Release Notes for Cisco Embedded Wireless Controller on Catalyst Access Points, Cisco IOS XE 17.15.x

First Published: 2024-08-14

Release Notes for Cisco Embedded Wireless Controller on Catalyst Access Points, Cisco IOS XE 17.15.x

Introduction to Cisco Embedded Wireless Controller on Catalyst Access Points

The Cisco Embedded Wireless Controller on Catalyst Access Points is a version of the Cisco IOS XE-based controller software on Catalyst access points (AP). In this solution, a Catalyst AP that is running the Cisco Embedded Wireless Controller on Catalyst Access Points software, is designated as the primary AP. Other APs, referred to as subordinate APs, associate to this primary AP.

The Cisco Embedded Wireless Controller on Catalyst Access Points provides enterprise-level WLAN features while maintaining operational simplicity and affordability. This solution is targeted at small and medium-sized business (SMB) customers or distributed enterprises, and can be run at single site deployments.

- The controllers come with high availability (HA) and seamless software updates. This keeps your services on always, both during planned and unplanned events.
- The deployment can be managed using a mobile application, Cisco Catalyst Center, Netconf/Restconf, web-based GUI, or CLI.

What's New in Cisco IOS XE 17.15.1

Table 1: New and Modified Software Features

Feature Name	Description and Documentation Link
Software-Defined Access (SDA) Restriction Update	Fabric in a Box (FIAB) is now supported from the 17.15.1 release. For more information, see the chapter Software-Defined Access Wireless.

Feature Name	Description and Documentation Link
SuiteB-1X and SuiteB-192-1X Support in FlexConnect Mode for WPA2 and WPA3	From Cisco IOS XE 17.15.1 onwards, Cisco WLAN FlexConnect mode supports enterprise authentication key management (AKM) — SuiteB-192-1X (AKM 12) and SuiteB-1X (AKM 11). This feature supports the configuration of SuiteB-192-1X and SuiteB-1X in FlexConnect mode, and also supports Galois Counter Mode Protocol 128 (GCMP-128), GCMP-256, and Counter Cipher Mode with Block Chaining Message Authentication Code Protocol 256 (CCMP-256) ciphers for pairwise transport keys (PTK) and group temporal key (GTK) derivation in FlexConnect Local Authentication mode and FlexConnect Central Authentication mode. For more information, see the chapter SuiteB-1X and SuiteB-192-1X Support in FlexConnect Mode for WPA2 and WPA3.
Wi-Fi Protected Access (WPA3) Security Enhancements for Access Points	The following are the security enhancements developed in Cisco IOS XE 17.15.1, for APs: • GCMP-256 Cipher and SuiteB-192-1X AKM • SAE-EXT-KEY Support • AP Beacon Protection • Multiple Cipher Support per WLAN • Opportunistic Wireless Encryption (OWE) Support with GCMP-256 Cipher The following commands are introduced: • **security wpa akm sae ext-key** • **security wpa akm ft sae ext-key** • **security wpa akm suiteb-192** • **security wpa akm suiteb** • **security wpa wpa2 ciphers** • **security wpa wpa3 beacon-protection** For more information, see the chapter Wi-Fi Protected Access (WPA3) Security Enhancements for Access Points.
Tier B/C/D Country Support for Cisco Catalyst 9124 Outdoor Access Points	From this release, Cisco Catalyst 9124 Outdoor APs are supported in the following countries: Bosnia, Hong Kong, India, Indonesia, Israel, Jordan, Kuwait, Puerto Rico, Qatar, Saudi Arabia, Singapore, South Africa, Taiwan, Turkey, and United Arab Emirates. For more information, see the chapter Country Codes.

Table 2: New and Modified GUI Features

Feature Name	GUI Path
SuiteB-1X and SuiteB-192-1X Support in FlexConnect Mode for WPA2 and WPA3	**Configuration > Tags & Profiles > WLANs**
Wi-Fi Protected Access (WPA3) Security Enhancements for Access Points	**Configuration > Tags & Profiles > WLANs**

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 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.
- From Cisco IOS XE Dublin 17.12.1 onwards, the maximum supported scale in Cisco Catalyst 9120AX Series APs, Cisco Catalyst 9124AX Series APs, and Cisco Catalyst 9130AX Series APs, is reduced to 50 APs from 100 APs and 1000 clients from 2000 clients.

Compatibility Matrix

The following table provides software compatibility information:

Table 6: Compatibility Information

Cisco Embedded Wireless Controller on Catalyst Access Points	Cisco ISE	Cisco CMX	Cisco Catalyst Center
Cisco IOS XE 17.15.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.

Browser	Version	Operating System	Status	Workaround
Google Chrome	77.0.3865.90	Windows 10 Version 1903 (OS Build 18362.267)	Works	Proceed through the browser warning.
Microsoft Edge	44.18362.267.0	Windows 10 Version 1903 (OS Build 18362.267)	Works	Proceed through the browser warning.
Mozilla Firefox	68.0.2	Windows 10 Version 1903 (OS Build 18362.267)	Works	Proceed through the browser warning.
Mozilla Firefox	69.0.3	Windows 10 Version 1903 (OS Build 18362.267)	Works only if exception is added.	Set the exception.
Google Chrome	78.0.3904.108	macOS Catalina 10.15.1	Does not work	NA

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*.

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 17.15.x software for Cisco Embedded Wireless Controller on Catalyst Access Points.

Choose the appropriate AP software based on the following:

- Cisco Embedded Wireless Controller on Catalyst Access Points software to be used for converting the AP from an unified wireless network CAPWAP lightweight AP to a Cisco Embedded Wireless Controller on Catalyst Access Points-capable AP (primary AP)

- AP software image bundle to be used either for upgrading the Cisco Embedded Wireless Controller on Catalyst Access Points software on the primary AP or for updating the software on the subordinate APs or both

Prior to ordering Cisco APs, see the corresponding ordering guide for your Catalyst or Aironet access point.

Table 8: Cisco Embedded Wireless Controller on Catalyst Access Points Software

Primary AP	AP Software for Conversion from CAPWAP to Cisco EWC	AP Software Image Bundle for Upgrade	AP Software in the Bundle
Cisco Catalyst 9115 Series	C9800-AP-universalk9.17.15.01.zip	C9800-AP-universalk9.17.15.01.zip	ap1g7
Cisco Catalyst 9117 Series	C9800-AP-universalk9.17.15.01.zip	C9800-AP-universalk9.17.15.01.zip	ap1g6
Cisco Catalyst 9120 Series	C9800-AP-universalk9.17.15.01.zip	C9800-AP-universalk9.17.15.01.zip	ap1g7
Cisco Catalyst 9124AXE/I/D	C9800-AP-universalk9.17.15.01.zip	C9800-AP-universalk9.17.15.01.zip	ap1g6a
Cisco Catalyst 9130	C9800-AP-universalk9.17.15.01.zip	C9800-AP-universalk9.17.15.01.zip	ap1g6a

Supported Access Point Channels and Maximum Power Settings

Supported access point channels and maximum power settings on Cisco APs are compliant with the regulatory specifications of channels, maximum power levels, and antenna gains of every country in which the access points are sold. For more information about the supported access point transmission values in Cisco IOS XE software releases, see the *Detailed Channels and Maximum Power Settings* document at https://www.cisco.com/c/en/us/support/ios-nx-os-software/ios-xe-17/products-technical-reference-list.html.

For information about Cisco Wireless software releases that support specific Cisco AP modules, see the "Software Release Support for Specific Access Point Modules" section in the *Cisco Wireless Solutions Software Compatibility Matrix* document.

Guidelines and Restrictions

Internet Group Management Protocol (IGMP)v3 is not supported on Cisco Aironet Wave 2 APs.

Embedded Wireless Controller SNMP configuration is supported in Cisco Catalyst Center.

High memory usage on AP running Embedded Wireless Controller. Enabling **crash kernel** on the AP consumes additional memory on the AP. Hence, if **crash kernel** is enabled, the overall memory usage of the device will increase and will impact the scale numbers. On Cisco Catalyst 9130 Access Points, the memory consumption is a high of 128 MB.

During the EWC HA pair selection, after a power outage, the standby AP fails to come up in the new EWC HA pair. Another EWC capable AP becomes the standby AP and fails to come up as well. To avoid this situation, ensure that the same IP address is enforced on the active or standby APs during HA pair selection.

Interoperability with Clients

This section describes the interoperability of the controller software with client devices.

The following table describes the configurations used for testing client devices.

Table 9: Test Configuration for Interoperability

Hardware or Software Parameter	Hardware or Software Type
Release	Cisco IOS XE Dublin 17.15.x

Access Points	• Cisco Aironet Series Access Points
	  • 1540
	  • 1560
	  • 1815i
	  • 1815w
	  • 1830
	  • 1840
	  • 1850
	  • 2800
	  • 3800
	  • 4800
	• Cisco Catalyst 9105AX Access Points
	• Cisco Catalyst 9115AX Access Points
	• Cisco Catalyst 9117AX Access Points
	• Cisco Catalyst 9120AX Access Points
	• Cisco Catalyst 9124AXE/I/D Access Points
	• Cisco Catalyst 9130AX Access Points

Radio	• 802.11ax • 802.11ac • 802.11a • 802.11g • 802.11n (2.4 GHz or 5 GHz)
Security	Open, PSK (WPA2-AES), 802.1X (WPA2-AES) (EAP-FAST, EAP-TLS), WPA3.

Hardware or Software Parameter	Hardware or Software Type
Cisco ISE	See Compatibility Matrix, on page 6.
Types of tests	Connectivity, traffic (ICMP), and roaming between two APs

The following table lists the client types on which the tests were conducted. Client types included laptops, hand-held devices, phones, and printers.

Table 10: Client Types

Client Type and Name	Driver / Software Version
Wi-Fi 6 Devices (Mobile Phone and Laptop)	
Apple iPhone 11	iOS 14.1
Apple iPhone SE 2020	iOS 14.1
Dell Intel AX1650w	Windows 10 (21.90.2.1)
DELL LATITUDE 5491 (Intel AX200)	Windows 10 Pro (21.40.2)
Samsung S20	Android 10
Samsung S10 (SM-G973U1)	Android 9.0 (One UI 1.1)
Samsung S10e (SM-G970U1)	Android 9.0 (One UI 1.1)
Samsung Galaxy S10+	Android 9.0
Samsung Galaxy Fold 2	Android 10
Samsung Galaxy Flip Z	Android 10
Samsung Note 20	Android 10
Laptops	
Acer Aspire E 15 E5-573-3870 (Qualcomm Atheros QCA9377)	Windows 10 Pro (12.0.0.832)
Apple Macbook Air 11 inch	OS Sierra 10.12.6
Apple Macbook Air 13 inch	OS Catalina 10.15.4
Apple Macbook Air 13 inch	OS High Sierra 10.13.4
Macbook Pro Retina	OS Mojave 10.14.3
Macbook Pro Retina 13 inch early 2015	OS Mojave 10.14.3
Dell Inspiron 2020 Chromebook	Chrome OS 75.0.3770.129
Google Pixelbook Go	Chrome OS 84.0.4147.136
HP chromebook 11a	Chrome OS 76.0.3809.136
Samsung Chromebook 4+	Chrome OS 77.0.3865.105

Client Type and Name	Driver / Software Version
DELL Latitude 3480 (Qualcomm DELL wireless 1820)	Win 10 Pro (12.0.0.242)
DELL Inspiron 15-7569 (Intel Dual Band Wireless-AC 3165)	Windows 10 Home (18.32.0.5)
DELL Latitude E5540 (Intel Dual Band Wireless AC7260)	Windows 7 Professional (21.10.1)
DELL XPS 12 v9250 (Intel Dual Band Wireless AC 8260)	Windows 10 (19.50.1.6)
DELL Latitude 5491 (Intel AX200)	Windows 10 Pro (21.40.2)
DELL XPS Latitude12 9250 (Intel Dual Band Wireless AC 8260)	Windows 10 Home (21.40.0)
Lenovo Yoga C630 Snapdragon 850 (Qualcomm AC 2x2 Svc)	Windows 10(1.0.10440.0)
Lenovo Thinkpad Yoga 460 (Intel Dual Band Wireless-AC 9260)	Windows 10 Pro (21.40.0)
Note For clients using Intel wireless cards, we recommend you to update to the latest Intel wireless drivers if advertised SSIDs are not visible.	
Tablets	
Apple iPad Pro	iOS 13.5
Apple iPad Air2 MGLW2LL/A	iOS 12.4.1
Apple iPad Mini 4 9.0.1 MK872LL/A	iOS 11.4.1
Apple iPad Mini 2 ME279LL/A	iOS 12.0
Microsoft Surface Pro 3 – 11ac	Qualcomm Atheros QCA61x4A
Microsoft Surface Pro 3 – 11ax	Intel AX201 chipset. Driver v21.40.1.3
Microsoft Surface Pro 7 – 11ax	Intel Wi-Fi chip (HarrisonPeak AX201) (11ax, WPA3)
Microsoft Surface Pro X – 11ac & WPA3	WCN3998 Wi-Fi Chip (11ac, WPA3)
Mobile Phones	
Apple iPhone 5	iOS 12.4.1
Apple iPhone 6s	iOS 13.5
Apple iPhone 8	iOS 13.5
Apple iPhone X MQA52LL/A	iOS 13.5
Apple iPhone 11	iOS 14.1
Apple iPhone SE MLY12LL/A	iOS 11.3
ASCOM SH1 Myco2	Build 2.1

Client Type and Name	Driver / Software Version
ASCOM SH1 Myco2	Build 4.5
ASCOM Myco 3 v1.2.3	Android 8.1
Drager Delta	VG9.0.2
Drager M300.3	VG2.4
Drager M300.4	VG2.4
Drager M540	DG6.0.2 (1.2.6)
Google Pixel 2	Android 10
Google Pixel 3	Android 11
Google Pixel 3a	Android 11
Google Pixel 4	Android 11
Huawei Mate 20 pro	Android 9.0
Huawei P20 Pro	Android 9.0
Huawei P40	Android 10
LG v40 ThinQ	Android 9.0
One Plus 8	Android 10
Oppo Find X2	Android 10
Redmi K20 Pro	Android 10
Samsung Galaxy S7	Andriod 6.0.1
Samsung Galaxy S7 SM - G930F	Android 8.0
Samsung Galaxy S8	Android 8.0
Samsung Galaxy S9+ - G965U1	Android 9.0
Samsung Galaxy SM - G950U	Android 7.0
Sony Experia 1 ii	Android 10
Sony Experia xz3	Android 9.0
Xiaomi Mi10	Android 10
Spectralink 8744	Android 5.1.1
Spectralink Versity Phones 9540	Android 8.1
Vocera Badges B3000n	4.3.2.5
Vocera Smart Badges V5000	5.0.4.30
Zebra MC40	Android 5.0
Zebra MC40N0	Android Ver: 4.1.1

Client Type and Name	Driver / Software Version
Zebra MC92N0	Android Ver: 4.4.4
Zebra TC51	Android 7.1.2
Zebra TC52	Android 8.1.0
Zebra TC55	Android 8.1.0
Zebra TC57	Android 8.1.0
Zebra TC70	Android 6.1
Zebra TC75	Android 6.1.1
Printers	
Zebra QLn320 Printer	LINK OS 6.3
Zebra ZT230 Printer	LINK OS 6.3
Zebra ZQ310 Printer	LINK OS 6.3
Zebra ZD410 Printer	LINK OS 6.3
Zebra ZT410 Printer	LINK OS 6.3
Zebra ZQ610 Printer	LINK OS 6.3
Zebra ZQ620 Printer	LINK OS 6.3
Wireless Module	
Intel 11ax 200	Driver v22.20.0
Intel AC 9260	Driver v21.40.0
Intel Dual Band Wireless AC 8260	Driver v19.50.1.6

Issues

Issues describe unexpected behavior in Cisco IOS releases. Issues that are listed as Open in a prior release are carried forward to the next release as either Open or Resolved.

Note All incremental releases will cover fixes from the current release.

Cisco Bug Search Tool

The Cisco Bug Search Tool (BST) allows partners and customers to search for software bugs based on product, release, and keyword, and aggregates key data such as bug details, product, and version. The BST is designed to improve the effectiveness in network risk management and device troubleshooting. The tool has a provision to filter bugs based on credentials to provide external and internal bug views for the search input.

To view the details of a caveat, click the corresponding identifier.

Open Issues for Cisco IOS XE 17.15.1

Identifier	Headline
CSCwh63050	Controller sends IGMP queries without IP address and MAC address on Cisco IOS XE Cupertino 17.9.3
CSCwi04855	APs repeatedly join and disjoin controller with traceback
CSCwj39057	Cisco Catalyst 9130 AP experiences traffic loss and delays due to perceived 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
CSCwj83526	APs become non-operational when connected to Cisco Catalyst 9300 Switch via mGig port
CSCwj85091	Controller unexpectedly reloads while running the **show wireless client mac-address detail** command
CSCwj89538	Cisco Aironet 2802 AP fails to send reassociation response or association request
CSCwk05809	%EVENTLIB-3-CPUHOG message observed on Cisco IOS XE 17.12
CSCwk14917	Controller reloads unexpectedly
CSCwk17102	Client experiences unexpected disconnect due to missing M1 packet
CSCwk17667	Controller reboots due to high ODM memory consumption
CSCwk37983	Client VLAN is retained after changing SSIDs if \"vlan-persistent\" is enabled
CSCwk39866	Client page is stuck in loading state
CSCwk46105	Controller experiences unexpected reloads with high WNCd memory
CSCwk48338	Cisco Catalyst 9130 does not accept clients on the 5 GHz band
CSCwk48634	FlexConnect local switching dropping upstream broadcast ARP from Android devices in data path in Cisco Catalyst 9130 AP
CSCwk52996	Cisco Catalyst 9120 AP unecpectedly reloads along with radio abnormalities on wlc_bmac_suspend_mac
CSCwk54291	Controller voice CAC BW is not cleared
CSCwk58326	Controller sends multicast packets with previous WMI
CSCwk61068	Controller unexpectedly reloads on 17.9.4 with reason "critical process WNCd fault"
CSCwk61854	Configuration update failure when AP is in delete pending state
CSCwk62836	Cisco Catalyst 9120 AP running on Cisco IOS XE Cupertino 17.9.5

Identifier	Headline
CSCwk64235	URL filter incnsistency observed post modifciation
CSCwk66988	Cisco Catalyst 9130 experiences radio failure

Resolved Issues for Cisco IOS XE 17.15.1

Identifier	Headline
CSCwh56566	Controller experiences flow monitor failure due to manual flow record parameters
CSCwh80060	Cisco Wave 2 APs connected to the controller are losing the FlexConnect WLAN-VLAN mapping
CSCwh81071	Slot 2 is down for GB country after performing factory reset
CSCwi16509	APs do not join the controller with invalid radio slot ID error
CSCwi22895	Controller becomes unresponsive within Radio Resource Management (RRM) service due to ReloadReason=Critical process rrm fault
CSCwi27380	Media stream feature does not work
CSCwi28382	Controller reloads unexpectedly due to Keymgmt: Failed to eapol key m1 retransmit failure
CSCwi55714	Controller unexpectedly reboots when handling NMSP TLS connection
CSCwi56780	MAC Authentication Bypass (MAB) is not initiated unless the client device is deauthenticated
CSCwi69251	Cisco Catalyst 9800-40 Wireless Controller becomes unresponsive on Critical process Radio Resource Management (RRM) fault on rp_0_0
CSCwi75759	Cisco Catalyst 9800-40 Wireless Controller reloads due to critical process WNCd fault
CSCwi99276	Controller does not have Network Access Control (NAC) in the policy profile configuration enabled on Prime Infrastructure
CSCwj08367	Cisco Catalyst 9800 Wireless Controller encounters unresponsiveness generating system report, 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
CSCwj25187	Controller does not display the redundancy details on the Web-UI, only on the CLI
CSCwj26196	Controller encounters an unexpected reset while trying to validate the MAC address with the EWLC_APP_INFRA_ID_MAGIC
CSCwj31356	Controller reboots due to Radio Resource Management (RRM) process fault on rp_0_0 (rc=139)

Identifier	Headline
CSCwj36962	Controller reboots unexpectedly due to invalid QoS parameters
CSCwj42408	Controller posture flow does not work when PMF is optional
CSCwj34379	Cisco Catalyst 9800-80 Wireless Controller encounters WNCd issues when accessing Crimson Database
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
CSCwj93153	Controller becomes unresponsive during WNCd process
CSCwk05030	Controller becomes unresponsive due to critical software exception
CSCwj40202	Controller does not send RADIUS accounting messages WLAN with PSK/MAB authentication
CSCwj60910	Controller and PI report observe RRM message mismatch
CSCwh88246	AP does not allow you to apply URL filter after invalid configuration
CSCwi01382	5-GHz and 2.4-GHz radios remain non-operational in an AP
CSCwj67158	Controller does not send mobile address to AP if the CoA is received when the user is in the ip_learn state
CSCwj72370	Controller uses incorrect username for "show platform" command when logging in GUI
CSCwi47294	Per client rate limit with FlexConnect AP is not functioning
CSCwi48980	Controller local password policy does not take effect on GUI login as expected
CSCwi50732	VLAN group support for DHCP and static IP clients feature does not work on FlexConnect Central Switching mode
CSCwi64010	Controller accepts the reserved IPv6 multicast address to be configured as a mobility multicast IPv6 address
CSCwi66582	Controller returns with error while uploading backup file with FTP on GUI
CSCwi69093	Controller GUI shows incorrect number of clients connected to the AP
CSCwj76892	Controller configures aggregation scheduler parameter incorrectly, causing low downlink speed
CSCwi83124	Pop-ups are not displayed correctly in dark mode in the controller
CSCwj00465	Active controller becomes ActiveRecovery when the redundancy port link is down

Identifier	Headline
CSCwj01446	Personal Identity Verification (PIV) authentication requires an additional backslash in the redirection URL to work successfully
CSCwj04177	AP undergoing Extensible Authentication Protocol (EAP) fails if the password is more than 31 characters
CSCwj15376	Cisco NMSP runs into security protocol issues
CSCwj25110	Controller reports incorrect values during SNMP polling
CSCwj77128	URL filter allows only letters as the first character
CSCwj33376	Incorrect selection of APs in load balancing
CSCwj94201	Controller experiences unresponsiveness CPUHOG
CSCwj68763	Enhanced URL is missing after FlexConnect AP CAPWAP flap
CSCwk35891	Controller experiences unresponsiveness after displaying "\clear ap geolocation derivation\" message
CSCwj42562	GUI does not display PC analytics statistics
CSCwk44459	Loadbalancer server holds incorrect AP IP address and stale entries
CSCwi44211	The "show run" command results are different from restore configuration
CSCwj29406	The "show ap summary sort descending client-count" command shows wrong client count
CSCwi29216	Unsupportive characters in the description field prevents re-sync
CSCwj83935	Controller shows tech X is empty when previous tech X term length stop didn't finish before SSH close
CSCwi70760	Controller encrypts ApDnaGlobalCfg token when the password encryption is configured using AES
CSCwj96620	Syntax errors observed in CISCO-LWAPP-DOT11-CLIENT-MIB
CSCwj96666	Syntax errors observed in CISCO-LWAPP-DOT11-MIB
CSCwj97107	Standby controller does not take active role after reloading the active controller with "reload slot" command
CSCwk02633	An RSA key pair is configured in the truspoint configuration when an EC keypair is selected when creating a trustpoint on the controller
CSCwk25182	Controller throws password policy alert while logging in GUI using TACACS+ credentials after upgrading to Cisco IOS XE 17.14
CSCwk28680	Controller unexpectedly reloads due to Cisco QuantumFlow Processor (QFP) ucode while updating the drop statistics

Identifier	Headline
CSCwj33979	Output for the **show ap summary** command takes lengthy duration to complete

Troubleshooting

For the most up-to-date, detailed troubleshooting information, visit the Cisco TAC website at:

https://www.cisco.com/en/US/support/index.html

Go to **Product Support** and select your product from the list, or enter the name of your product. Look under **Troubleshoot and Alerts** to find information about the problem that you are experiencing.

Related Documentation

Information about Cisco IOS XE is available at:

https://www.cisco.com/c/en/us/products/ios-nx-os-software/ios-xe/index.html

All the support documentation for Cisco Catalyst 9100 Access Points are available at: https://www.cisco.com/c/en/us/support/wireless/catalyst-9100ax-access-points/tsd-products-support-series-home.html

Cisco Validated Designs documents are available at:

https://www.cisco.com/go/designzone

Cisco Embedded Wireless Controller on Catalyst Access Points

For support information, see the following documents:

- Cisco Wireless Solutions Software Compatibility Matrix
- Cisco Embedded Wireless Controller on Catalyst Access Points Software Configuration Guide
- Cisco Embedded Wireless Controller on Catalyst Access Points Command Reference Guide

Installation guides for Catalyst Access Points are available at:

https://www.cisco.com/c/en/us/support/wireless/catalyst-9100ax-access-points/products-installation-guides-list.html

For all Cisco Wireless Controller software-related documentation, see:

https://www.cisco.com/c/en/us/support/wireless/catalyst-9800-series-wireless-controllers/tsd-products-support-series-home.html

Wireless Products Comparison

- Use this tool to compare the specifications of Cisco wireless APs and controllers:

  https://www.cisco.com/c/en/us/products/wireless/wireless-lan-controller/product-comparison.html

- Product Approval Status:

  https://prdapp.cloudapps.cisco.com/cse/prdapp/jsp/externalsearch.do?action=externalsearch&page=EXTERNAL_SEARCH

- Wireless LAN Compliance Lookup:

  https://www.cisco.com/c/dam/assets/prod/wireless/wireless-compliance-tool/index.html

Cisco Access Points–Statement of Volatility

The STATEMENT OF VOLATILITY is an engineering document that provides information about the device, the location of its memory components, and the methods for clearing device memory. Refer to the data security policies and practices of your organization and take the necessary steps required to protect your devices or network environment.

The Cisco Aironet and Catalyst AP Statement of Volatility (SoV) documents are available on Cisco Trust Portal at https://trustportal.cisco.com/c/r/ctp/trust-portal.html#/.

You can search by the AP model to view the SoV document.

Cisco Connected Mobile Experiences

Cisco Connected Mobile Experiences Documentation

Cisco Catalyst Center

Cisco Catalyst Center Documentation

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business 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.