Release Notes for Cisco Embedded Wireless Controller on Catalyst Access Points, Cisco IOS XE Dublin 17.11.x

First Published: 2023-03-28

Last Modified: 2023-03-26

Release Notes for Cisco Embedded Wireless Controller on Catalyst Access Points, Cisco IOS XE Dublin 17.11.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 Embedded Wireless Controller on Catalyst Access Points, Cisco IOS XE Dublin 17.11.1

Table 1: New and Modified Software Features

Feature Name	Description and Documentation Link
Background Scanning and MAP Fast Ancestor Find Mode	The Background Scanning and MAP Fast Ancestor Find Mode feature updates the child MAPs about their neighbors across all the channels. This feature also helps child MAPs to switch to a neighbor of any channel, and use that neighbor as the next parent for uplink. Background scanning allows MAPs to save time during the scan-and-seek phase while looking for a new parent. The following command is introduced: • **map-fast-ancestor-find** For more information, see the chapter Mesh Access Points.
Built-in Captive Portal Improvements	This release introduces support for special characters in the login portal banner title and banner text. The number of characters supported on the banner text has been doubled to 400. The following command is introduced: • **exec-character-bits** For more information, see the chapter Web-Based Authentication.
Convert Redundant 2.4-GHz Radios to Monitor Mode	From this release, you can select the redundant dual-band radios in a network to operate in monitor only mode. For more information, see the chapter Cisco Flexible Radio Assignment.
Jumbo Frame Support for RADIUS Packets	This release supports higher RADIUS packet fragmentation. The fragmentation size is increased to 9000 bytes. For more information, see the chapter Multiple Authentications for a Client.
Multiauthentication Combination of 802.1X and Local Web Authentication	This feature supports the merging of applied policies during the multiauthentication of 802.1X or MAC Authentication Bypass and Local Web Authentication. The following command is introduced: • **consent activation-mode merge** For more information, see the chapter Security.
New AAA Command	A new command is introduced to display brief information about AAA servers: • **show aaa server brief** For more information, see the Command Reference guide.

Feature Name	Description and Documentation Link
Reload Reason History	The Reload Reason History feature tracks the controller reload reason. Using the **show version** command and Network Configuration Protocol (NETCONF), you can view the reload reason history, which is useful for troubleshooting and serviceability.
RFID Hardening	The **show wireless rfid detail** command has been enhanced to display information about the neighbouring APs.
Secure Data Wipe	This feature allows you to securely erase files from the file system of Cisco Access Points. For more information, see the chapter Secure Data Wipe.
User-Configurable Ethernet Port LEDs	In this release, the Ethernet port LEDs in APs are enabled or disabled (switched ON or OFF) as per the system LED. For example, if the system LED is ON, the Ethernet LED will also be ON. For more information, see the chapter LED States for Access Points.
RAP Ethernet Daisy Chain with WSTP	RAP Ethernet Daisy Chain feature is enhanced in this release. WSTP hello message is used for root port detection to support flexible topology. A dedicated command is introduced to enable this feature: **rap-eth-daisychain**. The following command is introduced to configure primary ETH port: **ap name mesh backhaul ethernet**.
Wireless Client Latency Statistics	From this release onwards, the wireless client latency statistics allow you to view a client's statistics using the client's MAC address. The following command is introduced: • **show wireless client mac-address stats latency**

Table 2: New and Modified GUI Features

Feature Name	GUI Path
Convert Redundant 2.4-GHz Radios to Monitor Mode	• **Configuration** > **Radio Configurations** > **RRM** > **FRA**
Background Scanning and MAP Fast Ancestor Find Mode	• **Configuration** > **Wireless** > **Mesh** > **Profiles**
User-Configurable Ethernet Port LEDs	• **Configuration** >**Wireless** > **Access Points**

Interactive Help

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

You can start the interactive help in the following ways:

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

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

The following features have an associated interactive help:

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

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

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

Supported Cisco Access Point Platforms

The following Cisco access points are supported in the Cisco Embedded Wireless Controller on Catalyst Access Points network. Note that the APs listed as primary APs can also function as subordinate APs.

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

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

Table 4: Image Types and Supported APs in Cisco Embedded Wireless Controller on Catalyst Access Points

Image Type	Supported APs
ap1g4	Cisco Aironet 1810 Series Cisco Aironet 1830 Series Cisco Aironet 1850 Series
ap1g5	Cisco Aironet 1815i Cisco Aironet 1815w Cisco Aironet 1540 Series Cisco Aironet 1850 Series
ap1g6	Cisco Catalyst 9117 Series

Image Type	Supported APs
ap1g6a	Cisco Catalyst 9130 Cisco Catalyst 9124AXE/I/D
ap1g7	Cisco Catalyst 9115 Series Cisco Catalyst 9120 Series
ap1g8	Cisco Catalyst 9105 Series
ap3g3	Cisco Aironet 2800 Series Cisco Aironet 3800 Series Cisco Aironet 4800 Series Cisco Aironet 1560 Series Cisco Catalyst Industrial Wireless 6300 Heavy Duty Series Access Points Cisco 6300 Series Embedded Services Access Points

Maximum APs and Clients Supported

Table 5: Scale Supported in Cisco EWC Network

Primary AP Model	Maximum APs Supported	Maximum Clients Supported
Cisco Catalyst 9105 AWI	50	1000
Cisco Catalyst 9115 Series	50	1000
Cisco Catalyst 9117 Series	50	1000
Cisco Catalyst 9120 Series	100	2000
Cisco Catalyst 9124AXE/I/D	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 6: Compatibility Information

Cisco Embedded Wireless Controller on Catalyst Access Points	Cisco ISE	Cisco CMX	Cisco DNA Center
Dublin 17.11.x	3.0 2.7 2.6 2.4 2.3	10.6.3 10.6.2 10.6 10.5.1	See Cisco DNA Center Compatibility Information

Supported Browsers and Operating Systems for Web UI

Note The following list of Supported Browsers and Operating Systems is not comprehensive at the time of writing this document and the behavior of various browser for accessing the GUI of the EWC is as listed below.

Table 7: Supported Browsers and Operating Systems

Browser	Version	Operating System	Status	Workaround
Google Chrome	77.0.3865.120	macOS Mojave Version 10.14.6	Works	Proceed through the browser warning.
Safari	13.0.2 (14608.2.40.1.3)	macOS Mojave Version 10.14.6	Works	Proceed through the browser warning.
Mozilla Firefox	69.0.1	macOS Mojave Version 10.14.6	Works only if exception is added.	Set the exception.
Mozilla Firefox	69.0.3	macOS Mojave Version 10.14.6	Works only if exception is added.	Set the exception.
Google Chrome	77.0.3865.90	Windows 10 Version 1903 (OS Build 18362.267)	Works	Proceed through the browser warning.
Microsoft Edge	44.18362.267.0	Windows 10 Version 1903 (OS Build 18362.267)	Works	Proceed through the browser warning.
Mozilla Firefox	68.0.2	Windows 10 Version 1903 (OS Build 18362.267)	Works	Proceed through the browser warning.
Mozilla Firefox	69.0.3	Windows 10 Version 1903 (OS Build 18362.267)	Works only if exception is added.	Set the exception.

Browser	Version	Operating System	Status	Workaround
Google Chrome	78.0.3904.108	macOS Catalina 10.15.1	Does not work	NA

Before You Upgrade

The following Remote Procedure Call (RPCs) should be used for Cisco Catalyst 9800 Series Wireless Controller and Cisco Embedded Wireless Controller:

- Cisco Catalyst 9800 Series Wireless Controller: Use **ewlc-wncd-stats** within *Cisco-IOS-XE-wireless-ap-global-oper*.
- Cisco Embedded Wireless Controller: Use **ewlc-wncd-stats** within *Cisco-IOS-XE-wireless-access-point-oper*.

Upgrade Path to Cisco IOS XE Dublin 17.11.x

Table 8: Upgrade Path to Cisco IOS XE Dublin 17.11.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 17.11.x.
16.11.x	—	Upgrade first to 16.12.5 or 17.3.x and then to 17.11.x.
16.12.x	Upgrade first to 17.3.5 or 17.6.x or later and then to 17.11.x.	Upgrade first to 17.3.5 or 17.6.x or later and then to 17.11.x.
17.1.x	Upgrade first to 17.3.5 or 17.6.x or later and then to 17.11.x.	Upgrade first to 17.3.5 or 17.6.x or later and then to 17.11.x.
17.2.x	Upgrade first to 17.3.5 or 17.6.x or later and then to 17.11.x.	Upgrade first to 17.3.5 or 17.6.x or later and then to 17.11.x.
17.3.1 to 17.3.4	Upgrade first to 17.3.5 or 17.6.x or later and then to 17.11.x.	Upgrade first to 17.3.5 or 17.6.x or later and then to 17.11.x.
17.3.4c or later	Upgrade directly to 17.11.x.	Upgrade directly to 17.11.x.
17.4.x	Upgrade first to 17.6.x and then to 17.11.x.	Upgrade first to 17.6.x and then to 17.11.x.
17.5.x	Upgrade first to 17.6.x and then to 17.11.x.	Upgrade first to 17.6.x and then to 17.11.x.
17.6.x	Upgrade directly to 17.11.x.	Upgrade directly to 17.11.x.

Current Software	Upgrade Path for Deployments with 9130 or 9124	Upgrade Path for Deployments Without 9130 or 9124
17.7.x	Upgrade directly to 17.11.x.	Upgrade directly to 17.11.x.
17.8.x	Upgrade directly to 17.11.x.	Upgrade directly to 17.11.x.
17.9.x	Upgrade directly to 17.11.x.	Upgrade directly to 17.11.x.
17.10.x	Upgrade directly to 17.11.x.	Upgrade directly to 17.11.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 17.11.x software for Cisco Embedded Wireless Controller on Catalyst Access Points.

Choose the appropriate AP software based on the following:

- Cisco Embedded Wireless Controller on Catalyst Access Points software to be used for converting the AP from an unified wireless network CAPWAP lightweight AP to a Cisco Embedded Wireless Controller on Catalyst Access Points-capable AP (primary AP)
- AP software image bundle to be used either for upgrading the Cisco Embedded Wireless Controller on Catalyst Access Points software on the primary AP or for updating the software on the subordinate APs or both

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

Table 9: Cisco Embedded Wireless Controller on Catalyst Access Points Software

Primary AP	AP Software for Conversion from CAPWAP to Cisco EWC	AP Software Image Bundle for Upgrade	AP Software in the Bundle
Cisco Catalyst 9115 Series	C9800-AP-universalk9.17.11.01.zip	C9800-AP-universalk9.17.11.01.zip	ap1g7
Cisco Catalyst 9117 Series	C9800-AP-universalk9.17.11.01.zip	C9800-AP-universalk9.17.11.01.zip	ap1g6
Cisco Catalyst 9120 Series	C9800-AP-universalk9.17.11.01.zip	C9800-AP-universalk9.17.11.01.zip	ap1g7

Primary AP	AP Software for Conversion from CAPWAP to Cisco EWC	AP Software Image Bundle for Upgrade	AP Software in the Bundle
Cisco Catalyst 9124AXE/I/D	C9800-AP-universalk9.17.11.01.zip	C9800-AP-universalk9.17.11.01.zip	ap1g6a
Cisco Catalyst 9130	C9800-AP-universalk9.17.11.01.zip	C9800-AP-universalk9.17.11.01.zip	ap1g6a

Supported Access Point Channels and Maximum Power Settings

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

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

Guidelines and Restrictions

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

Embedded Wireless Controller SNMP configuration is supported in DNAC.

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

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

Interoperability with Clients

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

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

Table 10: Test Configuration for Interoperability

Hardware or Software Parameter	Hardware or Software Type
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
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.

Caveats

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

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

Cisco Bug Search Tool

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

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

Open Caveats for Cisco IOS XE 17.11.1

Identifier	Headline
CSCwe31030	Cisco Catalyst 9105AXW AP: Kernel panic crash is observed.
CSCwd78616	Cisco Catalyst AP9115 Tx power high and abnormal DCA channel assignment due to no neighbors.
CSCwd90742	Cisco Catalyst 9120AX AP: Kernel crash is observed.
CSCwe38431	Controller is remarking SIP packets from CS3 to CS0 in upstream/downstream when voice cac is configured.
CSCwd96484	Controller is relaoding unexpectedly and regularly generates "wncd" core files.
CSCwe45894	AP is not forwarding IGMPv3 query to wireless clients.
CSCwe55390	Cisco Aironet 3802AP buffering UP6/voice traffic~500ms after Spectralinkphone roam causing audioissues.
CSCwe18012	Crash is observed on standby controller while saving tbl QoS table to standby.
CSCwe32005	Cisco Catalyst 9130 AP: Packet loss is observed on Digital Signage device.
CSCwe49267	Controller is not sending GTK M5 packet to 8821 after FT roaming between wncds.
CSCwe44216	Cisco AP reloads unexpectedly due to kernel panic.
CSCwe43294	Cisco Catalyst 9105AXW and Cisco Aironet 1815W: Flex RLAN AP does not apply VLAN in the Ethernet port after AAA VLAN override.
CSCwe45300	Cisco Catalyst 9120 AP: Sending Msg:2 in mode:2 to hostapd failed.
CSCwe30473	Radio firmware reloads unexpectedly due to a frozen RC queue.

Identifier	Headline
CSCwe44991	Cisco Catalyst 9105AX AP: Kernel crash is observed.
CSCwe11747	Cisco Catalyst AX APs are decoding EAP request ID incorrectly.
CSCwe22861	AID leak is observed in Flex Cisco Wave 2 APs.
CSCwe54482	Cisco Catalyst 9120 AP is dropping DHCP offer in click. Not forwarding to wireless interface.
CSCwe54575	Dell Latitude 5531 Laptops (Wi-Fi 6) are not able to connect.
CSCwe45970	Cisco Catalyst 9105 AP is stuck in UBOOT.
CSCwe61597	One of the WNCD is stuck in 100% high CPU.
CSCwe62694	EVENTLIB-3-CPUHOG Traceback is observed.
CSCwe50033	Cisco Catalyst 9120AX AP: Clients continuously disconnecting with more than 10 clients using MS TEAMS.

Resolved Caveats for Cisco IOS XE 17.11.1

Identifier	Headline
CSCwb52755	Fast Transition capable Apple and Android clients are unable to authenticate with IPSK profile.
CSCwb69531	Controller initiates EAPOL reties for the client in RUN state.
CSCwb84621	The PSK keys are getting changed while doing edit on pure WPA3 SAE WLAN leading to client connectivty faliure.
CSCwc01644	COS APs are using native VLAN instead of the VLAN specified in the policy profile.
CSCwc04197	Secondary controller crash is observed during redundancy switchover.
CSCwc05366	Wireless AAA Dyn VLAN Assignment - wir clients cannot reach each other
CSCwc14629	Controller GUI is taking long time to show initial page due to http request wirelessDeviceSummary.
CSCwc15533	Continuous wncmgrd CPUHOG traceback with scale Flexible NetFlow (FNF) mapping to policy profile results in 100% wncd utilization.
CSCwc15944	Multicast data is not sent to clients; some APs are unable to join.
CSCwc22468	Client traffic fails when client roams between access points with a transition between dot11r and dot11i.
CSCwc26105	High Availability split brain is observed due to multiple secondary addresses in the interface.

Identifier	Headline
CSCwc32226	Zebra RF guns gets deleted from controller randomly due to reason: CO_CLIENT_DELETE_REASON_ZONE_CHANGE.
CSCwc36910	cEdge device pushes wrong (typo) syntax as "config wlan broadcase-ssid disable 2".
CSCwc42784	Client fails to connect when protocol based QoS is configured.
CSCwc55982	Observed stale entry in the output of the show wireless device tracking database ip command after client deletion.
CSCwc57227	Controller experiences an unexpected reset resulting in a system report containing a wncd core file.
CSCwc59518	Cisco Catalyst 9800-80 Series Controller crashes with reason critical process wncd fault.
CSCwd08678	The "Re-Authentication Timeout" is seen stuck as "Timer not running" and the client remains in RUN state after session timeout.
CSCwd16409	User-agent details needs to be truncated to string length 234 in WSA to prevent vstring corruption.
CSCwd17349	Active chassis might get stuck during the SSO failover.
CSCwb19227	Interim update is not sent to AAA during client reassociation/roam in GA.
CSCwb37457	Standby controller crashes when controller is configured in RMI+RP HA mode with wired guest feature.
CSCwb43548	Disable ip proxy-arp command by default.
CSCwb47040	Controller is not updating RFID location properly.
CSCwb58100	Controller is unable to map SSID with spaces in it on an attribute list.
CSCwb64761	Controller is discarding location updates from RFID tags.
CSCwb66603	CAPWAPAC_SMGR_TRACE_MESSAGE_AP_JOIN_DISJOIN does not have detail information about AP-NAME.
CSCwb67450	The **show process cpu platform sorted** command is needed in **show tech wireless** command output.
CSCwb78191	AAA VLAN override is not taken when iPSK authentication and anchor WLAN.
CSCwb91373	Cisco DNA Centre-Assurance-Duplicate Events: AP is connected to controller and the CAPWAP channel is up
CSCwb93513	Stale client entries are not deleted and is stuck on device-tracking database.
CSCwc26819	Controller does not send LLC or XID spoofed frames after a mobility event.
CSCwc28408	Controller crashes intermittently due to wncd critical process failure.

Identifier	Headline
CSCwc31759	Adding policy tag is not allowed in WLAN page even though it meets 32 character.
CSCwc36125	Radio Resource Management (RRM) startup mode gets triggered on every reboot as the controller does not keep track of the last state.
CSCwc38828	Invalid TDL pointers cause wncd crash.
CSCwc41358	MAC filtering: WLAN profile column displays the WLAN name + description.
CSCwc45018	Unable to add RADIUS server group if server name includes special character '&'.
CSCwc51857	Controller GUI is displaying 802.1x with a lowercase 'x' instead of 802.1X with a capital 'X'.
CSCwc57836	Restore configuration by HTTP mode does not work in EWC.
CSCwc62824	Controller is not sending LLC or XID spoofed frames after a mobility event.
CSCwc72047	Access Points operate in disabled RF profile channels.
CSCwc76905	Switch Integrated Security Features (SISF) crash is observed when handling the DHCP messages.
CSCwc86955	Dual DFS stats on AP do not match controller information.
CSCwd00711	WPA3, OWE transition enabled: Non-WPA3 clients are getting network access in webauth-pending state.
CSCwd00979	The output of the **show wlan all** command has incorrect WLAN radio policy information.
CSCwd06018	802.11r re-auth failed due to invalid Pairwise Master Key ID (PMKID) while doing inter-WNCD roaming.

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:

Installation guides for Catalyst Access Points are available at:

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

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

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

Wireless Products Comparison

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

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

- Product Approval Status:

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

- Wireless LAN Compliance Lookup:

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

Cisco Connected Mobile Experiences

Cisco Connected Mobile Experiences Documentation

Cisco DNA Center

Cisco DNA Center Documentation

Communications, Services, and Additional Information

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

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.

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.