.zip C9800-AP-universalk9.17.12.04.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 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 10: Test Configuration for Interoperability

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

Table 11: 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

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

Client Type and Name	Driver / Software Version
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 17.12.8

There are no open issues for Cisco IOS XE 17.12.8.

Open Issues for Cisco IOS XE 17.12.7a

There are no open issues for Cisco IOS XE 17.12.7a.

Open Issues for Cisco IOS XE 17.12.6a

Identifier	Headline
CSCwo89933	Controller zombie process \"date\" is not killed and exhausts available process ID, which leads to failures of other processes

Open Issues for Cisco IOS XE 17.12.5

Identifier	Headline
CSCwn18885	Cisco Catalyst 9136 APs encounter kernel unresponsiveness silently with the last reload reason 'unknown' [SF 07624324]
CSCwn27877	Cisco Catalyst 9105 AP does not respond to clients on 5GHz CS00012380774
CSCwn36778	Cisco Catalyst 9800-80 controller displays low memory leak potentially in the 'ipv4_addr' field
CSCwn66225	iPhone clients get disconnected following Tx power invalid on beacon frame
CSCwn81268	IOX-APP using USB in RUN state ends up in activated state after switch reload
CSCwn89252	Cisco Catalyst 9120 AP running 17.15.2 does not install Solum IOX APP
CSCwj53257	Catalyst APs report 3600 seconds NOP timer on the last radar detected channel from DCA list
CSCwn31021	Controller fails to represent the correct format of AP Name and VLAN ID in option 82
CSCwn33501	Controller does not relay any output for all the APs connected for the #show ap summary sort name command
CSCwn40321	Cisco Catalyst 9120 AP intermittently handles dynamic BW from iOS devices with 11ax enabled
CSCwn54374	Cisco Catalyst 9136 AP encounters kernel unresponsiveness
CSCwn55534	IP theft is observed on the controller when the client receives a second DHCP offer following DORA

Open Issues for Cisco IOS XE 17.12.4

Identifier	Headline
CSCwh63050	Controller sends IGMP queries without IP address and MAC address on Cisco IOS XE Cupertino 17.9.3

Identifier	Headline
CSCwi42059	AP unable to join controller due to stale entries in Cisco IOS XE Cupertino 17.9.4
CSCwj30587	CAPWAP messaging causes memory leak in WNCd
CSCwj39057	Cisco Catalyst 9130 AP observes traffic loss and delay due to channel utilization and interference
CSCwj42305	Client is unable to connect due to delete reason NACK_IFID_EXISTS
CSCwj80614	Clients are unable to connect due to assignment of IP address that is in use by stale client entry in device-tracking database in FlexConnect local switching
CSCwj89538	Cisco Aironet 2802 Series AP unable to send reassociation and association requests
CSCwj93876	Controller reloads with reason "Critical process wncmgrd fault on rp_0_0 (rc=134)\"
CSCwk05809	CPUHOG traceback messages observed in Cisco IOS XE Dublin 17.12.2
CSCwk07132	FlexConnect local switching client rate-limit pushed by AAA is applied per stream and not per client in Cisco IOS XE Dublin 17.12.3
CSCwk15357	Controller does not send EXR_OP_UPDATE event, which causes false alarms on Cisco Prime Infrastructure
CSCwk17102	Missing M1 packet causes unexpected client disconnect and inability to reconnect with the controller
CSCwk17667	Controller unexpectedly reboots due to high ODM memory consumption
CSCwk21570	Clients on FlexConnect are unable to pass traffic if rate-limiting AVP is missing
CSCwk32111	Controller generates -1 days messages even when registered using Air Gapped licensing

Open Issues 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.
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.

Identifier	Headline
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 Issues 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.
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.

Identifier	Headline
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 Issues for Cisco IOS XE 17.12.1

For the list of open issues, click here.

Resolved Issues for Cisco IOS XE 17.12.8

There are no resolved issues for Cisco IOS XE 17.12.8.

Resolved Issues for Cisco IOS XE 17.12.7a

Identifier	Headline
CSCwr28871	Delete EWC image when upgrading CAPWAP AP to 17.18.x or later

Resolved Issues for Cisco IOS XE 17.12.6a

Identifier	Headline
CSCwr09565	The controller does not send mDNS queries or responses after upgrade to 17.12.6 or 17.15.4
CSCwq70914	Controller encounters linux_iosd crash in the IGMP snooping process
CSCwj80614	Clients are unable to connect due to assignment of IP address that is in use by stale client entry in device-tracking database in FlexConnect local switching
CSCwk82116	Sonic: Unable to add/delete VLAN under VLAN page
CSCwm57815	RF group name is empty after assigning AI RF profile to sites
CSCwm67254	Accounting start and stop messages are missing CUI attributes
CSCwm73020	Controller relays unicast DHCP requests
CSCwn36778	Cisco Catalyst 9800-80 controller displays low memory leak potentially in the 'ipv4_addr' field
CSCwn83626	Client is stuck in association while changing WLAN from central switching profile to local profile
CSCwn90360	Controller is unable to start EAP process due to the delay of packet transmission from AP
CSCwn90874	Guest anchor controller shows error message when creating anchor-export-ACK
CSCwn92477	Controller unexpectedly reboots during WNCd process due to assertion failure with invalid BSSID
CSCwn92827	Secondary controller fails with rsync error
CSCwn98574	observing vrf name corrupt, causing client stuck at mobility while roamining and frequent disconncts
CSCwo02178	FT-SAE clients fails to roam between controller in same mobility group due to PMKID mismatch
CSCwo37680	Controller initiates client deletion with code: CO_CLIENT_DELETE_REASON_DOT11_MAX_STA
CSCwo60822	SJC Alpha eWLC always prints AP Image Predownload Successful even when it fails on some APs

Identifier	Headline
CSCwo61286	Audit session ID changes after inter-WNCd roam on Central Web Authentication (CWA) with PSK
CSCwo62157	Controller with CAPWAP enabled display memory leak in tdl_mac_addr object
CSCwo70030	Rogue processing is performed by WNCd even though the \"bssid-neighbor-stats\" configuration is disabled
CSCwo97161	Unable to push a large RPC config via Netconf over SSH
CSCwo97886	Controller display out of order packet issue with fragmented packet when AutoQOS is enabled
CSCwp07189	9800 WLC sending capwap control payload with DHCP_GW_NM payload to local mode APs
CSCwp13687	Cisco Catalyst 9800-CL controller modifies the script generating SSC to avoid issues with RSA key generation impacting AP join
CSCwp20530	Controller does not forward downstream packets to the wireless client after switchover
CSCwp26707	Controller fails to start L2 authentication for 11r clients with vlan-persitent configured in 17.12.5
CSCwp32113	Controller reloads due to kernel unresponsiveness with segmentation fault (11) in process IGMPSN
CSCwp65184	WLC crash after predownload initiated
CSCwp86129	Client connected to local mac-auth PSK or MPSK SSIDs get disconnected and do not remain connected to the controller
CSCwq30202	Frequent channel changes seen on 6GHz
CSCwf36148	Optimising the SISF code wrt to calling CO API to fetch the wireless client config info
CSCwh99327	APSP custom site filter config doesn't reflect in UI
CSCwi66855	Catalyst 9000 - Allow file uploads for files > 1GB
CSCwm09484	WNCD Crash in CiscoSSL Code
CSCwn31021	Controller fails to represent the correct format of AP Name and VLAN ID in option 82
CSCwn33501	Controller connected to the AP does not give any output while executing the #show ap summary sort name command
CSCwn45670	Controller GUI FlexConnect configuration page fails after upgrade to Cisco IOS XE 17.15.1

Identifier	Headline
CSCwn94159	Controller with 6 GHz support AP's radio channel bandwidth changes due to DCA happening frequently
CSCwo19011	Controller observes unexpected SISF reboot with WNCD core
CSCwo20395	Controller's rogue classification rules do not apply configured classifications
CSCwo21938	AFC is using manual geolocation co-ordinates
CSCwo29017	wncmgrd kernel unresponsiveness after issue command \u2018show ap config slots\u2019
CSCwo30925	Cisco Wi-Fi 6 and above APs do not support disabling WMM on radios that support 802.11n/11ac/11ax operation
CSCwo33572	Failed to collect RA tracing logs on Cisco IOS XE Release 17.9.5
CSCwo41248	Controller display wrong message when configuring 2 radios on the same UNII band (100 - 144)
CSCwo52310	Wireless cloud service consumes 100% CPU due to geolocation derivation
CSCwo64967	Mobility tunnel with data-link encryption intermittently disconnects when the fourth octet of the WMI address is 255
CSCwo66748	'cLApAssociatedClientCount' Object isn't working with 17.12.X
CSCwo67294	Controller unexpectedly reloads due to a corrupted value in IGMP Layer 2 Snooping process
CSCwo67413	Controller pushes aWIPS profiles from FQDN-only setup for intrusion detection
CSCwo73753	C9800 not enforcing SGT policies for static/sxp tags on the same L2 network
CSCwo89539	Controller reload unexpectedly when adding \"location civic-location-id\" to multiple interfaces
CSCwo98644	RRM does not update the default channel when using IPv6 only on the controller
CSCwp03988	Controller reloads unexpectedly due to unsuccessful copy of the MAC address
CSCwp06711	Controller overwrites the static AP location based on the Location Tag settings
CSCwp12959	Wireless clients may be excluded after one authentication failure or not excluded as expected
CSCwp16968	Client disconnection issue during fast roaming on WGB 1562 due to MAC address record mismatch
CSCwp20167	Access points- >Country code for \" Philippines \" misspelled as Philipines
CSCwp25552	BSSID-mac dispatched as 00:00:00:00:00:00 for slot 1 WLAN 1
CSCwp25836	Request for rpc support for dual band radio use-cases

Identifier	Headline
CSCwp59171	Users unable to add allowed user on Lobby admin page
CSCwp93598	Memory leak found in the controller process related to handling a specific database string
CSCwq19937	[17.18.1-SST] 9800 Webui Filter Does Not Contain filters does not work
CSCwj32611	AP kernel panic: \"vmap allocation for size 2093056 failed: use vmalloc=< size > to increase size.\"
CSCwk09142	9136 AP radio crash on process Fatal error received from wcss software
CSCwn66225	Non-ROW AP transmits invalid TX power IE in beacons, breaking client connectivity
CSCwn81268	Due to switch reload when AP boots up, IOX-APP is starting before USB is detected
CSCwn88092	Unable to view the events for wireless clients in the Client 360 section of the Event Viewer
CSCwn89252	AP running 17.15.2 not possible to install Solum IOX APP
CSCwn92652	Radio ucode crashes seen in 9105 APs in monitor mode
CSCwo04380	Beacons stuck on Radio 1 on 9162 APs after upgrade to 17.12.4.158
CSCwo58100	9130, and 916x APs on 17.12.x drop the EAP response coming from the AAA server
CSCwo61838	Cisco Catalyst 9120 / 17.12.4 ESW13 encounters kernel unresponsiveness due to OOM process gRPC
CSCwo68312	Cisco Catalyst 9124AXE-E APs identifies antennas wrongly
CSCwo69382	Need to remove Airdrop from the awips signature file on COS APs
CSCwp07242	Cisco Catalyst 9105 AP stops acking frames due to rxstuck
CSCwp59643	COS AP Crash due to Soft lockup and Null pointer dereference in 17.12.4
CSCwp61910	C9130AX - RHL driver bootup failure causes sh crash, which triggers kernel panic
CSCwp62799	C9130AX - RHL bootup failure due to Wbpll handshake failure
CSCwp99685	C9800 WLAN clients stuck in S_AUTHIF_ADD_MOBILE_ACK_WAIT_KM
CSCwq51138	SDA: AP Flooding SSDP Packets on L2-only VLAN with Wireless Pool Enabled
CSCwh80118	Couldnt convert the AP to WGB mode after factory reset to default
CSCwj40021	WLC 9800 AP hostname not displayed completely in out bound syslogs
CSCwj72174	AP2800 connected to same controller is detected as Rogue by other connected AP2800s
CSCwn61711	AP912X: wlc_dpc:506: PSM microcode watchdog fired;

Identifier	Headline
CSCwn91637	9800-80 running 17.12 9136 is working in quad-radio mode and not able to disable it
CSCwn92047	Cisco Catalyst 9105 Access Point controller fails to start after reboot when internal AP is configured as 802.1X supplicant
CSCwn99070	Radio core fails to generate properly causing operational issues
CSCwo08563	SFTP copy not working with IPv6 on COS APs
CSCwo14129	Wave 2 APs experience unresponsiveness due to soft lockup in version 17.12.4 causing system instability
CSCwo16038	Cisco Catalyst 9124 AP workgroup Bridge becomes unreachable connecting to Cisco 2800 Root Access Point when Wi-Fi Multimedia (WMM) is disabled
CSCwo34769	Access Point in FlexConnect mode does not advertise RSNxE in probe response frames
CSCwo37756	Cisco Aironet 1815t AP does not receive an internal DHCP IP address when connected to LAN3
CSCwo43801	AP duplicates DHCP request packets when using FlexConnect mode with Central Switching WLAN
CSCwo53891	Cisco 91xx AP reboots with incorrect reason 'Controller Last Sent: Channel0 Detected'
CSCwo72236	AP prints logs every 30 seconds : \\"RTNETLINK answers: No such file or directory\\"
CSCwo75325	SST:17.12.6: Crash due to radio failures (Beacon Stuck) seen on 1832 or 1852 APs
CSCwo75806	Reassociation Response from AP is delayed for over 200ms on AP WCP component intermittently
CSCwo82821	Cisco Catalyst 9120 Series APs experience kernel panic at txq_hw_fill+0x394
CSCwo89749	Cisco Catalyst 9105 Series APs reboot due to kernel panic
CSCwo94810	Cisco Wireless 916x Series, 9130 Series, and 917x Series APs reject association from IoT client TI module
CSCwp39841	AP9120 crashed as Kernel panic due to NMI watchdog timeout
CSCwp93242	AP serial number in IOX application
CSCwq17491	Observing randomly ICMP packet drops with 3802 AP and propietary high roaming device
CSCwq19861	IOX app not able to communicate with IOt chip

Resolved Issues for Cisco IOS XE 17.12.5

Identifier	Headline
CSCwk33521	Cisco Catalyst 9124, 913x and 916x AP in Local mode encounters kernel unresponsiveness
CSCwm09148	EWC rogue syslogs are missing
CSCwm30964	EWC does not start on RAP after factory reset
CSCwn09549	Cisco Catalyst 9124 MAP fails to join and intermittently disconnects with Cisco Catalyst 9124 RAP
CSCwk85707	SSH access remains unrestricted for EWC-capable APs connecting to the Cisco Embedded Wireless Controller
CSCwn04950	Cisco Embedded Wireless Controller in the Site Survey mode does not connect with the internal AP

Resolved Issues for Cisco IOS XE 17.12.4

Identifier	Headline
CSCwk05030	Controller observes unresponsiveness due to critical software exception
CSCwj93153	Controller becomes unresponsive during WNCd process
CSCwi99296	Cisco Catalyst 9120 AP encounters kernel unresponsiveness with the PC due to wlc_bmac_suspend_mac_and_wait
CSCwj10697	Cisco Catalyst 9124AX AP experiences image upgrade failure
CSCwj20953	Cisco Catalyst 9130AX APs in FlexConnect mode encounter kernel unresponsiveness
CSCwj42847	Cisco Catalyst 9120 AP encounters kernel unresponsiveness on Power Supply Module (PSM) watchdog CS00012342194
CSCwj49502	Cisco Catalyst 9115 AP becomes unresponsive due to Capwapd process crash
CSCwj55168	Multiple Cisco Catalyst 9130 APs encounter kernel unresponsiveness
CSCwj66429	Cisco Catalyst 9115 AP encounters kernel unresponsiveness
CSCwj97748	Cisco Catalyst 9130 AP encounters kernel unresponsiveness with PC at _raw_spin_locK/LR wlan_objmgr_peer_try_get_ref
CSCwi99566	Cisco Catalyst 9124AXI-E AP becomes unresponsive due to channel 36 not being supported in the Jordan regulatory domain
CSCwj34460	Cisco Catalyst 9120 AP encounters kernel unresponsiveness when PC is at wlc_txhinfo2bandunit

Identifier	Headline
CSCwj48018	Cisco Catalyst 9105 AP encounters kernel unresponsiveness when PC is at wlc_ampdu_dotxstatus+0x5c/0x5cc
CSCwh82872	Cisco Catalyst 9115AXI-S AP association request dropped on the Cisco Catalyst 9800-80 Wireless Controller
CSCwi27380	Media stream feature does not work
CSCwi56780	Mac Authentication Bypass (MAB) is not initiated unless the client device is deauthenticated
CSCwj08367	Cisco Catalyst 9800 Wireless Controller generates system report with crash information, segmentation fault - Process = IGMPSN
CSCwj09698	Cisco Catalyst 9800 Wireless Controller encounters an unexpected reset in wncmgrd with a scaled setup while being managed by the Meraki Dashboard
CSCwj26196	Controller running the IOS XE software encounters an unexpected reset while trying to validate the MAC address with the EWLC_APP_INFRA_ID_MAGIC
CSCwj31356	Cisco Catalyst 9800 Wireless Controller reboots due to Radio Resource Management (RRM) process fault on rp_0_0 (rc=139)
CSCwj42408	Controller posture flow does not work when PMF is optional
CSCwj79545	Controller unexpectedly reboots during WNCd process due to assertation failure with invalid BSSID
CSCwj86938	Memory leak in scale network with telemetry shared user events with Cisco Catalyst Center
CSCwi01382	5-GHz and 2.4-GHz radios remain non-operational down in an AP
CSCwi64010	Controller accepts configuration of a reserved IPv6 multicast address as a mobility IPv6 address
CSCwj15376	Cisco NMSP runs into security protocol issues
CSCwj25110	Controller reports incorrect values during SNMP polling
CSCwj33376	Incorrect selection of APs in load balancing
CSCwj34379	Controller encounters unresponsiveness when accessing crimson database
CSCwj40202	Controller does not send RADIUS accounting messages WLAN with PSK/MAB authentication
CSCwj60910	Controller and PI report observe RRM message mismatch
CSCwj67158	Controller does not send mobile address to AP if the CoA is received when the user is in the ip_learn state
CSCwj69755	Controller WebUI is not updating configuration port parameters

Identifier	Headline
CSCwj72370	Controller uses incorrect username for "show platform" command when logging in GUI
CSCwj76892	Controller configures aggregation scheduler parameter incorrectly, causing low downlink speed
CSCwj77128	URL filter allows only letters as the first character
CSCwj82898	Controller is unable to onboard on Cisco Spaces
CSCwj96620	Syntax errors observed in LWAPP
CSCwj96666	Syntax errors observed in LWAPP client
CSCwk02633	RSA key pair is configured in the TrustPoint configuration when EC keypair is selected while creating a trustpoint on the controller
CSCwk07124	802.1X timeout value is set to 0 by default when configuring RLAN through GUI

Resolved Issues 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 Issues 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.

Identifier	Headline
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.
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.

Identifier	Headline
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.
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.

Identifier	Headline
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.
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 Issues 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 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 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.

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)

© 2025 Cisco Systems, Inc. All rights reserved.