Release Notes for Cisco Embedded Wireless Controller on Catalyst Access Points, Cisco IOS XE 16.12.x

First Published: 2020-01-08

Last Modified: 2022-09-27

Release Notes for Cisco Embedded Wireless Controller on Catalyst Access Points, Cisco IOS XE Gibraltar 16.12.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. In this solution, a Catalyst access point (AP) that is running the Cisco Embedded Wireless Controller on Catalyst Access Points software, is designated as the primary AP. Other APs, referred to as subordinate APs, associate to this primary AP.

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

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

What's New in Cisco IOS XE Gibraltar 16.12.8

There are no new features in this release.

What's New in Cisco IOS XE Gibraltar 16.12.7

There are no new features in this release.

What's New in Cisco IOS XE Gibraltar 16.12.6a

There are no new features in this release.

What's New in Cisco IOS XE Gibraltar 16.12.5

There are no new features in this release.

What's New in Cisco IOS XE Gibraltar 16.12.4a

There are no new features in this release.

What's New in Cisco IOS XE Gibraltar 16.12.3

There are no new features in Cisco IOS XE Gibraltar 16.12.3 release.

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 1: 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 9130 Series[1]	Cisco Aironet 1815w
	Cisco Aironet 1830 Series
	Cisco Aironet 1840 Series
	Cisco Aironet 1850 Series
	Cisco Aironet 2800 Series
	Cisco Aironet 3800 Series
	Cisco Aironet 4800 Series
	Cisco Catalyst 9115 Series
	Cisco Catalyst 9117 Series
	Cisco Catalyst 9120 Series
	Cisco Catalyst 9130 Series

[1] Cisco Catalyst 9130AXE is not supported in Cisco IOS XE 16.12.2s and 16.12.3.

Table 2: Image Types and Supported APs in Cisco Embedded Wireless Controller on Catalyst Access Points

Image Type	Supported APs
ap1g4	Cisco Aironet 1810 Series Cisco Aironet 1830 Series Cisco Aironet 1850 Series
ap1g5	Cisco Aironet 1815i Cisco Aironet 1815w Cisco Aironet 1540 Series Cisco Aironet 1840 Series
ap1g6	Cisco Catalyst 9117 Series
ap1g6a	Cisco Catalyst 9130 Series
ap1g7	Cisco Catalyst 9115 Series Cisco Catalyst 9120 Series
ap3g3	Cisco Aironet 2800 Series Cisco Aironet 3800 Series Cisco Aironet 4800 Series Cisco Aironet 1560 Series

Maximum APs and Clients Supported

Table 3: Scale Supported in Cisco EWC Network

Primary AP Model	Maximum APs Supported	Maximum Clients Supported
Cisco Catalyst 9105 AWI	50	1000
Cisco Catalyst 9115 Series	50	1000
Cisco Catalyst 9117 Series	50	1000
Cisco Catalyst 9120 Series	100	2000
Cisco Catalyst 9130	100	2000

Note If 25 to 100 APs have joined the EWC network, the maximum clients on the EWC internal AP is limited to 20.

Compatibility Matrix

The following table provides software compatibility information:

Table 4: Compatibility Information

Cisco Embedded Wireless Controller on Catalyst Access Points	Cisco ISE	Cisco CMX	Cisco DNA Center
Gibraltar 16.12.x	2.6 2.4 2.3	10.6.2 10.6 10.5.1	1.3.3.0

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 5: 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

Upgrading the Controller Software

This section covers the various aspects of upgrading the controller software.

For information on upgrading the controller software, see the "Software Management" section in the Cisco Embedded Wireless Controller on Catalyst Access Points Online Help. For information on performing an image upgrade using CLI steps, see the Initiating Pre-Download (CLI) section.

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

Note An AP that joins the Embedded Wireless Controller (EWC) network, should already be running the software Version 8.10.x or later, or Version 16.12.x or later. If this is not the case, upgrade the AP with either of these options *before* the AP joins the EWC network.

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 6: 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-universalk9.16.12.8.zip C9800-AP-universalk9.16.12.7.zip C9800-AP-universalk9.16.12.6a.zip C9800-AP-universalk9.16.12.5.zip C9800-AP-universalk9.16.12.4a.zip C9800-AP-universalk9.16.12.3.zip C9800-AP-universalk9.16.12.2s.zip	C9800-AP-universalk9.16.12.8.zip C9800-AP-universalk9.16.12.7.zip C9800-AP-universalk9.16.12.6a.zip C9800-AP-universalk9.16.12.5.zip C9800-AP-universalk9.16.12.4a.zip C9800-AP-universalk9.16.12.3.zip C9800-AP-universalk9.16.12.2s.zip	ap1g7
Cisco Catalyst 9117 Series	C9800-AP-universalk9.16.12.8.zip C9800-AP-universalk9.16.12.7.zip C9800-AP-universalk9.16.12.6a.zip C9800-AP-universalk9.16.12.5.zip C9800-AP-universalk9.16.12.4a.zip C9800-AP-universalk9.16.12.3.zip C9800-AP-universalk9.16.12.2s.zip	C9800-AP-universalk9.16.12.8.zip C9800-AP-universalk9.16.12.7.zip C9800-AP-universalk9.16.12.6a.zip C9800-AP-universalk9.16.12.5.zip C9800-AP-universalk9.16.12.4a.zip C9800-AP-universalk9.16.12.3.zip C9800-AP-universalk9.16.12.2s.zip	ap1g6
Cisco Catalyst 9120 Series	C9800-AP-universalk9.16.12.8.zip C9800-AP-universalk9.16.12.7.zip C9800-AP-universalk9.16.12.6a.zip C9800-AP-universalk9.16.12.5.zip C9800-AP-universalk9.16.12.4a.zip C9800-AP-universalk9.16.12.3.zip C9800-AP-universalk9.16.12.2s.zip	C9800-AP-universalk9.16.12.8.zip C9800-AP-universalk9.16.12.7.zip C9800-AP-universalk9.16.12.6a.zip C9800-AP-universalk9.16.12.5.zip C9800-AP-universalk9.16.12.4a.zip C9800-AP-universalk9.16.12.3.zip C9800-AP-universalk9.16.12.2s.zip	ap1g7
Cisco Catalyst 9130 Series	C9800-AP-universalk9.16.12.8.zip C9800-AP-universalk9.16.12.7.zip C9800-AP-universalk9.16.12.6a.zip C9800-AP-universalk9.16.12.5.zip C9800-AP-universalk9.16.12.4a.zip C9800-AP-universalk9.16.12.3.zip C9800-AP-universalk9.16.12.2s.zip	C9800-AP-universalk9.16.12.8.zip C9800-AP-universalk9.16.12.7.zip C9800-AP-universalk9.16.12.6a.zip C9800-AP-universalk9.16.12.5.zip C9800-AP-universalk9.16.12.4a.zip C9800-AP-universalk9.16.12.3.zip C9800-AP-universalk9.16.12.2s.zip	ap1g6a

Guidelines and Restrictions

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

Embedded Wireless Controller SNMP configuration is supported in DNAC.

High memory usage on AP running Embedded Wireless Controller. Enabling **crash kernel** on the AP consumes additional memory on the AP. Hence, if **crash kernel** is enabled, the overall memory usage of the device will increase and will impact the scale numbers. On Cisco Catalyst 9130 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 7: Test Configuration for Interoperability

Hardware or Software Parameter	Hardware or Software Type
Release	Cisco IOS XE Gibraltar 16.12.x
Access Points	• Cisco Aironet Series Access Points • 1540 • 1560 • 1815i • 1815w • 1830 • 1840 • 1850 • 2800 • 3800 • 4800 • Cisco Catalyst 9115AX Access Points • Cisco Catalyst 9117AX Access Points • Cisco Catalyst 9120AX Access Points • Cisco Catalyst 9130AX Access Points

Hardware or Software Parameter	Hardware or Software Type
Radio	• 802.11ax • 802.11ac • 802.11a • 802.11g • 802.11n (2.4 GHz or 5 GHz)
Security	Open, PSK (WPA2-AES), 802.1X (WPA2-AES) (EAP-FAST, EAP-TLS), WPA3.
Cisco ISE	See Compatibility Matrix, on page 4.
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.

Caveats

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

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

There are no new Open and Resolved Caveats in Cisco IOS XE Gibraltar 16.12.3 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 Gibraltar 16.12.8

There are no open caveats.

Open Caveats for Cisco IOS XE Gibraltar 16.12.7

There are no open caveats.

Open Caveats for Cisco IOS XE Gibraltar 16.12.6a

Caveat ID	Description
CSCvw89083	The Cisco Catalyst 9120AX Series APs disconnect from the controller after receiving CAPWAP payload.
CSCvw99524	The RFID entries are not updated in the Cisco Catalyst 9800-40 Wireless Controller.
CSCvx13355	The Dynamic Channel Assignment (DCA) fails when the outdoor AP is on channel 100.
CSCvx40586	The controller does not sort the received RFID RSSI from APs, before sending 16 APs to the connector.
CSCvx44618	Devices are stuck when the controller consumes Internet Control Message Protocol (ICMP) randomly from 8821 phones.
CSCvr66442	The "Call Home EEM cb" process causes high CPU two days after increasing the logging buffer size.
CSCvu39249	Cisco Catalyst 9115 Series APs participate in the Air Quality report unexpectedly.
CSCvv78921	The controller console logs display error messages and tracebacks.
CSCvv84085	The new AP filter name does not reflect the filter name changes for the same tags.
CSCvx01835	The AP primary, secondary, or tertiary name configuration fails in the command line and SNMP.
CSCvz07021	The USB port on AP in the AP default-group needs to be disabled by default.

Open Caveats for Cisco IOS XE Gibraltar 16.12.5

Caveat ID	Description
CSCvv92772	OBSS-PD configuration from the RF profile does not get pushed to the AP.

Open Caveats for Cisco IOS XE Gibraltar 16.12.4a

Caveat ID	Description
CSCvs70701	APs are randomly taking longer time for off-channel scanning.

Caveat ID	Description
CSCvs77557	Cisco Aironet 3802 AP is not able to acknowledge EAP frames (EAP-TLS).
CSCvt52832	Cisco Catalyst 9120 AP reloads unexpectedly after few days of uptime.
CSCvt68112	Cisco Catalyst 9130 AP: OEAP GUI is not accessible.
CSCvt79194	Clients associated to Wave 2 AP having local switching WLAN with native VLAN is not able to resolve ARP.
CSCvt94052	Controller crashes while changing the password for an existing user.
CSCvu18085	Cisco Catalyst 9117 AP: Dot1x authentication is not working for clients.
CSCvu38986	Memory leak is observed under wncd_x due to CAPWAP messaging.
CSCvu40287	Cisco Catalyst 9120 AP reloads unexpectedly with watchdog_last.status reason:14.
CSCvu42653	Controller is not showing correct antenna mode.
CSCvu47560	Client goes into *exclusionlist* even when client exclusion is disabled.
CSCvu50834	Cisco Aironet 3802 AP: No Rx packets are seen for 5-GHz radio.
CSCvu54413	RFID OIDs are failing when AIRESPACE-WIRELESS-MIB RFID MIBs are used.
CSCvu55303	Cisco Catalyst 9120 AP: Kernel panic crash is observed due to sockets_in_use.
CSCvu57562	Cisco Catalyst 9130 AP is not discovering controller using the IP address returned in DHCP option 43 or DNS.
CSCvu58139	Cisco DNA Center 1.3.3.4: Default RF profile channel is configured as Best in Fabric-In-A-Box installation.
CSCvu58564	AP uses non-allowed channel on dual radio when setting is changed to 5Ghz.
CSCvu60464	Deletion and creation of second Control Plane IP is failing due to RPC ordering.
CSCvu66043	Cisco Catalyst 9130 AP is not sending DHCP messages over the air.

Caveat ID	Description
CSCvu71736	Cisco Catalyst 9100 Series AP: AXI-H AP models have 5Ghz radio operationally down with regulatory domain not supported for -H.
CSCvu71871	Cisco Catalyst 9800-80 controller crashes with SIGSEGV while removing timer RB tree color.
CSCvu73873	Cisco Catalyst 9800-80 controller is sending client traffic out of AP manager interface.
CSCvu75017	Cisco Catalyst 9115 AP: Syslog is only seen when using \"Kern\" facility value in AP join profile.
CSCvu78070	wncd crash is observed on Cisco IOS XE 16.12.3ES3.
CSCvu80092	RADIUS attribute [80] Message-Authenticator is not included for AP authorization.
CSCvu87637	Controller reloads unexpectedly due to double-linked list corruption.
CSCvu89996	AP disjoins after a client connects to SSID using LDAP with mode secure.

Open Caveats for Cisco IOS XE Gibraltar 16.12.2

Note For AP-specific bugs on Cisco IOS XE Gibraltar 16.12.x, see the Release Notes for Cisco Catalyst 9800 Series Wireless Controller, Cisco IOS XE Gibraltar 16.12.x.

Caveat ID	Description
CSCvr44175	System displays memory warning during the controller image download.
CSCvr39352	Traceback is observed after a switchover on the Cisco Catalyst 9120AXI AP.
CSCvs23423	After an image upgrade or a network reboot the preferred controller might not become the active EWC controller.
CSCvq58496	The **write erase** command is not activating startup-config sync to all the EWC-capable devices.
CSCvq82908	Controller displays error message after an HA switchover.

Resolved Caveats for Cisco IOS XE Gibraltar 16.12.8

There are no resolved caveats.

Resolved Caveats for Cisco IOS XE Gibraltar 16.12.7

Caveat ID	Description
CSCvz50654	Backout of the following bugs: CSCvy96790 and CSCvy72750.

Resolved Caveats for Cisco IOS XE Gibraltar 16.12.6a

Caveat ID	Description
CSCvv92772	The OBSS-PD configuration from WebUI does not get pushed to APs mapped to the RF profile.
CSCvw49225	Chromebook or Linux with Intel 11ax adapter does not connect to 11ax APs in local mode.
CSCvw50596	The controller crashes due to critical process RRM fault on rp_0_0 (rc=139).
CSCvw79225	The controller reloads due to qcp-ucode crash when the NBAR engine receives invalid packet length.
CSCvx27079	CMX in Non-FIPS mode cannot connect to the controller in FIPS mode. Certificate Validation Error.
CSCvx38286	The radarScan flag is not set for AP with channel 36 and channel width 160 MHz.
CSCvx47799	Apple iPhone iOS 14.4 PSK to SAE switch fails occasionally and the AP does not respond to client commit 1.
CSCvx77928	RRM ends abnormally while executing the Grouping Flush pending list.
CSCvx83965	WNCD ends abnormally at rrm_client_coverage_hole_algorithm.
CSCvy04449	Fragmented ping pushes to 100% CPU forever.
CSCvu98612	SAE iPSK uses the WLAN passphrase when there is no client specific passphrase received from the AAA server.
CSCvv19020	Client gets stuck in the Authenticating state while connecting to SAE IPSK + LWA.

Caveat ID	Description
CSCvy72750	Wireless controller is unable to use the **wireless broadcast vlan X** command.
CSCvy96790	Controller issue with **IsBroadcastEnable** as the GUI shows **Enabled** instead of **Disabled** and vice-versa.
CSCvr99905	Client gets stuck at **IPLEARN_PENDING** state in the controller or AP after **flex 11r local auth roam**.
CSCvt21958	Frame ID mismatch followed by FW radio 0 crash results in packet drops.
CSCvt86201	The WNM-notification bit in the Beacon frame is wrong in the Cisco Catalyst 9120 Series APs.
CSCvu31443	The WNM-notification bit in the Beacon frame is wrong in the Cisco Catalyst 9120 Series APs, in Flex Connect mode
CSCvu37638	Cisco Catalyst 9115 Series APs or 9120 Series AP crash continuously.
CSCvw51418	Probe suppression on macro cell does not work in Cisco Catalyst 9120 Series AP.
CSCvw53332	Dual5G radio/RHL NDP is transmitted on serving DFS channel without waiting for CAC timer to complete.
CSCvw87209	Kernel panic with PC occurs at rb_erase+0x220/0x33c while running overnight longevity.
CSCvx21682	Cisco Catalyst 9117AX Series APs skip concurrent FW coredump to avoid corruption.
CSCvx24439	Vulnerabilities are observed in Frame Aggregation and Fragmentation of 802.11ax APs [SPF 8.0].
CSCvx24452	Vulnerabilities are observed in Frame Aggregation and Fragmentation of 802.11ax APs [SPF 10.0].
CSCvx37875	Transmission power discrepancies observed in Cisco Catalyst 9130AX Series APs and Cisco Catalyst 9117AX Series APs.
CSCvx44538	NTP vulnerability is observed due to DHCP assigned NTP.
CSCvx61201	Clients get incorrect AP VLAN IP with Cisco Aironet 2800 AP in flex mode.
CSCvy24126	Cisco Catalyst 9105, 9115, or 9120 Series APs display 100% channel utilization.

Caveat ID	Description
CSCvy24397	Local mode AP deletes client if there is no response to EAP request within 30 seconds.
CSCvy35021	Cisco Catalyst 9120 and 9105 APs reload unexpectedly during regular operation due to kernel panic.
CSCvy75300	802.11ax APs: Kernel crash due to QCA Fragment and Forge patch for CVE-2020-24587.

Resolved Caveats for Cisco IOS XE Gibraltar 16.12.5

Caveat ID	Description
CSCvu18085	Cisco 9117 AP: Client authentication to Dot1x SSID (EAP type PEAP) fails on Cisco 9117 AP.
CSCvu23563	Cisco 9130 AP does not forward EAP-TLS packets intermittently. Increase in the drop_memfail counter.
CSCvu39206	Cisco 9130 AP: MTU mismatch between NSS and CAPWAP.
CSCvv22110	Cisco 9130 AP multicast traffic fails after GTK key index rotation for Vocera clients.
CSCvv35000	WPA3 SAE does not work EWC, in Cisco IOS XE 17.3 Release.
CSCvv51321	New AP joins an anchor controller with a different mobility group name.
CSCvw37503	Cisco 9105/9115/9120 APs experience unexpected "assert" kernel panics with Target Wait Time enabled
CSCvw52979	Cisco 9120 AP crashes after upgrade from Cisco IOS XE 17.3.1 to Cisco IOS XE 17.3.2a

Resolved Caveats for Cisco IOS XE Gibraltar 16.12.4a

Caveat ID	Description
CSCvi48253	Self-signed certificates cannot be created after the time expires.
CSCvt23051	Cisco 9120AX AP: AP does not use the correct data rates.
CSCvt51865	Unable to restrict the Guest User account to a specific SSID.

Caveat ID	Description
CSCvu34313	Cisco Catalyst 9800-80 Controller crashes frequently with corrupted stack ending in Sanet function.
CSCvs87163	Lobby admin with external RADIUS authentication is not working.
CSCvt75852	New AP joins an anchor controller with a different mobility group name.
CSCvu30088	Slow memory leak due to WNCD kernel process.
CSCvr55603	Cisco Aironet 3700 AP with HALO experiences unexpected reloads.
CSCvt17820	Client gets excluded after VLAN changes post machine and user authentication.
CSCvt37835	Client is unable to associate due to DOT11_STATUS_DENIED_RATES when extended rates are used.
CSCvt29596	Current Tx rate for 802.11AX clients are displayed incorrectly.
CSCvt63940	Authentication fails in Zebra clients, when local authentication is configured in the policy profile.
CSCvu37330	Client is getting deleted due to DOT11_STATUS_DENIED_RATES.
CSCvt47787	Roaming is not successful when NAC is enabled in the policy profile.
CSCvu04970	Cisco Catalyst 9800-CL Controller running IOS XE Gibraltar 16.12.2s wncd crashes due to CPU HOG.
CSCvu41863	Controller does not send the discovery response with its public IP after reboot.
CSCvr46316	Controller does not populate AP load information in the discovery response.
CSCvs39458	AP Link Latency feature is not working.
CSCvs60927	Frequent AP channel changes are observed on 5GHz band radio.
CSCvt19281	XOR channel changes frequently when band configuration is static.
CSCvs72078	Values of client retries and Rx packets on Cisco DNA-C are different from the values seen on the AP.

Caveat ID	Description
CSCvt55482	Controller shows incorrect number of interferers.
CSCvs93903	WNCd process down due to assert for BSSID magic check.
CSCvt34987	Cisco Catalyst 9800-80 Controller HA running 'wncd' crashes frequently.
CSCvu19379	Do not present "host mode" configuration options when the RLAN profile is set to open.
CSCvs62246	The WebUI is not showing 2.4GHz channels 12, 13, or 14 for radios in country's that support these channels.
CSCvt00145	Optimize SVI/VLAN page loading.
CSCvt40291	Controller GUI: AP page is stuck in buffering mode (refresh to recover the page) when filters are applied.
CSCvs94544	AP mode count is incorrect in the **show wireless summary** output.
CSCvr24930	Observed wncd crash@ewlc_dgram_msg_and_msgbuf_free with ISSU flow in scale.
CSCvu37389	Traceback: When AP's interface operational status goes down, SNMP trap triggers, and device reloads.
CSCvu15936	FlexConnect local-sw client is not assigned to VLAN1 when VLAN assignment is done through AAA.
CSCvp76426	Controller does not honour timezone when configuring DCA anchortime.
CSCvs77734	Frequent channel changes on the Cisco AP Aironet 4800 AP slot 0 radio using 5GHz.
CSCvs83955	Control packets not honoring Mobility PMTU.
CSCvu04994	Controller GUI: SNMPv3 privilege and authentication credentials are swapped when adding a user.
CSCvs81893	SNMP v3: Users page on the GUI does not allow configuration of passwords with special characters.
CSCvt19605	Guest anchor fails to load balance clients across anchors.
CSCvt23733	AP CAC GUI parameter displays incorrect unit. Displays bytes instead of "medium time".

Caveat ID	Description
CSCvt34247	AAA page does not load after upgrading to IOS XE Gibraltar 16.12.2s.
CSCvt34307	FT gets enabled during static WEP WLAN creation - WLAN modification throws error.
CSCvt55181	Unable to configure SNMP settings through the GUI in Japanase mode.
CSCvt64768	Unable to delete or deauthenticate excluded clients through the GUI.
CSCvt96188	Deleting a policy profile that is mapped under a policy tag should display a warning.
CSCvr91736	Tri Radio: Controller GUI does not display slot-2 details in the 360 degree view.
CSCvs73952	Client count shows zero in the **show ap dot11 5ghz/2.4ghz load-info** command output while CHD is disabled.
CSCvu23990	Controller displays that 802.11ac is not supported on XOR radios of APs.
CSCvt83553	Cisco Catalyst 9800-40 Controller: Stale FMAP-FP/CPP tunnel issue.
CSCvp88342	Controller may reload as WNCD process is held down with scaled clients.
CSCvs03712	Data rates need to be updated when the client is moving from one AP to another.
CSCvt24635	CAPWAP DTLS session is closed for AP, because of the DTLS server session shutdown.
CSCvt63822	AP sends lower bytes of packets while performing PMTU negotiations.
CSCvt73263	DTLS teardown is observed on 9120, 9115, and 9105 series of APs.
CSCvs68187	Controller-AP: Primary controller name and IP address mismatch.
CSCvs83590	AP Policy/RF/Site tags set to UNKNOWN unless tag-config is explicitly written from the controller.
CSCvs63467	IPv6 dual stack does not work.
CSCvr68729	HA failed to initialize NVRAM after multiple power cycles.

Caveat ID	Description
CSCvs03177	Client stuck in IP learn state with FlexConnect local switching + central DHCP + DHCP required.
CSCvs11453	When the power box is reset, DNS resolution for Radius and TACACS is delayed for scale.
CSCvs50944	Controller loses smart licensing registration if integrated with DNA spaces after a reboot.
CSCvt06125	Cisco Aironet 1570 series AP crashes if WLAN with ID >= 17 is configured in the policy tag.
CSCvt08645	Multicast replicates over CAPWAP with global multicast disabled
CSCvt31138	Controller goes down and reloads when AVC is enabled.
CSCvt31798	Cisco 9800 running IOS XE Gibraltar 16.12.3 does not send RSSI messages over NMSP.
CSCvt34850	CWA GA scenario client removed after export anchor response received from WLC due profile plumb.
CSCvt41053	Controller is assigned to native VLAN instead of client VLAN.
CSCvt75205	Controller crashes on WMM action, while roaming.
CSCvt83796	APs do not apply client QoS policy in FlexConnect local-sw and local-auth.
CSCvs75087	Global AP pre-image download is not working.
CSCvs82976	CDP entries are not showing up on the controller.
CSCvt27421	Cannot remove AdvIPServices license.
CSCvt27712	Critical Syslog notification support required when unsupported SFPs are connected.
CSCvt29373	9800-40/80 UDP Port 5246 based ACL filter fails to select DTLS encrypted CAPWAP control packets.
CSCvt30657	Controller crashed with the following reason "Critical process cpp_cp_svr fault on fp_0_0 (rc=134)".
CSCvt47898	Controller reloads when processing AVC or FNF.
CSCvt52436	Controller is unable to downgrade license: Device is not authorized to use the given license level.

Caveat ID	Description
CSCvt61509	Cisco Aironet 3700 APs are unable to join controller as the VLAN interface name exceeds character limit in flex profile.
CSCvt62706	Require MAB username delimiter with single hypen.
CSCvt79712	Client is deleted due to the CO_CLIENT_DELETE_REASON_NOOP reason code.
CSCvt80690	ARP request comes from a formerly active controller on HA with split brain scenario.
CSCvt31484	Controller may crash when an AP joins and does not report the correct radios.
CSCvt33624	Cisco Aironet 2800 AP - XOR in 5g: Clients unable to join, AP deauth reason "Invalid group cipher (0x0012)?".
CSCvt49983	Invalid values for AP performance profile.
CSCvs89556	Pubd crash observed just after SSO.
CSCvs06271	RRM AP transmit power is not moving into the maximum or minimum configured power.
CSCvu31306	CWA ACL is removed from the existing flex AP, when a new flex profile is created with same ACL.
CSCvt01659	Cisco Wave1 AP: Client traffic is stuck after client is in RUN state for CWA/LWA.
CSCvt70299	Radius server password field shows no value (blank) in the GUI.
CSCvr86115	Controller GUI has no option to configure AP LED state for IOS APs.
CSCvt17800	Unable to map the attribute map to a user through the GUI.
CSCvu36251	CleanAir Admin Status is displayed as DISABLED on controller Japanese GUI.
CSCvt18875	Basic Wireless setup error, "Use of default ACL preauth v4 is not permitted".
CSCvt13127	Cisco Catalyst 9800-CL Controller is unable to display medium power when AP sends 25W POE message.

Caveat ID	Description
CSCvt17801	Cisco Aironet AP 2800/3800/4800/1560 and Cisco IW 6300 AP gets into a loop after attempting to join controller with FIPS enabled.
CSCvm68624	Cisco Wave 1 AP console displays 'DTX DUMP' logs.
CSCvn25452	Cisco Aironet 2800/3800/4800/1560 APs unexpectedly reloads.
CSCvo10708	Cisco Aironet 2800 and 3800 APs exhibit choppiness during the multicast voice call.
CSCvo83091	FlexConnect AP in standalone mode gets stranded and does not send CAPWAP discovery.
CSCvp54103	Cisco Wave 1 APs reload unexpectedly with 'Unexpected exception to CPU' in logs.
CSCvp70382	Kernel panic is observed.
CSCvp86151	Cisco Wave 1 AP: Radio is reset with code 44.
CSCvq27679	Cisco Aironet 1572 AP: Radio is reset due to pak count mismatch, false detection.
CSCvq76143	Cisco Aironet 2800 AP reloads unexpectedly on Sxpd process.
CSCvq81388	Cisco Wave 1 AP: Radio is reset with code 44.
CSCvq95330	Cisco Wave 2 APs: Workgroup bridge (WGB) does not send Internet Access Point Protocol (IAPP) message in static IP config.
CSCvr10424	Cisco FlexConnect AP drops UDP packet (port 2598).
CSCvr50874	Cisco Aironet 3800 AP: Kernel panic crash is observed.
CSCvr75831	Cisco Wave 1 AP: Clients are losing connectivity while roaming.
CSCvr76299	Decipher radio reset code 44 to more specific reason codes.
CSCvr87573	Cisco Aironet 2800/3800/4800/1560 series AP stops sending broadcast address resolution protocol (ARP) to wireless.
CSCvr93760	VLAN bridging problem on Cisco Aironet 1810W AP with Remote LAN (RLAN).

Caveat ID	Description
CSCvr97142	Root Access Point (RAP) drops radio connection, causing the Mesh Access Point (MAP) to drop. After restoring the connection, switches are not able to pass traffic.
CSCvs00593	Cisco Aironet 3800 AP is failing to send Neighbor Discovery Protocol (NDP) Tx on 5GHz.
CSCvs02759	Beacon is stuck followed by firmware assert. The AP radio is on channel 36 while controller thinks it's on different channel.
CSCvs12223	Cisco Aironet 3802 AP crash on watchdog reset (wcpd).
CSCvs19137	Authentication failure Extensible Authentication Protocol (EAP) timeout on a Cisco Aironet 1852 AP with data Datagram Transport Layer Security (DTLS) encryption isenabled.
CSCvs22835	Cisco AP with SHA2 message integrity check (MIC) certificate fails to join controller.
CSCvs28459	Low Received Signal Strength Indicator (RSSI) on 2.4GHz for Cisco Catalyst 9120AX-E AP as compared Cisco Aironet 2800 AP.
CSCvs41893	Cisco Aironet 3702 AP reloads unexpectedly.
CSCvs52266	Cisco Catalyst 9800-CL Controller is displaying wrong Application Visibility and Control (AVC) data on the GUI page.
CSCvs70502	Cisco Wave 1 AP reloads unexpectedly which relates to fast roaming state machine.
CSCvs72354	Cisco Catalyst 9130E AP: NSS reloads unexpectedly causing AP to be stuck in continuous loop.
CSCvs81190	AP crash is observed due to kernel panic triggered by Dynamic Frequency Selection (DFS) channel use.
CSCvs82874	Flex standalone with 11r Fallback FT Auth response code change to 53.
CSCvs88238	Client ARP and DHCP failures are observed after roaming among Cisco Wave 1 APs.
CSCvs89410	Cisco Aironet 3602 AP image corruption issue.
CSCvs93660	Frequent radio resets are observed during continuous roam (11r-OTA).

Caveat ID	Description
CSCvs95922	Cisco Catalyst 9120 AP: All clients are loosing connectivity on flex standalone.
CSCvt03401	AVC status is getting disabled while configuring service-policy input from DNA.
CSCvt03983	Intel clients are experiencing latency or drops when connected to Cisco Catalyst 9120 APs.
CSCvt04454	Cisco Catalyst 9120 AP: Flex connected to standalone; clients are loosing data.
CSCvt04710	Cisco Aironet 3700 AP: FlexConnect deauth status code is changed from 28 to 53 if 11r Pairwise Master Key (PMK) is not present.
CSCvt08586	Flex connected mode: Incorrect PMK ID causes delay in client association (Local Switch, Central Auth).
CSCvt09218	Flex connected mode: After continuous roam, client takes a longer time to reconnect.
CSCvt16983	Cisco Aironet 2700 AP: In flex standalone mode, the AP send identity request only once; need to send more.
CSCvt22353	Cisco Aironet 2800/3800/4800/1560 APs are not transmitting data frames over the air.
CSCvt26140	Clients cannot connect to Cisco Wave 1 APs with dot1x-sha256 received assoc-resp 20.
CSCvt37863	Rate limiting is not working for downstream traffic when ACL is pushed from ISE.
CSCvt38486	EAP-PEAP flex authentication fails occasionally because of low eap-timeout.
CSCvt40272	Clients connected to 2 different autonomous APs with ISE VLAN override cannot ping in 5GHz radio.
CSCvt44004	Cisco Aironet 2800 AP: Dual-Band (XOR) radio does not beacon after few iterations of moving from AUTO to 5G.
CSCvt53819	CPU exceeds 90 % with high volume traffic.
CSCvt68068	Cisco Wave 1 AP reports itself as a threat and logs \"AP Impersonation\" alerts.
CSCvt73463	Cisco Aironet 1800 AP unexpectedly reloads.
CSCvt75359	Cisco Wave 1 APs are not sending deauth rc 7 after rx frame from non assoc client.

Caveat ID	Description
CSCvt81606	Cisco Aironet 1832 AP kernel panic crash.
CSCvt84649	Cisco Aironet 2700 and 3800 APs are dropping ARP_REPLY packets.
CSCvt92754	Cisco Aironet 1532 AP: Ethernet interface is loosing packets.
CSCvu44330	Memory leak is observed under process SACRcvWQWrk2 when Smart Licensing is enabled.
CSCvu49805	Cisco Catalyst 9115AXI AP reloads unexpectedly with a kernel panic.
CSCvu78679	Cisco Aironet 2800 AP is dropping from the controller.
CSCvq81315	Cisco Aironet 2700 AP PCI0 reloads unexpectedly when Cisco CleanAir is enabled.
CSCvq98797	Traceroute fails: /bin/sh: /usr/bin/traceroute: not found.
CSCvr11240	Cisco Aironet 1815T AP is leaking client MAC from LAN3 to WAN port.
CSCvr33340	Wave 2 APs in FlexConnect mode are sending Auth Request to AAA without Local Auth Enabled.
CSCvr36185	Cisco Aironet 2800 APs are using 802.11n rates with WPA+TKIP only WLAN.
CSCvr36693	WLC 8540 OID returns small number than actual traffic size.
CSCvr39587	MAPs failing mesh_sec_auth and excluding Parent upon RAP failure.
CSCvr50653	Cisco Aironet 1562 AP in UWGB mode is unable to associate when powered up outside wireless coverage area.
CSCvr61717	WGB wired client is not getting IP when associating to Cisco Catalyst 9130 AP.
CSCvs05669	Clients connected to same SSID using different autonomous Cisco 2702 APs can not ping each other.
CSCvs09716	Cisco AP is not handling EXPIRE_MIC_PAYLOAD message.
CSCvs14548	Trustpoint configuration fails on Wave 2 APs in WGB.

Caveat ID	Description
CSCvs29874	802.11v Directed Multicast Service (DMS) is not shown as supported within beacon of Cisco Aironet 1852 AP.
CSCvs40887	Cisco Aironet 4800/3800/2800/1562 APs are stuck in "BootROM: Image checksum verification FAILED".
CSCvs50731	Cisco Catalyst 9130I and Cisco Aironet 1852 APs \"{watchdogd} Process syslogd gone for 60s\" & \" can't open '3410/maps'\".
CSCvs67811	Cisco APs acting as MAPs are not able to see RAPs.
CSCvs71672	Cisco AP fails to attach the VLAN tag when client user ID changes from central to local switching.
CSCvs81424	Cisco IW3702 AP: Samsung S10 client fails to associate on flex:local auth+local switch in 11r security.
CSCvs89401	Cisco Wave 2 AP beacons disabled SSID.
CSCvt01409	Dual-band static channel configuration switches to DCA after AP rejoin.
CSCvt06414	Cisco Catalyst 9130 AP: Kernel panic at cisco_wlan_crypto_decap.
CSCvt10962	Clients cannot connect to Cisco Aironet 1800 AP with 2.4 GHz with hidden SSID.
CSCvt15152	Cisco Aironet 4800 APs stopped supporting European weather band 5600-5650MHz- channels 120,124, and 128.
CSCvt17006	Cisco Aironet 1850AP: Clients are unable to connect to the AP.
CSCvt28616	Flexconnect reap count for current users not getting decremented causing new Wi-Fi client disconnect.
CSCvt53637	EWC conversion fails for Cisco Catalyst 9115AX AP with -T domain.
CSCvt55612	Cisco Catalyst 9120 power is lower than Cisco Aironet 2800/3800 APs with CCK rates disabled(2.4GHz).
CSCvt64308	Cisco OfficeExtend access point (OEAP) configuration doesn't get saved to AP flash.

Caveat ID	Description
CSCvt87401	Cisco Catalyst 9120 AP is not applying trust-dscp-upstream and CAPWAP traffic marked with UP to DSCP.
CSCvt87904	2.4GHz throughput does not change based on the number of streams.
CSCvt89989	Mesh AP: With ACL blocks ping to gateway, AP can't join controller if it doesn't complete within 45sec.
CSCvu03384	Cisco Wave 2 APs silver UP 00 to DSCP upstream mapping not capped by bronze profile.
CSCvu24770	Various models of Android 10 devices fail to associate.
CSCvu25264	AIR-AP2802I-H-K9 WCPd crash: AP is failing to decode discovery response and reboot with flash core.

Troubleshooting

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

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

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

Related Documentation

Information about Cisco IOS XE 16 is available at:

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

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

Cisco Validated Designs documents are available at:

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

Cisco Embedded Wireless Controller on Catalyst Access Points

For support information, see the following documents:

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

Installation guides for Catalyst Access Points are available at:

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

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

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

Wireless Products Comparison

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

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

- Product Approval Status:

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

- Wireless LAN Compliance Lookup:

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

Cisco Mobility Services Engine

Cisco Mobility Services Engine Documentation

Cisco Connected Mobile Experiences

Cisco Connected Mobile Experiences Documentation

Cisco DNA Center

Cisco DNA Center Documentation

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

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