Release Notes for Cisco Catalyst 9800 Series Wireless Controller, Cisco IOS XE Cupertino 17.9.x

First Published: 2022-08-01

Last Modified: 2024-03-19

Release Notes for Cisco Catalyst 9800 Series Wireless Controller, Cisco IOS XE Cupertino 17.9.x

Introduction to Cisco Catalyst 9800 Series Wireless Controllers

The Cisco Catalyst 9800 Series Wireless Controllers comprise next-generation wireless controllers (referred to as *controller* in this document) built for intent-based networking. The Catalyst 9800 Series Wireless Controllers are Cisco IOS XE based and integrate the radio frequency (RF) capabilities from Cisco Aironet with the intent-based networking capabilities of Cisco IOS XE to create a best-in-class wireless experience for your organization.

The Catalyst 9800 controllers are enterprise ready to power your business-critical operations and transform end-customer experiences:

- The controllers come with high availability and seamless software updates that are enabled by hot and cold patching. This keeps your clients and services up and running always, both during planned and unplanned events.
- The controllers come with built-in security, including secure boot, run-time defenses, image signing, integrity verification, and hardware authenticity.
- The controllers can be deployed anywhere to enable wireless connectivity, for example, on an on-premise device, on cloud (public or private), or embedded on a Cisco Catalyst switch (for SDA deployments) or a Cisco Catalyst access point (AP).
- The controllers can be managed using Cisco Cisco Catalyst Center, programmability interfaces, for example, NETCONF and YANG, or web-based GUI or CLI.
- The controllers are built on a modular operating system. Open and programmable APIs enable the automation of your day zero to day *n* network operations. Model-driven streaming telemetry provides deep insights into your network and client health.

The Catalyst 9800 Series controllers are available in multiple form factors to cater to your deployment options:

- Catalyst 9800 Series Wireless Controller Appliance
- Catalyst 9800 Series Wireless Controller for Cloud
- Catalyst 9800 Embedded Wireless Controller for a Cisco switch

Note All the Cisco IOS-XE programmability-related topics on the Cisco Catalyst 9800 controllers are supported by DevNet, either through community-based support or through DevNet developer support. For more information, go to https://developer.cisco.com.

What's New in Cisco IOS XE Cupertino 17.9.5

Table 1: New and Modified Software Features

Feature Name	Description and Documentation Link
Cloud Monitoring for Catalyst Controllers	The Cloud Monitoring for Catalyst Controllers feature helps to monitor Wireless Controllers using the Meraki dashboard. Currently, this feature is in a limited customer beta and is not supported by Cisco TAC. For more information on this feature, see Cloud Monitoring for Catalyst. For further help, contact the following mailerlist: c9800-dashboard-monitoring@external.cisco.com

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

Feature Name	Description and Documentation Link

	From Cisco IOS XE 17.9.5 onwards, the following changes have been introduced for trustpoints:
	• Trustpoint names for existing SUDI certificates
	If your device supports Cisco Manufacturing CA III certificate and is not disabled, the trustpoint names are as follows:
	• For *Cisco Manufacturing CA III* certificate, the trustpoint name has changed from CISCO_IDEVID_SUDI to CISCO_IDEVID_CMCA3_SUDI
	• For *Cisco Manufacturing CA SHA2* certificate, the trustpoint name has changed from CISCO_IDEVID_SUDI_LEGACY to CISCO_IDEVID_CMCA2_SUDI
	If your device does not support Cisco Manufacturing CA III certificate or if the certificate is disabled using **no platform sudi cmca3** command, the trustpoint names are as follows:
	• For *Cisco Manufacturing CA SHA2* certificate, the trustpoint name has changed from CISCO_IDEVID_SUDI to CISCO_IDEVID_CMCA2_SUDI
	• For *Cisco Manufacturing CA* certificate, the trustpoint name has changed from CISCO_IDEVID_SUDI_LEGACY to CISCO_IDEVID_CMCA_SUDI
	• Hardware SUDI certificates
	• If your device supports *High Assurance SUDI CA* certificate, this certificate is loaded under CISCO_IDEVID_SUDI trustpoint.
	• If your device does not support *High Assurance SUDI CA* certificate, *ACT2 SUDI CA* certificate is loaded under CISCO_IDEVID_SUDI trustpoint.
	• **show wireless management trustpoint** command output
	If Cisco Catalyst 9300 Series Switch is used with a Cisco Catalyst 9800 Series Wireless Controller for wireless deployments, the trustpoint name in the output of **show wireless management trustpoint** command is updated to the modified trustpoint name as mentioned previously.
	The following example shows a sample output of **show wireless management trustpoint** command. Note that if your device does not support Cisco Manufacturing CA III certificate or if the certificate is disabled, the Trustpoint Name in the following output displays CISCO_IDEVID_CMCA2_SUDI.
	`Device# show wireless management trustpoint`
	`Trustpoint Name : CISCO_IDEVID_CMCA3_SUDI`
	`Certificate Info : Available`

Feature Name	Description and Documentation Link
	Certificate Type : MIC Certificate Hash : <SHA1 - hash> Private key Info : Available FIPS suitability : Not Applicable • **show ip http server status** command output If you configure the trustpoint for the HTTP server as CISCO_IDEVID_SUDI, the output of **show ip http server status** command displays the operating trustpoint along with the configured trustpoint. The following example shows a sample output of **show ip http server status** command with both the configured and the operating trustpoint names. Note that if your device does not support Cisco Manufacturing CA III certificate or if the certificate is disabled, the operating trustpoint in the following output displays CISCO_IDEVID_CMCA2_SUDI. Device# show ip http server status … HTTP secure server trustpoint: CISCO_IDEVID_SUDI HTTP secure server operating trustpoint: CISCO_IDEVID_CMCA3_SUDI

What's New in Cisco IOS XE Cupertino 17.9.4a

There are no new features in this release. This release provides a fix for CSCwh87343: Cisco IOS XE Software Web UI Privilege Escalation Vulnerability. For more information, see Security Advisory: cisco-sa-iosxe-webui-privesc-j22SaA4z.

What's New in Cisco IOS XE Cupertino 17.9.4

Table 2: New and Modified Software Features

Feature Name	Description and Documentation Link
ROW Support for UAE Country	From this release, ROW domain country code United Arab Emirates (AE) is supported on Cisco Catalyst IW9167E Heavy Duty Access Points.

Feature Name	Description and Documentation Link
Product Analytics	This feature allows for the collection of non-personal usage device systems information for Cisco products, which helps in continuous product improvements. This feature is supported on the Cisco Catalyst 9800 Series Wireless Controllers (9800-80, 9800-40, 9800-L, and 9800-CL). You can use the the **pae** command to enable or disable this feature. The following commands are introduced as part of this feature: • **pae** • **show product-analytics kpi** • **show product-analytics report** • **show product-analytics stats** **Note** Turning off Smart Licensing Device Systems Information does not impact other Systems Information collection including from Cisco Catalyst Center or vManage. **Important**: Cisco is constantly striving to advance our products and services. Knowing how you use our products is key to accomplishing this goal. To that end, Cisco will collect device and licensing Systems Information through Cisco Smart Software Manager (CSSM) for product and customer experience improvement, analytics, and adoption. Cisco processes your data in accordance with the General Terms and Conditions, the Cisco Privacy Statement and any other applicable agreement with Cisco. To modify your organization's preferences for device and licensing systems information, use the **pae**command. See Cisco Catalyst 9800 Series Wireless Controller Command Reference → **pae**. Additional information on this feature can be found here .

What's New in Cisco IOS XE Cupertino 17.9.3

Table 3: New and Modified Software Features

Feature Name	Description and Documentation Link
Cisco Catalyst IW9167E Heavy Duty Access Point	Cisco Catalyst IW9167E Heavy Duty Access Point is supported from this release and can operate as a Wi-Fi 6 AP or Cisco Ultra-Reliable Wireless Backhaul.
Site Load Balancing	This feature allows you to specify a site load for better load balancing. For more information, see the Chapter Enhanced Site Tag-Based Load Balancing.

Feature Name	Description and Documentation Link
Support for KVM/SUSE version 15 SP3 with Cisco Catalyst 9800-CL in Private Cloud	Limited support to SDA Wireless deployments for Cisco Catalyst 9800-CL running on KVM/SUSE version 15 SP3.
Wave 1 Access Points	Support for the following Wave 1 APs are reintroduced from this release. • **Cisco Aironet 1570 Series Access Point** • **Cisco Aironet 1700 Series Access Point** • **Cisco Aironet 2700 Series Access Point** • **Cisco Aironet 3700 Series Access Point** **Note** • Support for these APs does not extend beyond the normal product lifecycle support. Refer to the individual End of Support bulletins. • Feature support is on parity with 17.3.x release. Features introduced in 17.4.1 or later are not supported on these APs in 17.9.3 release. • You can migrate directly to 17.9.3 from 17.3.x, where x=4c or above. For more information on support for Wave 1 APs, see the FAQ.

What's New in Cisco IOS XE Cupertino 17.9.2

Table 4: New and Modified Software Features

Feature Name	Description and Documentation Link
AP Fallback to Controllers Using AP Priming Profile	This feature helps to configure primary, secondary, and tertiary controllers for a group of APs matching regular expression (regex) or for an individual AP using priming profiles. The following commands are introduced: • **primary (ap prime)** • **secondary (ap prime)** • **tertiary (ap prime)** • **priming-override** • **profile (prime-filter)** • **wireless profile ap priming** • **show ap filters active type priming** • **show ap filters all type priming** • **show wireless profile ap priming all** • **show wireless profile ap priming summary** For more information, see the Chapter AP Fallback to Controllers Using AP Priming Profile.
Country Compliance Support for Cisco Catalyst 9136 Series Access Points and Cisco Catalyst 916x Series Access Points	An additional 75 countries are supported in Cisco Catalyst 916x Series Access Points and Cisco Catalyst 9136 Series Access Points. For more information about the list of countries that are supported, see the Chapter Regulatory Compliance Domain.

Feature Name	Description and Documentation Link
IPv6 Address Tracking for Wireless Clients	Until Cisco IOS XE 17.9.1, the controller supported a maximum of eight IPv6 addresses per wireless client. After eight IPv6 addresses were learnt for a wireless client, the controller dropped that wireless client's data traffic coming with new IPv6 source addresses. However, in Cisco IOS XE 17.9.2, the controller allows data traffic of the wireless clients coming with new IPv6 source addresses even after eight addresses have been learnt for respective wireless clients. The controller continues to learn new IPv6 addresses of the wireless clients from the wireless clients' control traffic (IPv6 NS/NA and DHCPv6), but keeps track of only a maximum of eight addresses (the latest) per wireless client. **Note** In Cisco IOS XE 17.9.2, because the controller allows IPv6 traffic without address tracking beyond the eight IPv6 address limit, some of the features such as, User Defined Network, iPSK Peer-to-Peer Blocking, Management over Wireless, Neighbor Discovery Suppression, IP Theft Detection, and so on, may not work for the wireless clients using more than eight addresses. You can disable the new behavior by enabling the IP Source Guard feature when loading the Cisco IOS XE 17.9.2 images. The following command is supported: **wireless ipv6 nd ns-forward** For more information, see the Chapter IPv6 Client IP Address Learning.
Support for Cisco Catalyst 9162I Series Wi-Fi 6E Access Points	From Cisco IOS XE Cupertino 17.9.2, Cisco Catalyst 9162I Series Wi-Fi 6E Access Points are supported.
Support for Terminal Doppler Weather Radar Channels 120, 124, 128 for -E Regulatory Domain	Terminal Doppler Weather Radar (TDWR) channels 120, 124, and 128 for the -E regulatory domain are supported in the following APs: • Cisco Catalyst 9124 Series Access Points • Cisco Catalyst 9130 Series Access Points
UNII-3 Band on ROW Regulatory Domain for UK Cisco Catalyst 9136I and Cisco Wireless 916xI Access Points	From Cisco IOS XE Cupertino 17.9.2, UNII-3 channels are enabled for the country code GB under the -ROW domain on the Cisco Catalyst 9136I and Cisco Wireless 916xI access points. The maximum Tx power on these non-Dynamic Frequency Selection (DFS) channels is 23dBm. This feature is enabled automatically after you upgrade to Cisco IOS XE Cupertino 17.9.2. Use the **show controllers dot11Radio** command to verify the channel list information after the upgrade.

Feature Name	Description and Documentation Link
Wi-Fi Protected Access 3 Simultaneous Authentication of Equals Hash-to-Element Support with Identity PSK	From Cisco IOS XE Cupertino 17.9.2, the iPSK passphrase is supported for SAE H2E authentication in local mode. During client SAE authentication, the Identity Preshared Key (iPSK) passphrase configured in the client authorization policy in the RADIUS server replaces the one in WLAN profile. Hence, the use of unique preshared keys for individuals is considered as a more secure and granular authentication scheme than using a common key for all the users in WLAN. If iPSK passphrase is not configured in the authorization policy, SAE H2E falls back to the passphrase in the WLAN profile. For more information, see the Chapter Wi-Fi Protected Access 3.
VMware vSphere vMotion Support	VMware vSphere vMotion is supported on the Cisco Catalyst 9800 Wireless Controller for Cloud. For more information, see https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-wireless-controllers-cloud/218438-verify-support-vmware-vsphere-vmotion-wi.html#anc6 and https://www.cisco.com/c/en/us/products/collateral/wireless/catalyst-9800-cl-wireless-controller-cloud/nb-06-cat9800-cl-wirel-cloud-dep-guide-cte-en.html.

MIBs

The following MIB is newly added or modified:

- CISCO-ENVMON-MIB

What's New in Cisco IOS XE Cupertino 17.9.1

Table 5: New and Modified Software Features

Feature Name	Description and Documentation Link
802.11r Fast Transition for SAE (FT-SAE) Authenticated Clients	From this release, the Fast Transition supports SAE-based Fast Roaming along with PMK caching. The following command is introduced: • **security wpa akm ft sae** For more information, see the chapter 802.11r BSS Fast Transition.

Feature Name	Description and Documentation Link
Access Points Survey Mode Support in Cisco Catalyst 9136 Series Access Points, Cisco Catalyst 9164 Series Wi-Fi 6E Access Points, and Cisco Catalyst 9166 Series Wi-Fi 6E Access Points	In this release, you can use the **ap-type survey** command to switch the AP to the survey mode. The AP GUI is also enhanced to support the survey mode. This feature is supported on Cisco Catalyst 9136 Series APs, Cisco Catalyst 9164 Series Wi-Fi 6E APs, and Cisco Catalyst 9166 Series Wi-Fi 6E APs. For more information, see the chapter Access Points Survey Mode.
Authentication and Accounting Support for Both Radius and TACACS+ Servers for Standby Unit in an SSO Pair	From this release, Authentication and Accounting is supported on RADIUS and TACACS+ servers for standby HA unit using RMI interface: • RADIUS Accounting • TACACS+ Authentication • TACACS+ Accounting For more information, see the chapter Redundancy Management Interface.
BLE Concurrent Scanning and Beaconing	From this release, BLE concurrent scanning and beaconing is supported on Cisco Catalyst Wi-Fi 6 APs in basic mode or Cisco IOx mode. The BLE radio on an AP can stop a scan for beacon transmission, and return to the scan after completing the beacon transmission. For more information, see the chapter Cisco Hyperlocation.
Chargeable User Identity in RADIUS Accounting	Chargeable User Identity (CUI) is a unique identifier for a client visiting a network. This attribute can be used as an alternative for the client's username as part of the authentication process. The following command is introduced: • **access-session wireless cui-enable** For more information, see the chapter RADIUS Accounting.
Cisco AI-Enhanced RRM Supports Wi-Fi 6E	From this release, the Cisco's AI-Enhanced RRM feature in Cisco DNA Center supports Wi-Fi 6E. For more information, see the chapter Radio Resource Management.

Feature Name	Description and Documentation Link
CleanAir Pro Scanning Support in 2.4-GHz and 5-GHz Bands	The CleanAir Pro Scanning feature monitors and reports the different categories of non-Wi-Fi interference in the 2.4-GHz and 5-GHz bands. The following commands are introduced: • **ap dot11 6ghz cleanair** • **ap dot11 cleanair alarm air-quality** • **ap dot11 cleanair alarm device cont-tx** • **ap dot11 cleanair alarm unclassified** For more information, see the chapter CleanAir.
Concurrent Radio Support for Workgroup Bridge Wireless Clients on Cisco Catalyst Access Points	From this release onwards, Workgroup Bridge supports one radio for uplink (backhaul) connectivity and another radio for serving wireless clients. This feature is supported on Cisco Catalyst 9105 APs, Cisco Catalyst 9115 APs, and Cisco Catalyst 9120 APs. The following commands are introduced on the AP console: • **configure ssid-profile ssid dtim-period** • **configure dot11Radio wlan add** • **configure dot11Radio wlan delete** • **configure dot11Radio channel** • **configure dot11Radio beacon-interval** • **configure radius address port** • **configure qos profile** • **configure ssid-profile ssid qos profile** For more information, see the chapter Workgroup Bridges.
Configuring mDNS Location-Based Filtering Using Location Group	From this release, the AP grouping for mDNS is extended to include AP locations. The following commands are introduced: • **wireless rule application mdns** • **group-method** For more information, see the chapter Multicast Domain Name System.

Feature Name	Description and Documentation Link
Configuring the AP Console	This feature allows you to configure the AP console from the controller. The following command is introduced: • **console** For more information, see the chapter Configuring the AP Console.
Flexible Radio Assignment Support in Cisco Catalyst 9166I Series Wi-Fi 6E Access Points	From this release onwards, the dual-band radio in Cisco Catalyst 9166I Series Wi-Fi 6E Access Points offers the ability to serve either in 5-GHz or 6-GHz band, as monitor or sniffer on the same AP. The following commands are introduced: • **ap fra 5-6ghz** • **ap fra 5-6ghz freeze** • **ap fra 5-6ghz interval** • **ap dot11 6ghz rf-profile** • **client-aware-fra** • **show ap fra 5-6ghz** For more information, see the chapter Cisco Flexible Radio Assignment.
High Availability Deployment for Application Centric Infrastructure (ACI) Network	This feature avoids interleaving traffic between the old and new active controller using the following functionalities: • Bringing down the Wireless Management Interface (WMI) faster. • Disabling fast switchover notifications. The following commands are introduced: • **no redun-management fast-switchover** • **redun-management garp-retransmit burst** • **no redun-management garp-retransmit initial** For more information, see the chapter High Availability.
Interim Accounting	From this release, the **no accounting-interim** command is introduced under the policy profile to disable interim accounting. For more information, see the chapter Interim Accounting.

Feature Name	Description and Documentation Link
Link Layer Discovery Protocol Support in Standby Controller	From this release, the Link Layer Discovery Protocol (LLDP) process is supported in both active and standby controllers. The following commands are introduced: • **lldp run** • **lldp holdtime** • **lldp reinit** • **lldp timer** • **lldp tlv-select** • **show lldp** • **show lldp neighbors** • **show lldp neighbors detail** • **show lldp errors** • **show lldp traffic** For more information, see the chapter Link Layer Discovery Protocol.
Logging Web UI-Based Configuration Changes in TACACS+ Server	This feature logs all the configuration changes made in the controller's UI. For more information, see the chapter Web UI Configuration Command Accounting in TACACS+ Server.
Management Mode Migration in Cisco Catalyst 916x Series Wi-Fi 6E Access Points (CW9164 and CW9166)	From this release onwards, in Cisco Catalyst 916x APs (CW9164 and CW9166) you can migrate management modes between DNA Management Mode (controller based) and Meraki Management Mode, depending on the requirement. The following commands are introduced: • **ap name management-mode meraki** • **clear ap meraki stats** • **show ap management-mode meraki capability summary** • **show ap management-mode meraki failure summary** • **show ap management-mode meraki change summary** For more information, see the chapter Management Mode Migration in Cisco Catalyst 916x Series Wi-Fi 6E Access Points.

Feature Name	Description and Documentation Link
Mesh Backhaul RRM Support	From this release onwards, RRM DCA runs on mesh backhaul in auto mode, when you configure the **wireless mesh backhaul rrm auto-dca** command. For APs that do not have dedicated (RHL) radios, DCA is triggered by running commands in privileged EXEC mode. Mesh RRM DCA runs in the background for RHL radio enabled APs. The following commands are introduced: • **ap dot11 rrm channel-update mesh** • **ap dot11 rrm channel-update mesh bridge-group** • **ap name dot11 rrm channel update mesh** • **show wireless mesh rrm dca status** • **wireless mesh backhaul rrm auto-dca** For more information, see the chapter Mesh Access Points.
Mutual Authentication for gRPC Telemetry	A new gRPC TLS profile that contains a pair of trustpoints was added to the telemetry configuration so that a client ID certificate can be specified for mutual authentication. This new profile can be used instead of the trustpoint containing the server CA certificate when configuring the receiver profile. The trustpoint containing the server CA certificate is now configured as part of the gRPC TLS profile. For more information, see the Programmability Configuration Guide.
Quality of Service Gaps and Fixes in Cisco Catalyst 9800 Series Wireless Controllers	This feature addresses the gaps in the existing metal policy implementation with reference to RFC 8325. With this enhancement, the existing hard-coded policy-maps and class-maps associated with each metal policy is modified as per RFC 8325, so that upstream and downstream ceiling is achieved. For more information, see the chapter Quality of Service.
Regulatory Domain Reduction	From Cisco IOS XE Cupertino 17.9.1, more countries are added to the Rest of the World (RoW) domain. For more information, see the chapter Regulatory Compliance Domain.
Rogue Detection Enhancements on Cisco Catalyst 9164 and 9166 Series Wi-Fi 6E Access Points	In this release, the rogue detection and containment functionality is enhanced to handle dual 5-GHz configuration on Cisco Catalyst 9164 Series Wi-Fi 6E APs and Cisco Catalyst 9166 Series Wi-Fi 6E APs.

Feature Name	Description and Documentation Link
Rogue Full Scale Quotas and Priorities	The Rogue Full Scale Quotas and Priorities feature helps you to improve the scalability, performance, manageability, and serviceability of rogue APs. The following commands are introduced: • **wireless wps rogue scale quota** • **wireless wps rogue scale priority** • **wireless wps rogue scale mode hybrid** For more information, see the chapter Managing Rogue Devices.
RUM Report Throttling	For all topologies where the product instance initiates communication, the minimum reporting frequency is throttled to one day. This means the product instance does not send more than one RUM report a day. The affected topologies are: *Connected Directly to CSSM*, *Connected to CSSM Through CSLU* (product instance-initiated communication), *CSLU Disconnected from CSSM* (product instance-initiated communication), and *SSM On-Prem Deployment* (product instance-initiated communication). This resolves the problem of too many RUM reports being generated and sent for certain licenses. It also resolves the memory-related issues and system slow-down that was caused by an excessive generation of RUM reports. You can override the reporting frequency throttling, by entering the **license smart sync** command in privileged EXEC mode. This triggers an on-demand synchronization with CSSM or CSLU, or SSM On-Prem, to send and receive any pending data. RUM report throttling also applies to the Cisco IOS XE Amsterdam 17.3.6 and later releases of the 17.3.x train, and Cisco IOS XE Bengaluru 17.6.4 and later releases of the 17.6.x train. From Cisco IOS XE Cupertino 17.9.1, RUM report throttling is applicable to *all* subsequent releases.

Feature Name	Description and Documentation Link
Site-Based Rolling AP Upgrade in N+1 Networks	The Site-Based Rolling AP Upgrade in an N+1 Network feature allows you to perform a staggered upgrade of APs in each site in an N+1 deployment. The following commands are introduced: • **ap upgrade staggered iteration completion** • **ap upgrade staggered iteration error** • **ap upgrade staggered iteration timeout** • **show ap upgrade site** For more information, see the chapter Site-Based Rolling AP Upgrade in an N+1 Network.
Site-Based Rolling AP Upgrade using Netconf/YANG Models	From Cisco IOS XE Cupertino 17.9.1, you can use NETCONF/YANG models to configure site-based APSP and N+1 hitless software upgrade. For more information, see the *Programmability Configuration Guide* at: https://www.cisco.com/c/en/us/support/ios-nx-os-software/ios-xe-17/products-installation-and-configuration-guides-list.html For more information on the YANG models, see the Cisco IOS XE Programmability Configuration Guide and YANG Data Models on Github at: https://github.com/YangModels/yang/tree/master/vendor/cisco/xe. You can contact the Developer Support Community for NETCONF/YANG features at: https://developer.cisco.com/
Support 6-GHz radio for Canada	In this release, Canada (CA) is added to the list of countries supporting 802.11 6-GHz radio band.
Support for Cisco Catalyst 9164I Series Wi-Fi 6E Access Points and Cisco Catalyst 9166I Series Wi-Fi 6E Access Points	From this release onwards, Cisco Catalyst 9164I Series Wi-Fi 6E Access Points and Cisco Catalyst 9166I Series Wi-Fi 6E Access Points are supported.

Feature Name	Description and Documentation Link
Support for RFC 5580 Location Attributes in the Controller	This feature uses the RFC 5580 location attributes to convey location-related information for authentication and accounting exchanges. The following commands are introduced: • **radius-server attribute wireless location delivery out-of-band** • **location civic-location identifier** • **location geo-location identifier** • **location operator identifier** • **location civic-location-id** • **location geo-location-id** • **location operator-id** • **radius-server attribute wireless location civic-location-id** • **radius-server attribute wireless location geo-location-id** • **radius-server attribute wireless location operator-id** For more information, see the chapter Configuring RFC 5580 Location Attributes.
VLAN Group to Support DHCP and Static IP Clients	The VLAN Group to Support DHCP and Static IP Clients feature aims to handle the network access of clients whose static IP address is not a part of the VLAN's IP list. For more information, see the chapter VLAN Groups.
Walkme for Usage and Troubleshooting	The following new workflows have been implemented: • **AP Join troubleshooting**: A collection of workflows that takes you through various troubleshooting commands to find out why AP join has failed. • **FlexConnect workflow**: A collection of workflows that show how to configure FlexConnect.
Wireless Rogue Channel Width Support	In this release, the Wireless Rogue Channel Width feature is supported. Rogue channel width changes are implemented at the TDL level. Because the telemetry child table cannot be accessed by Cisco DNA Center because of the TDL limitation, all radio band information is now available in the top-level table. Telemetry data can be validated through the SSH Netconf console to check the correct radio band with channel width values.

Feature Name	Description and Documentation Link
TrustSec Support in Cisco Catalyst Wi-Fi 6 Access Points	From this release onwards, Cisco Catalyst Wi-Fi 6 Access Points support TrustSec feature with the controller. **Note** The Wi-Fi 6 Access Points support the Software-Defined Access solution with Security Group Tag (SGT) feature in earlier releases.
Zero Wait Dynamic Frequency Selection	When an access point (AP) moves to Dynamic Frequency Selection (DFS) channel, a service outage can occur. This feature helps to avoid service outages in regulatory domains. As of now, the US and Europe are the only supported domains. For more information, see the chapter Dynamic Frequency Selection.

Table 6: New and Modified GUI Features

Feature Name	GUI Path
802.11r Fast Transition for SAE Authenticated Clients	• **Configuration > Tags & Profiles > WLANs**
Additional Client Information on Client 360 View	• **Monitoring > Wireless > Clients > 360**
Configuring the AP Console	• **Configuration > Tags & Profiles > AP Join**
Flexible Radio Assignment Support in Cisco Catalyst 9166I Series Wi-Fi 6E Access Points	• **Configuration > Radio Configurations > RRM > FRA**
Management Mode Migration in Cisco Catalyst 916x Series Wi-Fi 6E Access Points (CW9164 and CW9166)	• **Configuration > Wireless > Migrate to Meraki Management Mode**
Site-based Rolling AP Upgrade in N+1 Networks	• **Administration > Software Management**

MIBs

The following MIBs are newly added or modified:

- AIRESPACE-WIRELESS-MIB
- CISCO-LWAPP-AP-MIB
- CISCO-LWAPP-MOBILITY-MIB
- CISCO-LWAPP-RF-MIB

- CISCO-LWAPP-RRM-MIB
- CISCO-LWAPP-SI-MIB
- CISCO-LWAPP-TAGS-MIB
- CISCO-LWAPP-WLAN-MIB
- CISCO-LWAPP-WLAN-SECURITY-MIB

Behavior Changes

- The Cisco Centralized Key Management (CCKM) feature is being deprecated from Cisco IOS XE Dublin 17.10.x.
- The J2 country code is not supported for Japan. Use J4 as country code for Japan, instead of J2.
- The following commands are effective only in service-peer mode:

  For information on service-peer, see the *Understanding Local Area Bonjour for Wireless FlexConnect Mode* section in the chapter Configuring Local Area Bonjour for Wireless FlexConnect Mode.

  - **query-response**
  - **sdg-agent**
  - **service-announcement-count**
  - **service-announcement-timer**
  - **service-mdns-query**
  - **service-query-count**
  - **service-query-timer**
  - **service-receiver-purge**
  - **active-response**

- If wireless multicast is disabled in service-peer mode, the mDNS packets are sent to each CAPWAP interface. If wireless multicast and multicast tunnel are enabled, the mDNS packets are sent over multicast tunnel.
- The install commands cannot be executed if there is any unsaved configuration with or without the prompt-level option.
- If location is not specified in the service policy, the location is considered from the global mDNS gateway. By default, the global mDNS gateway location is defined as **lss**.
- When country is configured in the AP profile, you cannot override it using the per-AP country configuration.
- You cannot see 802.1x passwords in cleartext from this release because they are encrypted. If you downgrade to an earlier image that doesn't support an encrypted password, the APs will get stuck and repeatedly fail the dot1x authentication due to wrong credentials. You will need to disable 802.1x on the AP switch port to allow the AP to join the controller before setting the cleartext password.

- The output of the following show commands are updated:
  - **show ap dot11 cleanair device type**
  - **show ap name dot11 cleanair device**
  - **show ap dot11 5ghz SI device type**
  - **show ap name dot11 SI device**
- The following commands are introduced:
  - **ap name dot11 24ghz cleanair**
  - **ap name dot11 5ghz cleanair**
  - **ap name dot11 6ghz cleanair**

  The following commands are deprecated:
  - **ap name dot11 24ghz slot cleanair**
  - **ap name dot11 5ghz slot cleanair**
  - **ap name dot11 dual-band cleanair band**
  - **ap name dot11 ap name dot11 dual-band slot cleanair band**
  - **ap name dot11 dual-band cleanair band**
  - **ap name dot11 ap name dot11 dual-band slot cleanair band**
  - **ap name dot11 ap name dot11 dual-band slot cleanair**
  - **ap name dot11 rx-dual-band slot cleanair band**
  - **ap name dot11 rx-dual-band slot cleanair**
- Information on FIPS is added to the output of the AP **show security system state** command.
- Device analytics reports are cached for five minutes before they are made available through the **show wireless client mac stats pc-analytics** command.
- TLS 1.3 is supported for HTTPS communication on web administration from this release onwards.
- The following table describes the deprecated and replaced show commands:

Table 7: Deprecated and Replaced Show Commands

Deprecated Commands	Replaced Commands
show ap persona meraki capability summary	**show ap management-mode meraki capability summary**
show ap persona meraki change summary	**show ap management-mode meraki change summary**
show ap persona meraki failure summary	**show ap management-mode meraki failure summary**

- The **ap name <ap-name> persona meraki [force] [noprompt]** command is deprecated and replaced with **ap name <ap-name> management-mode meraki [force] [noprompt]** command.
- The USB port in the AP profile is disabled by default.

  If you are using Cisco IOx application with USB dongles, re-configure the USB port in the AP profile on reload, to ensure that the USB port is enabled before the APs join.

  For more information about the workaround, see the details in CSCvz07021.
- Controller communicates with the dnaservices.com for Product Analytics and Automatic Frequency Coordination (AFC). Even when DNS is not configured in the controller, the controller uses the hardcoded DNS server. Even when Product Analytics is disabled for AFC, the controller still tries to reach the dnaservices.com.

Note This applies from Cisco IOS XE Cupertino 17.9.4 release onwards.

- From Cisco IOS XE Cupertino 17.9.5 release onwards, the Product Analytics is enabled by default.

  For more information about Product Analytics, see Wireless Product Analytics FAQ.
- If you have configured CISCO_IDEVID_SUDI trustpoint in your configuration, you will need to replace it with CISCO_IDEVID_CMCA3_SUDI to avoid client connection and AP join issues. The reason for this change being the CISCO_IDEVID_SUDI changed from SW-SUDI certificate in previous releases to HW-SUDI certificate. The processing of HW-SUDI certificate is much slower than the SW-SUDI. Here, CISCO_IDEVID_CMCA3_SUDI is the new SW-SUDI certificate.

Note This applies from Cisco IOS XE Cupertino 17.9.3 release onwards.

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.

Important Notes

- To migrate public IP address from 16.12.x to 17.x. ensure that you configure the **service internal** command. If you do not configure the **service internal** command, the IP address does not carry forward.
- The Cisco Aironet 2800 and 3800 APs do not reset an interface (to clear any Ethernet interface physical layer issues) if the Dynamic Host Configuration Protocol (DHCP) does not resolve the IP address within a certain duration.

Supported Hardware

The following table lists the supported virtual and hardware platforms. (See Table 10: Supported PIDs and Ports for the list of supported modules.)

Table 8: Supported Virtual and Hardware Platforms

Platform	Description
Cisco Catalyst 9800-80 Wireless Controller	A modular wireless controller with up to 100-GE modular uplinks and seamless software updates. The controller occupies a 2-rack unit space and supports multiple module uplinks.
Cisco Catalyst 9800-40 Wireless Controller	A fixed wireless controller with seamless software updates for mid-size to large enterprises. The controller occupies a 1-rack unit space and provides four 1-GE or 10-GE uplink ports.

Platform	Description
Cisco Catalyst 9800-L Wireless Controller	The Cisco Catalyst 9800-L Wireless Controller is the first low-end controller that provides a significant boost in performance and features.
Cisco Catalyst 9800 Wireless Controller for Cloud	A virtual form factor of the Catalyst 9800 Wireless Controller that can be deployed in a private cloud (supports VMware ESXi, Kernel-based Virtual Machine [KVM], Microsoft Hyper-V, and Cisco Enterprise NFV Infrastructure Software [NFVIS] on Enterprise Network Compute System [ENCS] hypervisors), or in the public cloud as Infrastructure as a Service (IaaS) in Amazon Web Services (AWS), Google Cloud Platform (GCP) marketplace, and Microsoft Azure.
Cisco Catalyst 9800 Embedded Wireless Controller for Switch	The Catalyst 9800 Wireless Controller software for the Cisco Catalyst 9000 switches brings the wired and wireless infrastructure together with consistent policy and management. This deployment model supports only Software Defined-Access (SDA), which is a highly secure solution for small campuses and distributed branches.

The following table lists the host environments supported for private and public cloud.

Table 9: Supported Host Environments for Public and Private Cloud

Host Environment	Software Version
VMware ESXi	• VMware ESXi vSphere 6.0, 6.5, 6.7, and 7.0 • VMware ESXi vCenter 6.0, 6.5, 6.7, and 7.0
KVM	• Linux KVM-based on Red Hat Enterprise Linux 7.6, 7.8, and 8.2 • Ubuntu 16.04.5 LTS, Ubuntu 18.04.5 LTS, Ubuntu 20.04.5 LTS • KVM/SUSE version 15 SP3 (restricted to SDA Wireless deployments)
AWS	AWS EC2 platform
NFVIS	ENCS 3.8.1 and 3.9.1
GCP	GCP marketplace
Microsoft Hyper-V	Windows 2019 Server and Windows Server 2016 (Version 1607) with Hyper-V Manager (Version 10.0.14393)
Microsoft Azure	Microsoft Azure

The following table lists the supported Cisco Catalyst 9800 Series Wireless Controller hardware models.

The base PIDs are the model numbers of the controller.

The bundled PIDs indicate the orderable part numbers for the base PIDs that are bundled with a particular network module. Running the **show version**, **show module**, or **show inventory** command on such a controller (bundled PID) displays its base PID.

Note that unsupported SFPs will bring down a port. Only Cisco-supported SFPs (GLC-LH-SMD and GLC-SX-MMD) should be used on the route processor (RP) ports of C9800-80-K9 and C9800-40-K9.

Table 10: Supported PIDs and Ports

Controller Model	Description
C9800-CL-K9	Cisco Catalyst Wireless Controller as an infrastructure for cloud.
C9800-80-K9	Eight 1/10-Gigabit Ethernet SFP or SFP+ ports and two power supply slots.
C9800-40-K9	Four 1/10-Gigabit Ethernet SFP or SFP+ ports and two power supply slots.
C9800-L-C-K9	• 4x2.5/1-Gigabit ports • 2x10/5/2.5/1-Gigabit ports
C9800-L-F-K9	• 4x2.5/1-Gigabit ports • 2x10/1-Gigabit ports

The following table lists the supported SFP models.

Table 11: Supported SFPs

SFP Name	C9800-80-K9	C9800-40-K9	C9800-L-C-K9	C9800-L-F-K9
DWDM-SFP10G-30.33	Supported	Supported	—	—
DWDM-SFP10G-61.41	Supported	Supported	—	—
FINISAR-LR – FTLX1471D3BCL [1]	Supported	Supported	—	Supported
FINISAR-SR – FTLX8574D3BCL	Supported	Supported	—	Supported
GLC-BX-D	Supported	Supported	Supported	Supported
GLC-BX-U	Supported	Supported	Supported	Supported
GLC-EX-SMD	Supported	Supported	—	—
GLC-LH-SMD	Supported	Supported	Supported	—
GLC-SX-MMD	Supported	Supported	Supported	Supported

SFP Name	C9800-80-K9	C9800-40-K9	C9800-L-C-K9	C9800-L-F-K9
GLC-T	Supported	—	Supported	—
GLC-TE	Supported	Supported	Supported	Supported
GLC-ZX-SMD	Supported	Supported	Supported	Supported
QSFP-100G-LR4-S	Supported	—	—	—
QSFP-100G-SR4-S	Supported	—	—	—
QSFP-40G-BD-RX	Supported	—	—	—
QSFP-40G-ER4	Supported	—	—	—
QSFP-40G-LR4	Supported	—	—	—
QSFP-40G-LR4-S	Supported	—	—	—
QSFP-40G-SR4	Supported	—	—	—
QSFP-40G-SR4-S	Supported	—	—	—
QSFP-40GE-LR4	Supported	—	—	—
SFP-10G-AOC10M	Supported	Supported	—	—
SFP-10G-AOC1M	Supported	Supported	—	—
SFP-10G-AOC2M	Supported	Supported	—	—
SFP-10G-AOC3M	Supported	Supported	—	—
SFP-10G-AOC5M	Supported	Supported	—	—
SFP-10G-AOC7M	Supported	Supported	—	—
SFP-10G-ER	Supported	Supported	—	—
SFP-10G-LR	Supported	Supported	—	Supported
SFP-10G-LR-S	Supported	Supported	—	Supported
SFP-10G-LR-X	Supported	Supported	—	Supported
SFP-10G-LRM	Supported	Supported	—	Supported
SFP-10G-SR	Supported	Supported	—	Supported
SFP-10G-SR-S	Supported	Supported	—	Supported
SFP-10G-SR-X	Supported	Supported	—	Supported
SFP-10G-ZR	Supported	Supported	—	—

SFP Name	C9800-80-K9	C9800-40-K9	C9800-L-C-K9	C9800-L-F-K9
SFP-H10GB-ACU10M	Supported	Supported	—	Supported
SFP-H10GB-ACU7M	Supported	Supported	—	Supported
SFP-H10GB-CU1.5M	Supported	Supported	—	Supported
SFP-H10GB-CU1M	Supported	Supported	—	Supported
SFP-H10GB-CU2.5M	Supported	Supported	—	Supported
SFP-H10GB-CU2M	Supported	Supported	—	Supported
SFP-H10GB-CU3M	Supported	Supported	—	Supported
SFP-H10GB-CU5M	Supported	Supported	—	Supported

[1] The FINISAR SFPs are not Cisco specific and some of the features, such as DOM, may not work properly.

Optics Modules

The Cisco Catalyst 9800 Series Wireless Controller supports a wide range of optics. The list of supported optics is updated on a regular basis. See the tables at the following location for the latest transceiver module compatibility information:

https://www.cisco.com/en/US/products/hw/modules/ps5455/products_device_support_tables_list.html

Network Protocols and Port Matrix

Table 12: Cisco Catalyst 9800 Series Wireless Controller - Network Protocols and Port Matrix

Source	Destination	Protocol	Destination Port	Source Port	Description
Any	Cisco Catalyst 9800 Series Wireless Controller	TCP	22	Any	SSH
Any	Cisco Catalyst 9800 Series Wireless Controller	TCP	23	Any	Telnet
Any	Cisco Catalyst 9800 Series Wireless Controller	TCP	80	Any	HTTP

Source	Destination	Protocol	Destination Port	Source Port	Description
Any	Cisco Catalyst 9800 Series Wireless Controller	TCP	443	Any	HTTPS
Any	Cisco Catalyst 9800 Series Wireless Controller	UDP	161	Any	SNMP Agent
Any	Any	UDP	5353	5353	mDNS
Any	Cisco Catalyst 9800 Series Wireless Controller	UDP	69	69	TFTP
Any	DNS Server	UDP	53	Any	DNS
Any	Cisco Catalyst 9800 Series Wireless Controller	TCP	830	Any	NetConf
Any	Cisco Catalyst 9800 Series Wireless Controller	TCP	443	Any	REST API
Any	WLC Protocol	UDP	1700	Any	Receive CoA packets.
AP	Cisco Catalyst 9800 Series Wireless Controller	UDP	5246	Any	CAPWAP Control
AP	Cisco Catalyst 9800 Series Wireless Controller	UDP	5247	Any	CAPWAP Data
AP	Cisco Catalyst 9800 Series Wireless Controller	UDP	5248	Any	CAPWAP MCAST
AP	Cisco Catalyst Center	UDP	57778	Any	Intelligent capture and RF telemetry

Source	Destination	Protocol	Destination Port	Source Port	Description
AP	AP	UDP	16670	Any	Client Policies (AP-AP)
Cisco Catalyst 9800 Series Wireless Controller	Cisco Catalyst 9800 Series Wireless Controller	UDP	16666	16666	Mobility Control
Cisco Catalyst 9800 Series Wireless Controller	SNMP	UDP	162	Any	SNMP Trap
Cisco Catalyst 9800 Series Wireless Controller	RADIUS	UDP	1812/1645	Any	RADIUS Auth
Cisco Catalyst 9800 Series Wireless Controller	RADIUS	UDP	1813/1646	Any	RADIUS ACCT
Cisco Catalyst 9800 Series Wireless Controller	TACACS+	TCP	49	Any	TACACS+
Cisco Catalyst 9800 Series Wireless Controller	Cisco Catalyst 9800 Series Wireless Controller	UDP	16667	16667	Mobility
Cisco Catalyst 9800 Series Wireless Controller	NTP Server	UDP	123	Any	NTP
Cisco Catalyst 9800 Series Wireless Controller	Syslog Server	UDP	514	Any	SYSLOG
Cisco Catalyst 9800 Series Wireless Controller	NetFlow Server	UDP	9996	Any	NetFlow

Source	Destination	Protocol	Destination Port	Source Port	Description
Cisco Catalyst 9800 Series Wireless Controller	Cisco Connected Mobile Experiences (CMX)	UDP	16113	Any	NMSP
Cisco Catalyst Center	Cisco Catalyst 9800 Series Wireless Controller	TCP	32222	Any	Device Discovery

Supported APs

The following Cisco APs are supported in this release.

Indoor Access Points

- Cisco Catalyst 9105AXI Access Points
  - VID 04 or later - supported from 17.9.2
  - VID 03 or earlier - supported in all 17.9.x releases
- Cisco Catalyst 9105AXW Access Points
  - VID 02 or later - supported from 17.9.2
  - VID 01 or earlier - supported in all 17.9.x releases
- Cisco Catalyst 9115AX (I/E) Access Points
- Cisco Catalyst 9117AXI Access Points
- Cisco Catalyst 9120AX (I/E) Access Points
  - VID 07 or later - supported from 17.9.2
  - VID 06 or earlier - supported in all 17.9.x releases
- Cisco Catalyst 9120AXP Access Points
- Cisco Catalyst 9130AX (I/E) Access Points
  - VID 03 or later - supported from 17.9.2
  - VID 02 or earlier - supported in all 17.9.x releases

  (For information about Cisco Catalyst 9105, 9120, or 9130 Access Points version support, see the Field Notice 72424.)
- Cisco Catalyst 9136I Access Points
- Cisco Catalyst 9162I Series Access Points - supported from 17.9.2

- Cisco Catalyst 9164I Series Access Points
- Cisco Catalyst 9166I Series Access Points
- Cisco Aironet 1800I, 1815 (I/W), 1830 (I), 1840 (I), and 1850 (I/E) Access Points
- Cisco Aironet 2800 (I/E) Series Access Points
- Cisco Aironet 3800 (I/E/P) Series Access Points
- Cisco Aironet 4800 Series Access Points

Support is reintroduced for the following APs from 17.9.3:

- Cisco Aironet 1570 Series Access Points
- Cisco Aironet 1700 Series Access Points
- Cisco Aironet 2700 Series Access Points
- Cisco Aironet 3700 Series Access Points

Outdoor Access Points

- Cisco Aironet 1540 Series Access Points
- Cisco Aironet 1560 Series Access Points
- Cisco Industrial Wireless 3700 Series Access Points
- Cisco Catalyst Industrial Wireless 6300 Heavy Duty Series Access Point
- Cisco 6300 Series Embedded Services Access Point
- Cisco Catalyst 9124AX (I/D) Access Points
- Cisco Catalyst IW9167 (E) Heavy Duty Access Point - supported from 17.9.3

Integrated Access Points

- Integrated Access Point on Cisco 1100 ISR (ISR-AP1100AC-x, ISR-AP1101AC-x, and ISR-AP1101AX-x)

Network Sensor

- Cisco Aironet 1800s Active Sensor

Pluggable Modules

- Wi-Fi 6 Pluggable Module for Industrial Routers

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.

Compatibility Matrix

The following table provides software compatibility information.

Table 13: Compatibility Information

Cisco Catalyst 9800 Series Wireless Controller Software	Cisco Identity Services Engine	Cisco Prime Infrastructure	Cisco AireOS-IRCM Interoperability	Cisco Catalyst Center	Cisco Spaces: Connector	Cisco CMX
Cupertino 17.9.5	3.3 3.2 3.1 3.0 2.7 2.6 2.4	3.10.2	8.10.196.0 8.10.190.0 8.10.183.0 8.10.182.0 8.10.181.0 8.10.171.0 8.10.162.0 8.10.151.0 8.10.142.0 8.10.130.0 8.8.130.0 8.5.176.2 8.5.182.104	See Cisco Catalyst Center Compatibility Information	2.3.1 2.3 2.2	11.0 10.6.3

Cisco Catalyst 9800 Series Wireless Controller Software	Cisco Identity Services Engine	Cisco Prime Infrastructure	Cisco AireOS-IRCM Interoperability	Cisco Catalyst Center	Cisco Spaces: Connector	Cisco CMX
Cupertino 17.9.4a	3.3 3.2 3.1 3.0 2.7 2.6 2.4	3.10.2	8.10.196.0 8.10.190.0 8.10.185.0 8.10.183.0 8.10.182.0 8.10.181.0 8.10.171.0 8.10.162.0 8.10.151.0 8.10.142.0 8.10.130.0 8.8.130.0 8.5.176.2 8.5.182.104	See Cisco Catalyst Center Compatibility Information	2.3.1 2.3 2.2	11.0 10.6.3
Cupertino 17.9.4	3.3 3.2 3.1 3.0 2.7 2.6 2.4	3.10.2	8.10.183.0 8.10.182.0 8.10.181.0 8.10.171.0 8.10.162.0 8.10.151.0 8.10.142.0 8.10.130.0 8.8.130.0 8.5.176.2 8.5.182.104	See Cisco Catalyst Center Compatibility Information	2.3.1 2.3 2.2	11.0 10.6.3

Cisco Catalyst 9800 Series Wireless Controller Software	Cisco Identity Services Engine	Cisco Prime Infrastructure	Cisco AireOS-IRCM Interoperability	Cisco Catalyst Center	Cisco Spaces: Connector	Cisco CMX
Cupertino 17.9.3	3.3 3.0 2.7 2.6 2.4	3.10.2	8.10.183.0 8.10.182.0 8.10.181.0 8.10.171.0 8.10.162.0 8.10.151.0 8.10.142.0 8.10.130.0 8.8.130.0 8.5.176.2 8.5.182.104	See Cisco Catalyst Center Compatibility Information	2.3.1 2.3 2.2	11.0 10.6.3
Cupertino 17.9.2	3.3 3.0 2.7 2.6 2.4	3.10.2	8.10.183.0 8.10.182.0 8.10.181.0 8.10.171.0 8.10.162.0 8.10.151.0 8.10.142.0 8.10.130.0 8.8.130.0 8.5.176.2 8.5.182.104	See Cisco Catalyst Center Compatibility Information	2.3.1 2.3 2.2	11.0 10.6.3

Cisco Catalyst 9800 Series Wireless Controller Software	Cisco Identity Services Engine	Cisco Prime Infrastructure	Cisco AireOS-IRCM Interoperability	Cisco Catalyst Center	Cisco Spaces: Connector	Cisco CMX
Cupertino 17.9.1	3.3 3.0 2.7 2.6 2.4	3.10 MR1	8.10.181.0 8.10.171.0 8.10.162.0 8.10.151.0 8.10.142.0 8.10.130.0 8.8.130.0 8.5.176.2 8.5.182.104	See Cisco Catalyst Center Compatibility Information	2.3.1 2.3 2.2	11.0 10.6.3

GUI System Requirements

The following subsections list the hardware and software required to access the Cisco Catalyst 9800 Controller GUI.

Table 14: Hardware Requirements

Processor Speed	DRAM	Number of Colors	Resolution	Font Size
233 MHz minimum[2]	512 MB[3]	256	1280 x 800 or higher	Small

[2] We recommend 1 GHz.
[3] We recommend 1-GB DRAM.

Software Requirements

Operating Systems:

- Windows 7 or later
- Mac OS X 10.11 or later

Browsers:

- Google Chrome: Version 59 or later (on Windows and Mac)
- Microsoft Edge: Version 40 or later (on Windows)
- Safari: Version 10 or later (on Mac)

- Mozilla Firefox: Version 60 or later (on Windows and Mac)

Note Firefox Version 63.x is not supported.

The controller GUI uses Virtual Terminal (VTY) lines for processing HTTP requests. At times, when multiple connections are open, the default number of VTY lines of 15 set by the device might get exhausted. Therefore, we recommend that you increase the number of VTY lines to 50.

To increase the VTY lines in a device, run the following commands in the following order:

1. **device#** configure terminal
2. **device(config)#** line vty 50

   A best practice is to configure the service tcp-keepalives to monitor the TCP connection to the device.
3. **device(config)#** service tcp-keepalives-in
4. **device(config)#** service tcp-keepalives-out

Before You Upgrade

Ensure that you familiarize yourself with the following points before proceeding with the upgrade:

APs running Cisco IOS-XE 17.9.3 might encounter issues when attempting to upgrade their software due to insufficient space in the /tmp directory. When the /tmp space on the AP becomes full, it prevents the download of the new AP image. In such instances, we recommend that you reboot the AP.

Caution During controller upgrade or reboot, if route processor ports are connected to any Cisco switch, ensure that the route processor ports are not flapped (shut/no shut process). Otherwise, it may lead to a kernel crash.

- ISSU feature is supported only within and between major releases, for example, 17.3.x (within a release) and 17.3.x to 17.6.x (among major releases).
- Controller upgrade from Cisco IOS XE Bengaluru 17.3.x to Cisco IOS XE Bengaluru 17.6.x or Cisco IOS XE Cupertino 17.9.x or later using ISSU may fail if the **domain** command is configured. Ensure that you run the **no domain** command before starting an ISSU upgrade because the **domain** command has been removed from Cisco IOS XE Bengaluru 17.6.x.
- Controller upgrade from Cisco IOS XE Bengaluru 17.3.x to any release using ISSU may fail if the **snmp-server enable traps hsrp** command is configured. Ensure that you remove the **snmp-server enable traps hsrp** command from the configuration before starting an ISSU upgrade because the **snmp-server enable traps hsrp** command has been removed from Cisco IOS XE Bengaluru 17.4.x.
- Controller upgrade to Cisco IOS XE Dublin 17.12.x from any prior release using ISSU may fail if the **snmp-server enable traps license** command is configured. Ensure that you remove the **snmp-server enable traps license** command from the configuration before starting an ISSU upgrade because the **snmp-server enable traps license** command has been removed from Cisco IOS XE Dublin 17.12.x.
- Rolling AP upgrade, which is a part of the ISSU feature, is not supported for mesh APs.
- Ensure that you add Authentication and Key Management (AKM) setting when you configure WPA3. In older releases, this scenario was not mandatory which resulted in an invalid configuration. However, from 17.9 and higher releases, this invalid scenario is detected and prevented.

Cisco Wave 2 APs may get into a boot loop when upgrading software over a WAN link. For more information, see: https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/220443-how-to-avoid-boot-loop-due-to-corrupted.html.

The following Wave 1 APs are not supported from 17.4 to 17.9.2, 17.10.x, 17.11.x, 17.13.x, and 17.14.x:

- **Cisco Aironet 1570 Series Access Point**
- **Cisco Aironet 1700 Series Access Point**
- **Cisco Aironet 2700 Series Access Point**
- **Cisco Aironet 3700 Series Access Point**

Note

- Support for the above APs was reintroduced from Cisco IOS XE Cupertino 17.9.3.
- Support for these APs does not extend beyond the normal product lifecycle support. Refer to the individual End-of-Support bulletins on Cisco.com.
- Feature support is on parity with the 17.3.x release. Features introduced in 17.4.1 or later are not supported on these APs in the 17.9.3 release.
- You can migrate directly to 17.9.3 from 17.3.x, where x=4c or later.

- From Cisco IOS XE Dublin 17.10.x, Key Exchange and MAC algorithms like diffie-hellman-group14-sha1, hmac-sha1, hmac-sha2-256, and hmac-sha2-512 are not supported by default and it may impact some SSH clients that only support these algorithms. If required, you can add them manually. For information on manually adding these algorithms, see the **SSH Algorithms for**

Common Criteria Certification document available at:
https://www.cisco.com/c/en/us/td/docs/routers/ios/config/17-x/sec-vpn/b-security-vpn/m_sec-secure-shell-algorithm-ccc.html

- If APs fail to detect the backup image after running the **archive download-sw** command, perform the following steps:

  1. Upload the image using the **no-reload** option of the **archive download-sw** command:

     ```
     Device# archive download-sw /no-reload tftp://<tftp_server_ip>/<image_name>
     ```

  2. Restart the CAPWAP process using **capwap ap restart** command. This allows the AP to use the correct backup image after the restart (reload is not required.)

     ```
     Device# capwap ap restart
     ```

Caution The AP will lose connection to the controller during the join process. When the AP joins the new controller, it will see a new image in the backup partition. So, the AP will not download a new image from the controller.

- You might observe a high Confd CPU when full synchronization occurs between NETCONF datastore and Cisco IOS configuration. This behavior is normal and is triggered by the **line vty** command.
- From Cisco IOS XE Cupertino 17.7.1 onwards, for Cisco Catalyst 9800-CL Wireless Controller, ensure that you complete Resource Utilization Measurement (RUM) reporting and ensure that the ACK is made available on the product instance at least once. This is to ensure that correct and up-to-date usage information is reflected in the Cisco Smart Software Manager (CSSM).
- From Cisco IOS XE Amsterdam 17.3.1 onwards, the Cisco Catalyst 9800-CL Wireless Controller requires 16 GB of disk space for new deployments.

  If you are upgrading to Cisco IOS XE Amsterdam 17.3.x from a previous release, resizing of disk space is not supported. If the current disk space is lesser than 16 GB, you need to redeploy the VM to meet the new disk space requirements.
- Fragmentation lower than 1500 is not supported for the RADIUS packets generated by wireless clients in the Gi0 (OOB) interface.
- Cisco IOS XE allows you to encrypt all the passwords used on the device. This includes user passwords and SSID passwords (PSK). For more information, see the "Password Encryption" section of the Cisco Catalyst 9800 Series Configuration Best Practices document.
- While upgrading to Cisco IOS XE 17.3.x and later releases, if the **ip http active-session-modules none** command is enabled, you will not be able to access the controller GUI using HTTPS. To access the GUI using HTTPS, run the following commands in the order specified below:

  1. **ip http session-module-list pkilist OPENRESTY_PKI**
  2. **ip http active-session-modules pkilist**

- Cisco Aironet 1815T OfficeExtend Access Point will be in local mode when connected to the controller. However, when it functions as a standalone AP, it gets converted to FlexConnect mode.
- The Cisco Catalyst 9800-L Wireless Controller may fail to respond to the BREAK signals received on its console port during boot time, preventing users from getting to the ROMMON. This problem is observed on the controllers manufactured until November 2019, with the default config-register setting

of 0x2102. This problem can be avoided if you set config-register to 0x2002. This problem is fixed in the 16.12(3r) ROMMON for Cisco Catalyst 9800-L Wireless Controller. For information about how to upgrade the ROMMON, see the Upgrading ROMMON for Cisco Catalyst 9800-L Wireless Controllers section of the Upgrading Field Programmable Hardware Devices for Cisco Catalyst 9800 Series Wireless Controllers document.

- By default, the controller uses a TFTP block size value of 512, which is the lowest possible value. This default setting is used to ensure interoperability with legacy TFTP servers. If required, you can change the block size value to 8192 to speed up the transfer process, using the **ip tftp blocksize** command in global configuration mode.
- We recommend that you configure the **password encryption aes** and the **key config-key password-encrypt** *key* commands to encrypt your password.
- If the following error message is displayed after a reboot or system crash, we recommend that you regenerate the trustpoint certificate:

  ```
  ERR_SSL_VERSION_OR_CIPHER_MISMATCH
  ```

  Use the following commands in the order specified below to generate a new self-signed trustpoint certificate:

  1. device# configure terminal
  2. device(config)# **no crypto pki trustpoint** *trustpoint_name*
  3. device(config)# **no ip http server**
  4. device(config)# **no ip http secure-server**
  5. device(config)# **ip http server**
  6. device(config)# **ip http secure-server**
  7. device(config)# **ip http authentication** *local/aaa*

- Do not deploy OVA files directly to VMware ESXi 6.5. We recommend that you use an OVF tool to deploy the OVA files.
- Ensure that you remove the controller from Cisco Prime Infrastructure before disabling or enabling Netconf-YANG. Otherwise, the system may reload unexpectedly.
- Unidirectional Link Detection (UDLD) protocol is not supported.
- SIP media session snooping is not supported on FlexConnect local switching deployments.
- The Cisco Catalyst 9800 Series Wireless Controllers (C9800-CL, C9800-L, C9800-40, and C9800-80) support a maximum of 14,000 leases with internal DHCP scope.
- Configuring the mobility MAC address using the **wireless mobility mac-address** command is mandatory for both HA and 802.11r.
- If you have Cisco Catalyst 9120 (E/I/P) and Cisco Catalyst 9130 (E) APs in your network and you want to downgrade, use only Cisco IOS XE Gibraltar 16.12.1t. Do not downgrade to Cisco IOS XE Gibraltar 16.12.1s.
- The following SNMP variables are not supported:
  - CISCO-LWAPP-WLAN-MIB: cLWlanMdnsMode

- CISCO-LWAPP-AP-MIB.my: cLApDot11IfRptncPresent, cLApDot11IfDartPresent

- If you are upgrading from Cisco IOS XE Gibraltar 16.11.x or an earlier release, ensure that you unconfigure the *advipservices* boot-level licenses on both the active and standby controllers using the **no license boot level advipservices** command before the upgrade. Note that the **license boot level advipservices** command is not available in Cisco IOS XE Gibraltar 16.12.1s and 16.12.2s.
- The Cisco Catalyst 9800 Series Wireless Controller has a service port that is referred to as *GigabitEthernet 0* port.

  The following protocols and features are supported through this port:

  - Cisco Catalyst Center
  - Cisco Smart Software Manager
  - Cisco Prime Infrastructure
  - Telnet
  - Controller GUI
  - DNS
  - File transfer
  - GNMI
  - HTTP
  - HTTPS
  - LDAP
  - Licensing for Smart Licensing feature to communicate with CSSM
  - Netconf
  - NetFlow
  - NTP
  - RADIUS (including CoA)
  - Restconf
  - SNMP
  - SSH
  - SYSLOG
  - TACACS+

- During device upgrade using GUI, if a switchover occurs, the session expires and the upgrade process gets terminated. As a result, the GUI cannot display the upgrade state or status.
- From Cisco IOS XE Bengaluru 17.4.1 onwards, the telemetry solution provides a name for the receiver address instead of the IP address for telemetry data. This is an additional option. During the controller downgrade and subsequent upgrade, there is likely to be an issue—the upgrade version uses the newly

named receivers, and these are not recognized in the downgrade. The new configuration gets rejected and fails in the subsequent upgrade. Configuration loss can be avoided when the upgrade or downgrade is performed from Cisco Catalyst Center.

- From Cisco IOS XE Bengaluru 17.4.1 onwards, session timeout under the policy profile is supported.
- Communication between Cisco Catalyst 9800 Series Wireless Controller and Cisco Prime Infrastructure uses different ports:
  - All the configurations and templates available in Cisco Prime Infrastructure are pushed through SNMP and CLI, using UDP port 161.
  - Operational data for controller is obtained over SNMP, using UDP port 162.
  - AP and client operational data leverage streaming telemetry:
    - Cisco Prime Infrastructure to controller: TCP port 830 is used by Cisco Prime Infrastructure to push the telemetry configuration to the controller (using NETCONF).
    - Controller to Cisco Prime Infrastructure: TCP port 20828 is used for Cisco IOS-XE 16.10.x and 16.11.x, and TCP port 20830 is used for Cisco IOS-XE 16.12.x, 17.1.x and later releases.
- To migrate public IP address from 16.12.x to 17.x. ensure that you configure the **service internal** command. If you do not configure the **service internal** command, the IP address does not get carried forward.
- RLAN support with Virtual Routing and Forwarding (VRF) is not available.
- When you encounter the SNMP error *SNMP_ERRORSTATUS_NOACCESS 6*, it means that the specified SNMP variable is not accessible.
- We recommend that you perform a controller reload whenever there is a change in the controller's clock time to reflect an earlier time.

Note Before upgrading the Cisco Catalyst 9800-40 Series Wireless Controller image to Cisco IOS XE Cupertino 17.9.x using bundle mode, you must ensure that the ROMMON version is 17.7(3r) or later.

For other platforms, such as Cisco Catalyst 9800-80 Series Wireless Controllers, you should upgrade to 17.3(3r) and for Cisco Catalyst 9800-L Series Wireless Controllers, we recommend that you upgrade the ROMMON version to 16.12(3r) or later.

After the upgrade, you cannot downgrade to older ROMMON versions.

Note The DTLS version (DTLSv1.0) is deprecated for Cisco Aironet 1800 based on latest security policies. Therefore, any new out-of-box deployments of Cisco Aironet 1800 APs will fail to join the controller and you will get the following error message:

```
%APMGR_TRACE_MESSAGE-3-WLC_GEN_ERR: Chassis 1 R0/2: wncd: Error in AP Join, AP <AP-name>,
mac:<MAC-address>Model AIR-AP1815W-D-K9, AP negotiated unexpected DTLS version v1.0
```

To onboard new Cisco Aironet 1800 APs and to establish a CAPWAP connection, explicitly set the DTLS version to 1.0 in the controller using the following configuration:

```
config terminal
ap dtls-version dtls_1_0
end
```

Note that setting the DTLS version to 1.0 affects all the existing AP CAPWAP connections. We recommend that you apply the configuration only during a maintenance window. After the APs download the new image and join the controller, ensure that you remove the configuration.

To upgrade the field programmable hardware devices for Cisco Catalyst 9800 Series Wireless Controllers, see *Upgrading Field Programmable Hardware Devices for Cisco Catalyst 9800 Series Wireless Controllers*.

Important Before you begin a downgrade process, you must manually remove the configurations which are applicable in the current version but not in older version. Otherwise, you might encounter an unexpected behavior.

- When you downgrade an AP from a higher version to Cisco IOS XE Amsterdam 17.3.x, the AP will not be accessible through SSH or the console due to the denial of the **enable** password, when the AP has not yet joined a controller. If the AP joins a controller, then the AP becomes accessible without any password denial.

Upgrade Path to Cisco IOS XE Cupertino 17.9.x

Table 15: Upgrade Path to Cisco IOS XE Cupertino 17.9.x

Current Software	Upgrade Path for Deployments with 9130 or 9124	Upgrade Path for Deployments Without 9130 or 9124
16.10.x	—[4]	Upgrade first to 16.12.5 or 17.3.x and then to 17.9.x.
16.11.x	—	Upgrade first to 16.12.5 or 17.3.x and then to 17.9.x.
16.12.x	Upgrade first to 17.3.5 or later or 17.6.x or later, and then to 17.9.x.	Upgrade first to 17.3.5 or later or 17.6.x or later, and then to 17.9.x.
17.1.x	Upgrade first to 17.3.5 or later and then to 17.9.x.	Upgrade first to 17.3.5 or later and then to 17.9.x.

Current Software	Upgrade Path for Deployments with 9130 or 9124	Upgrade Path for Deployments Without 9130 or 9124
17.2.x	Upgrade first to 17.3.5 or later and then to 17.9.x.	Upgrade first to 17.3.5 or later and then to 17.9.x.
17.3.1 to 17.3.4	Upgrade first to 17.3.5 or later or 17.6.x or later, and then to 17.9.x.	Upgrade directly to 17.9.x.
17.3.4c or later	Upgrade directly to 17.9.x.	Upgrade directly to 17.9.x.
17.4.x	Upgrade first to 17.6.x and then to 17.9.x.	Upgrade directly to 17.9.x.
17.5.x	Upgrade first to 17.6.x and then to 17.9.x.	Upgrade directly to 17.9.x.
17.6.x	Upgrade directly to 17.9.x.	Upgrade directly to 17.9.x.
17.7.x	Upgrade directly to 17.9.x.	Upgrade directly to 17.9.x.
17.8.x	Upgrade directly to 17.9.x.	Upgrade directly to 17.9.x.
8.9.x or any 8.10.x version prior to 8.10.171.0	Upgrade first to 8.10.171.0 or later, 17.3.5 or later, or 17.6.x or later, and then to 17.9.x.	Upgrade directly to 17.9.x.
8.10.171.0 and above	Upgrade directly to 17.9.x.	Upgrade directly to 17.9.x.

[4] The Cisco Catalyst 9130 and 9124 APs are not supported in 16.10.x and 16.11.x releases.

Upgrading the Controller Software

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

For information on the upgrade process and the methods to upgrade the Cisco Catalyst 9800 Series Wireless Controller software, see the "Upgrading the Cisco Catalyst 9800 Wireless Controller Software" chapter of the *Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide*.

Finding the Software Version

The package files for the Cisco IOS XE software are stored in the system board flash device (flash:).

Use the **show version** privileged EXEC command to see the software version that is running on your controller.

Note Although the **show version** output always shows the software image running on the controller, the model name shown at the end of the output is the factory configuration, and does not change if you upgrade the software license.

Use the **show install summary** privileged EXEC command to see the information about the active package.

Use the **dir** *filesystem:* privileged EXEC command to see the directory names of other software images that you have stored in flash memory.

Software Images

- **Release**: Cisco IOS XE Cupertino 17.9.x
- **Image Names (9800-80, 9800-40, and 9800-L)**:
  - C9800-80-universalk9_wlc.17.09.x.SPA.bin
  - C9800-40-universalk9_wlc.17.09.x.SPA.bin
  - C9800-L-universalk9_wlc.17.09.x.SPA.bin
- **Image Names (9800-CL)**:
  - **Cloud**: C9800-CL-universalk9.17.09.x.SPA.bin
  - **Hyper-V/ESXi/KVM**: C9800-CL-universalk9.17.09.x.iso, C9800-CL-universalk9.17.09.x.ova
  - **KVM**: C9800-CL-universalk9.17.09.x.qcow2
  - **NFVIS**: C9800-CL-universalk9.17.09.x.tar.gz

Software Installation Commands

Cisco IOS XE, Cupertino, 17.9.x	
To install and activate a specified file, and to commit changes to be persistent across reloads, run the following command: **device# install add file** *filename* **[activate |commit]** To separately install, activate, commit, end, or remove the installation file, run the following command: **device# install ?** **Note** We recommend that you use the GUI for installation.	
add file tftp: *filename*	Copies the install file package from a remote location to a device, and performs a compatibility check for the platform and image versions.
activateauto-abort-timer]	Activates the file and reloads the device. The **auto-abort-timer** keyword automatically rolls back image activation.
commit	Makes changes that are persistent over reloads.
rollback to committed	Rolls back the update to the last committed version.
abort	Cancels file activation, and rolls back to the version that was running before the current installation procedure started.
remove	Deletes all unused and inactive software installation files.

Licensing

The Smart Licensing Using Policy feature is automatically enabled on the controller. This is also the case when you upgrade to this release. By default, your Smart Account and Virtual Account in Cisco Smart Software Manager (CSSM) are enabled for Smart Licensing Using Policy. For more information, see the "Smart Licensing Using Policy" chapter in the *Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide*.

For a more detailed overview on Cisco Licensing, see cisco.com/go/licensingguide.

Interoperability with Clients

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

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

Table 16: Test Configuration for Interoperability

Hardware or Software Parameter	Hardware or Software Type
Release	Cisco IOS XE, Cupertino, 17.9.x
Cisco Wireless Controller	See Supported Hardware, on page 23.
Access Points	See Supported APs.
Radio	• 802.11ax • 802.11ac • 802.11a • 802.11g • 802.11n • 802.11ax in 6GHz (Wi-Fi 6E)
Security	Open, PSK (WPA2-AES), 802.1X (WPA2-AES) (EAP-FAST, EAP-TLS) WPA3 AKM 802.11ax
RADIUS	See Compatibility Matrix, on page 32.
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 17: Client Types

Client Type and Name	Driver or Software Version
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 High Sierra 10.13.4
Macbook Pro Retina	OS Catalina
Macbook Pro Retina 13 inch early 2015	OS Mojave 10.14.3
Macbook Pro OS X	OS X 10.8.5
Macbook Air	OS Sierra v10.12.2
Macbook Air 11 inch	OS X Yosemite 10.10.5
MacBook M1 Chip	OS Catalina
Dell Inspiron 2020 Chromebook	Chrome OS 75.0.3770.129
Google Pixelbook Go	Chrome OS 97.0.4692.27
HP chromebook 11a	Chrome OS 76.0.3809.136
Samsung Chromebook 4+	Chrome OS 77.0.3865.105
Dell Latitude (Intel AX210)	Windows 11 (22.110.x.x)
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 (21.40.0)
Dell Latitude E5540 (Intel Dual Band Wireless AC7260)	Windows 7 Professional (21.10.1)
Dell Latitude E5430 (Intel Centrino Advanced-N 6205)	Windows 7 Professional (15.18.0.1)
Dell Latitude E6840 (Broadcom Dell Wireless 1540 802.11 a/g/n)	Windows 7 Professional (6.30.223.215)
Dell XPS 12 v9250 (Intel Dual Band Wireless AC 8260)	Windows 10 Home (21.40.0)
Dell Latitude 5491 (Intel AX200)	Windows 10 Pro (21.20.1.1)
Dell XPS Latitude12 9250 (Intel Dual Band Wireless AC 8260)	Windows 10 Home
Dell Inspiron 13-5368 Signature Edition	Windows 10 Home (18.40.0.12)
FUJITSU Lifebook E556 Intel 8260 (Intel Dual Band Wireless-AC 8260 (802.11n))	Windows 8 (19.50.1.6)

Client Type and Name	Driver or Software Version
Lenovo Yoga C630 Snapdragon 850 (Qualcomm AC 2x2 Svc)	Windows 10 Home
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 that you to update to the latest Intel wireless drivers if the advertised SSIDs are not visible.	
Tablets	
Apple iPad 2021	iOS 15.0
Apple iPad 7the Gen 2019	iOS 14.0
Apple iPad MD328LL/A	iOS 9.3.5
Apple iPad 2 MC979LL/A	iOS 11.4.1
Apple iPad Air MD785LL/A	iOS 11.4.1
Apple iPad Air2 MGLW2LL/A	iOS 10.2.1
Apple iPad Mini 4 9.0.1 MK872LL/A	iOS 11.4.1
Apple iPad Mini 2 ME279LL/A	iOS 11.4.1
Apple iPad Mini 4 9.0.1 MK872LL/A	iOS 11.4.1
Microsoft Surface Pro 3 13 inch (Intel AX201)	Windows 10 (21.40.1.3)
Microsoft Surface Pro 3 15 inch (Qualcomm Atheros QCA61x4A)	Windows 10
Microsoft Surface Pro 7 (Intel AX201)	Windows 10
Microsoft Surface Pro 6 (Marvell Wi-Fi chipset 11ac)	Windows 10
Microsoft Surface Pro X (WCN3998 Wi-Fi Chip)	Windows
Mobile Phones	
Apple iPhone 5	iOS 12.4.1
Apple iPhone 6s	iOS 13.5
Apple iPhone 7 MN8J2LL/A	iOS 11.2.5
Apple iPhone 8	iOS 13.5
Apple iPhone 8 Plus	iOS 14.1
Apple iPhone 8 Plus MQ8D2LL/A	iOS 12.4.1
Apple iPhone X MQA52LL/A	iOS 13.1
Apple iPhone 11	iOS 15.1
Apple iPhone 12	iOS 15.1
Apple iPhone 12 Pro	iOS 15.1

Client Type and Name	Driver or Software Version
Apple iPhone 13	iOS 15.1
Apple iPhone 13 Mini	iOS 15.1
Apple iPhone 13 Pro	iOS 15.1
Apple iPhone 14	iOS 16
Apple iPhone 15	iOS17
Apple iPhone SE MLY12LL/A	iOS 11.3
Apple iPhone SE	iOS 15.1
ASCOM i63	Build v 3.0.0
ASCOM Myco 3	Android 9
Cisco IP Phone 8821	11.0.6 SR1
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 3a	Android 11
Google Pixel 4	Android 11
Google Pixel 5	Android 11
Google Pixel 6	Android 11
Huawei Mate 20 pro	Android 9.0
Huawei P20 Pro	Android 10
Huawei P40	Android 10
LG v40 ThinQ	Android 9.0
One Plus 8	Android 11
Oppo Find X2	Android 10
Redmi K20 Pro	Android 10
Samsung Galaxy S9+ - G965U1	Android 10.0
Samsung Galaxy S10 Plus	Android 11.0
Samsung S10 (SM-G973U1)	Android 11.0
Samsung S10e (SM-G970U1)	Android 11.0
Samsung S20 Ultra	Android 10.0

Client Type and Name	Driver or Software Version
Samsung S21 Ultra 5G	Android 11.0
Samsung Fold 2	Android 10.0
Samsung Note20	Android 10.0
Samsung G Note 10 Plus	Android 11.0
Samsung Galaxy A01	Android 11.0
Samsung Galaxy A21	Android 10.0
Sony Experia 1 ii	Android 11
Sony Experia	Android 11
Xiaomi Mi 9T	Android 9
Xiaomi Mi 10	Android 11
Spectralink 84 Series	7.5.0.x257
Spectralink 87 Series	Android 5.1.1
Spectralink Versity Phones 92/95/96 Series	Android 10.0
Vocera Badges B3000n	4.3.3.18
Vocera Smart Badges V5000	5.0.6.35
Zebra MC40	Android 4.4.4
Zebra MC40N0	Android 4.1.1
Zebra MC92N0	Android 4.4.4
Zebra MC9090	Windows Mobile 6.1
Zebra MC55A	Windows 6.5
Zebra MC75A	OEM ver 02.37.0001
Zebra TC51	Android 6.0.1
Zebra TC52	Android 10.0
Zebra TC55	Android 8.1.0
Zebra TC57	Android 10.0
Zebra TC70	Android 6.1
Zebra TC75	Android 10.0
Zebra TC8000	Android 4.4.3
Printers	
Zebra QLn320 Mobile Printer	LINK OS 5.2

Client Type and Name	Driver or Software Version
Zebra ZT230 IndustrialPrinter	LINK OS 6.4
Zebra ZQ310 Mobile Printer	LINK OS 6.4
Zebra ZD410 Industrial Printer	LINK OS 6.4
Zebra ZT410 Desktop Printer	LINK OS 6.4
Zebra ZQ610 Industrial Printer	LINK OS 6.4
Zebra ZQ620 Mobile Printer	LINK OS 6.4
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
Intel AX 210	Driver v22.110.x.x (or above)
Samsung S21 Ultra	Driver v20.80.80
QCA WCN6855	Driver v1.0.0.901
PhoenixContact FL WLAN 2010	Firmware version: 2.71

Issues

Issues describe unexpected behavior in Cisco IOS releases in a product. 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 contain 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 an issue, click the corresponding identifier.

Open Caveats for Cisco IOS XE Cupertino 17.9.5

Identifier	Headline
CSCwi51168	FlexConnect setup fails to renew 4-way handshake when Pairwise Master Key (PMK) ID does not match.

Identifier	Headline
CSCwi55714	Controller reboots when handling Cisco Network Mobility Services Protocol (NMSP) Transport Layer Security (TLS) connection.
CSCwi53481	Controller loses SUDI MIC trustpoint when upgrading from Cisco IOS-XE 17.6.4 to 17.9.4a via SDA.
CSCwh63050	Controller with Cisco IOS-XE 17.9.3 sends Internet Group Management Protocol (IGMP) queries with a non-WLC IP address and MAC address.
CSCwi16509	APs do not join the controller with **Invalid radio slot id** error.
CSCwi60173	Security Group Tag (SGT) is not applied to wireless client in Software Defined-Access (SDA) fabric.
CSCwi28382	Controller reloads unexpectedly due to **Keymgmt: Failed to eapol key m1 retransmit failure. Max retries for M1 over**.
CSCwi57179	A client with a static IP is assigned to the wrong VLAN (vlan group) during roaming.
CSCwh18613	Encrypted mesh pre-shared key changes each time the **password encryption aes** is applied.
CSCwi62934	Cisco Catalyst 9120 AP drops the large frame downstream towards the wireless client.
CSCwi16104	Controller experiences an unexpected reboot in DBM during the Flex VLAN list retrieval.
CSCwi66133	Cisco Catalyst 9130 AP reloads unexpectedly due to kernel panic.
CSCwi42112	Wired clients learn MAC address from the Cisco Catalyst 9124 MAP port.
CSCwi56780	The MAC Authentication Bypass (MAB) is not initiated unless the controller deauthenticates the device.
CSCwi04855	Cisco Catalyst 9115 APs join and disjoin repeatedly with traceback.
CSCwi51025	Cisco Catalyst 9130 AP reloads unexpectedly resulting in kernel panic crash.
CSCwi27380	Media stream feature does not work.
CSCwi29636	Cisco Catalyst 9800-40 Wireless Controller reloads unexpectedly when Cisco IOS-XE 17.9.3 WNCD is down.
CSCwi54064	APs connected to the same controller classify each other as rogue and generate an "AP Impersonation" threat warning.

Open Caveats for Cisco IOS XE Cupertino 17.9.4a

From this release, the list of caveats is displayed using BST tool. When you click the BST link, it opens a separate window and lists the bugs sorted by severity. You can filter it further using the options in the tool.

Identifier	Headline
CSCwh37783	Lobby admin page does not load in the controller.

Click on the following link to view the other Open Caveats: BST Link

Open Caveats for Cisco IOS XE Cupertino 17.9.4

From this release, the list of caveats is displayed using BST tool. When you click the BST link, it opens a separate window and lists the bugs sorted by severity. You can filter it further using the options in the tool.

Click on the following link to view the Open Caveats: BST Link

Open Caveats for Cisco IOS XE Cupertino 17.9.3

Identifier	Headline
CSCwa67566	Cisco Catalyst 9800 Series Controller/AireOS parity: Rejects clients with wrong PMKID when changing AKM from FT to dot1x to FT again.
CSCwc06025	Mesh APs cannot associate to Root AP after disabling 'Backhaul Client Access' on IW9167EH Root AP.
CSCwc76174	Client download to DP failed and floods the sytandby console with Traceback @cpp_wlclient_create.
CSCwd31523	Flex WLAN provisioning is failing on C9800-CL hosted on Azure.
CSCwd46815	EAP-TLS is failing for the wired clients behind MAP for Cisco 2800, 3800, 4800, 1562, 6300 series APs.
CSCwd56391	Controller is not providing RSSI location data for some of the RFID tags in database.
CSCwd79502	Controller is tracking stale entry due to anchored client getting IPv4 and IPv6 in different VLANs.
CSCwd86288	Load average warning is displayed even when Cisco Catalyst 9800-80 Series Controller is healthy.
CSCwd90742	Cisco Catalyst 9120AX AP kernel crash - PC is at rhb_del_interface+0xc.
CSCwd91054	COS-APs are not encrypting EAP_ID_REQ after M1-M4 and not updating PMKID for dot1x OKC.
CSCwd96484	Controller reloads unexpectedly after generating "wncd" core files.
CSCwd98332	Controller reloads after failing to match the interface ID in the anchor message.
CSCwe04602	Cisco Catalyst 9120 AP fails to forward traffic to wireless client for about 60 seconds.
CSCwe07802	Cisco APs such as 2800, 3800, 4800, and 1562 are dropping upstream EAP packets.
CSCwe11315	Cisco Catalyst 9164 and 9166 APs running Cisco IOS-XE 17.9.2 is facing DFS detections in all channels.

Identifier	Headline
CSCwe11747	Cisco Catalyst AX Series APs are decoding EAP request ID incorrectly.
CSCwe14729	Controller reloads due to memory corruption when processing DHCP Reply Option82.
CSCwe16892	Traceback and reload occurs after detecting a bad magic number in chunk header.
CSCwe18012	Standby controller crashes while saving tbl QoS table.
CSCwe22861	AID leak is observed in Flex COS APs.
CSCwe25446	Unexpected reboot due WNCD.
CSCwe25610	Client delete initiated. Reason: CO_CLIENT_DELETE_REASON_REMOTE_MOBILITY_DELETE - Mobility Local.
CSCwe30473	Radio firmware crash is observed due to a frozen rc queue.
CSCwe31030	Cisco Catalyst 9105AXW AP is crashing.
CSCwe31270	Clients stop passing traffic when there is a missing bandwidth limit AAA attribute on the controller.
CSCwe32005	Cisco Catalyst 9130 AP: Packet loss is observed on Digital Signage device.
CSCwe38431	Controller is re-marking SIP packets from CS3 to CS0 in upstream/downstream when voice cac is configured.
CSCwe39039	Traceback is observed after provisioning controller from Cisco DNA Center.
CSCwe42211	EWC time offset is not updated on GUI.
CSCwe42302	IRCM Mobility client is deleted silently after a profile name mismatch.
CSCwe43294	Cisco Catalyst 9105AXW AP and Cisco Aironet 1815W Flex RLAN AP does not apply VLAN in the ethernet port after AAA vlan override.
CSCwe44216	AP crash is observed due to kernel panic (PC is at vfp_reload_hw+0x30/0x44).
CSCwe44991	Cisco Catalyst 9105AX AP: Kernel panic crash is observed.
CSCwe45300	Cisco Catalyst 9120 AP: Sending Msg:2 in mode:2 to hostapd failed.
CSCwe45894	AP are not forwarding IGMPv3 query to wireless clients.
CSCwe45970	APs are stuck in UBOOT.
CSCwe49267	Controller is not sending GTK M5 packet to 8821 after FT roaming between wncds.
CSCwe49356	Cisco Catalyst 9136 AP Kernel Panic: Unexpected reload csd_lock_wait+0x10/0x18.
CSCwe50033	Cisco Catalyst 9120AX AP: Clients are continuously disconnecting if more than 10 clients are using MS TEAMS.
CSCwe61084	Pubd crash is seen while performing ISSU upgrade from 17.3.7 to 17.9.3.

Open Caveats for Cisco IOS XE Cupertino 17.9.2

Caveat ID	Description
CSCwc24994	Cisco Aironet 3800 Access Point ends abnormally due to kernel panic.
CSCwc32182	Cisco Aironet 1852 Access Point experiences radio firmware crash.
CSCwc49992	Timeout during Direct Memory Access (DMA) transaction causes kernel panic in Access Point.
CSCwc75732	Cisco Aironet 4800 Access Point experiences firmware radio crash in Cisco IOS-XE 17.3.5b release.
CSCwd05213	Kernel panic crash observed when gRPC server process is executed.
CSCwd05689	Cisco Catalyst 9124 Access Point AXI RSSI is 7 dBm to 8 dBm weaker at a distance compared to other Access Point models.
CSCwd08068	Cisco Aironet 1815W Access Point crashes due to OOM when wcpd process hogs the memory.
CSCwd10570	Cisco Catalyst 9130 Access Point displays different beacon data-rates for different Basic Service Set Identifiers (BSSIDs).
CSCwd22017	Apple iOS devices are deleted due to IP Learn timeout.
CSCwd26693	The N+1 High Availability setup for FlexConnect access points is not working.
CSCwd30828	Cisco Catalyst 9120 Access Point crashes and reloads due to kernel panic.
CSCwd33981	Kernel panic crash is observed when PC is at "cpuidle_not_available".
CSCwd35577	Double bit ECC error causes the standby controller to reload.
CSCwc64201	Cisco Catalyst 9105 Access Point experiences communication gaps when working as a workgroup bridge (WGB).
CSCwc87688	Cisco Catalyst 9120 Access Point randomly displays high noise level in 5-GHz radio.
CSCwd03803	Cisco Aironet 1815I Access Point reboots when PC is at edma_poll or LR is at dma_cache_maint_page.
CSCwd20476	Wireless peers are unable to reach each other when passive client is enabled.
CSCwd21996	Cisco Catalyst 9120 Access Point experiences CleanAir sensor crash.

Caveat ID	Description
CSCwd22430	Access Points fail to view the backup image after using the "archive download-sw" command.
CSCwd25931	Wireless client does not receive IPv6 RA from wired FlexConnect local Dynamic Host Configuration Protocol (DHCP).
CSCwd28109	Cisco Catalyst 9130 Access Point experiences high latency or packet drops during TFTP.
CSCwd32900	Cisco Catalyst 9120 Access Point drops M4 during four-way handshake.
CSCwd34908	Dynamic Channel Allocation (DCA) debug in the controller does not display Slot 2 when nearby Access Point uses channel 36.
CSCwd36187	Controller does not regularly send license sync report to Cisco Smart Software Manager (CSSM).
CSCwc97199	Re-association request processing is delayed between the driver and wcp.

Open Caveats for Cisco IOS XE Cupertino 17.9.1

Caveat ID	Description
CSCwb70620	WPA TKIP client is unable to join due to mic error from client.
CSCwc00005	Cisco Catalyst 9136 AP: Auto-RF on the controller is reporting lower interference when rogue is using 40/80 MHz bandwidth.
CSCwc05366	Wireless AAA dynamic VLAN assignment: Clients cannot reach each other.
CSCwc15944	Cisco Catalyst 9800-L: Multicast traffic is not forwarded from wireless system to wireless clients.
CSCwc24994	Cisco AireOS 3800 series AP is crashing due to kernel panic.
CSCwc25974	Cisco Catalyst 9136 AP: Traffic running on AP itself is seen as interference on adjacent channels.
CSCwc28757	Cisco AireOS 3800 series AP: Radio crashes on Slot 0.
CSCwc30314	Cisco AireOS 4800 series AP is sending upstream DHCP packets in CAPWAP when in FlexConnect local switching local DHCP.
CSCwc31406	Stale entries in device-tracking database is causing false IP theft for IPv6 addresses.
CSCwc32182	Cisco AireOS 1852 AP: Radio firmware crash is observed.
CSCwc32360	Controller is deleting clients due to IP theft detection.

Caveat ID	Description
CSCwc39384	Cisco Wireless 9164 AP crashes @ PC is at cnss_wait_for_fw_ready+0xd4/0x118.
CSCwc41616	Cisco Catalyst 9105 AP: Crash is observed due to kernel panic.
CSCwc46702	Cisco Catalyst 9800-L: Crash is observed with reason critical process wncd fault on rp_0_0 (rc=134).
CSCwc60273	The AAA dashboard of Cisco DNA Centre does not display any AAA transaction data after the software upgrade.

Resolved Caveats for Cisco IOS XE Cupertino 17.9.5

Identifier	Headline
CSCwh60483	Cisco Catalyst 9136I APs manufactured between April 2023 and September 2023 display incorrect temperature readings.
CSCwf79175	Wireless clients fail to roam in FlexConnect central authentication with Pairwise Master Key ID (PMKID) mismatch.
CSCwf99932	Cisco Catalyst 9120 AP radio 1 reloads unexpectedly.
CSCwh09642	IP Theft is observed when zone ID is 0x00000000.
CSCwd63620	WNCD reloads unexpectedly in the controller when modifying the RF tag mapping for a RLAN slot.
CSCwh63270	Cisco Catalyst 9130AXI APs reload unexpectedly due to radio failure.
CSCwh71608	Cisco Aironet 1562 MAP is unable to join the RAP using Extensible Authentication Protocol (EAP) and flex-bridge site tag.
CSCwf22246	Cisco Catalyst 9130 APs calculate the management frame count differently across AP chipsets.
CSCwh27366	Cisco Aironet 3800 AP experiences radio firmware crash.
CSCwf13879	Cisco Catalyst 9800-CL Wireless Controller reloads unexpectedly.
CSCwf13107	Cisco Catalyst 9105 AP experiences radio crash during longevity test.
CSCwf96138	Apple iPhone SE third edition experiences roaming failure.
CSCwh81332	Cisco Catalyst 9130 APs experience kernel panic after an upgrade to Cisco IOS-XE 17.6.6.
CSCwh12481	Cisco Catalyst 9130 AXI-E AP does not join the controller with TZ country code.
CSCwh57076	Controller does not forward the broadcast Address Resolution Protocol (ARP) request to the wireless client.

Identifier	Headline
CSCwf53520	Cisco Catalyst 1815 AP ends abnormally due to kernel panic in Cisco IOS-XE Cupertino 17.9.2.
CSCwh14232	Controller does not send the LLC or XID spoofed frames after a mobility event.
CSCwh92425	Cisco Catalyst 9130 or 9136 APs transmit data frames to a client in power save mode.
CSCwh54762	AP experiences kernic panic when SCB is in delete pending state.
CSCwf83292	Cisco Catalyst 9130 APs do not send DHCP offer and acknowledgement over radio interface to the client.
CSCwi22895	Controller ends abnormally when the reload reason is Critical process radio resource management (RRM).
CSCwi08147	Controller GUI does not allow modifying quality of service (QoS) policies when **QoS SSID policy** is not set in the policy profile.
CSCwf07384	Wired clients behind Cisco Catalyst 9105 AP does not pass traffic.
CSCwf65794	Cisco Aironet 1852 AP reloads unexpectedly due to radio failure.
CSCwh74663	Cisco Aironet 2800, or 3800, or 4800, or 1560, or Cisco Catalyst 6300 APs do not send QoS data frames downstream.
CSCwh29924	Antenna-a does not function properly when **ab-Antenna** is included in the configuration for Cisco Catalyst 9105, 9115, or 9120 APs.
CSCwf52815	Cisco Wave 1 APs improve PMTU Discovery mechanism to honor the ICMP unreachable MTU value.
CSCwf75646	Controller MIB file to include all coded integer values for **cRFStatusLastSwactReasonCode** object.
CSCwf44441	Radio firmware ends abnormally in Cisco Catalyst 9162 and 9164 APs.
CSCwh82872	Dataplane issue between the controller and AP causes the association request drop.
CSCwf76119	Clients join using Pairwise Master Key (PMK) cache after Change of Authorization (CoA) and Access-Reject.
CSCwe71996	Cisco Catalyst Center does not display the associated APs.
CSCwh59543	Cisco Catalyst 9120 AP radio firmware and CAPWAP ends abnormally during scale longevitiy.
CSCwf78066	Cisco Catalyst Center users view "No radios in the selected band" message in the floor map.
CSCwf13804	Cisco Catalyst 9120 APs fail to onboard new client associations.
CSCwh56147	Controller does not display the SNMP OID for AP location tag.
CSCwh92459	Controller ends abnormally with wncd fault on rp_0_0.

Identifier	Headline
CSCwf40430	Mobile devices cannot prompt incorrect password in Cisco Catalyst 9130 AP after a change in Private Shared Key (PSK) SSID password.
CSCwh20944	Cisco Catalyst 9120 AP ends abnormally due to kernel panic.
CSCwh70511	Redundancy Management Interface (RMI) flaps with **Closed transport communication channel** message.
CSCwf32342	Clients are unable to roam successfully and pass traffic in SDA environment.
CSCwi07401	Controller ends abnormally while collecting wireless client statistics.
CSCwh49810	Client loses network access after inter-WNCD roam.
CSCwf88890	Cisco Catalyst 9800-L Wireless Controller GUI is stuck while loading the **Monitoring > Wireless > AP Statistics > General** page for a specific Cisco Aironet 3800 AP.
CSCwf54827	Wireless client is deauthenticated after an idle timeout.
CSCwh87903	Cisco Catalyst 9120 AP sends authentication response failures for a specific client MAC address.
CSCwh89539	CAPWAP messages are queued for more than x seconds when client throttling is turned ON.
CSCwa16835	Fabric AP and VXLAN tunnel are not updated after the switch virtual interface (SVI) MAC change.
CSCwh63050	Controller running Cisco IOS-XE 17.9.3 sends IGMP queries without controller IP and MAC addresses.
CSCwh62342	AP in FlexConnect mode as mDNS gateway does not respond correctly when Location Specific Services (LSS) filter is enabled in 5-GHz band.
CSCwh31966	Controller ends abnormally during a database abort in WNCD process.
CSCwf93992	Cisco Aironet 2800 AP in FlexConnect mode does not process the EAP-TLS fragmented packets beyond a delay of 50milliseconds.
CSCwf81866	Radio 0 workgroup bridge (WGB) configuration is not backed up correctly during a TFTP backup configuration.
CSCwf63818	Cisco Aironet 1832 AP with Cisco IOS-XE Cupertino 17.9.2 version ends abnormally due to kernel panic.
CSCwh58099	Controller allows client reconnection after client deletion and Change of Authorization (CoA) termination.
CSCvx90714	The **show interface status** command displays maximum link speed in the auto-negotiation port.
CSCwf83132	Controller does not send 802.11r mobility payload when changing the wireless mobility group name.

Identifier	Headline
CSCwh20306	FastLocate feature is disabled automatically when Cisco Advanced Wireless Intrusion Prevention System (aWIPS) is enabled.
CSCwh87343	Controller GUI experiences privilege escalation vulnerability.
CSCwi08442	APs do not join the controller when CBAR is enabled.
CSCwf32806	Controller experiences unexpected reload with "Critical process wncd fault on rp_0_0 (rc=134)".
CSCwf84639	Cisco Catalyst 9120 AP in XOR mode is not updated in **radio_oper_data** database.
CSCwi07094	Apple client does not connect to Flex WPA2+WPA3 SSID when Simultaneous Authentication of Equals (SAE) is enabled and Opportunistic Key Caching (OKC) is disabled.
CSCwi06785	Controller does not send Gratuitous ARP (GARP) in IPv4 or Neighbor Advertisement (NA) in IPv6 for wireless client in RUN state after switchover.
CSCwf59348	Cisco Catalyst 9105, 9115, and 9120 APs set the maximum transmit power level to -128dBm in Country IE.
CSCwh09879	Wave1 APs in FlexConnect mode do not allow clients to connect and sends association-response failure after changing country code.
CSCwh75431	Cisco Aironet 1830 or 1850 APs report false high channel utilization causing performance issues across 5-GHz band.
CSCwh17592	Cisco Catalyst 9130AXI AP slot 1 does not announce HT(802.11an), VHT(802.11ax) and HE(802.11ax) capabilities when dual-radio is enabled.
CSCwh30078	Cisco Aironet 1852 AP ends abnormally during throughput testing.
CSCwh88100	Cisco Aironet 3800 AP experiences kernel panic with PC at skb_unlink+0x40/0x54.
CSCwf92519	AP power profile status displays unexpected "Insufficient De-rating".
CSCwf04815	Coverage Hole Detection reduces the transmission power in Slot 0 and 1 of AP.
CSCwh02698	Controller sends incomplete Scalable Group Tag (SGT) information to Cisco ISE.
CSCwf87281	Controller ends abnormally due to unexpected reload in the Wireless Network Controller Daemon (WNCd) process.
CSCwd68141	The **show wireless wps rogue ap detail** command does not show the rogue client containment details.
CSCwh27425	Cisco Catalyst 9115AX AP does not forward a part of the CAPWAP data packets to the uplink direction.
CSCwh93655	2.4-GHz or 5-GHz radios stream both 2x2 when Cisco Catalyst 9120 AP is in **critical** condition.

Identifier	Headline
CSCwh08892	Controller GUI displays blank page after the User Login page.
CSCwh59048	Controller supports -A domain access points in Guatemala (GT) country.
CSCwh93462	The **show wireless stats ap loadbalance summary** command displays a negative value for joined or discovered APs.
CSCwe24263	Cisco Catalyst 9130 AP experiences inconsistent transmission power levels advertised in Country information of beacon frames.
CSCwf62051	AP reloads unexpectedly due to kernel panic when multicast DNS (mDNS) is enabled.
CSCwh35072	Cisco Aironet 3800 AP reloads unexpectedly due to FIQ or NMI reset.
CSCwi02479	Cisco Catalyst 9800-80 Series Wireless Controller running Cisco IOS-XE 17.9.3 reloads unexpectedly due to segmentation fault.
CSCwh99036	Controller reloads unexpectedly when WNCd ends abnormally while processing the supported AP channels.
CSCwh61011	Cisco Catalyst 9120 and 9115 APs unexpectedly disjoins from the controller and does not establish DTLS again.
CSCwh68360	Cisco Catalyst 9120 AP ends abnormally due to kernel panic.
CSCwh59420	Cisco Catalyst 9136 AP ends abnormally in Cisco IOS-XE Cupertino 17.9.4.
CSCwh50681	New SSID arp0v0 is broadcasted only after a Cisco IOS-XE Cupertino 17.9.3 wireless upgrade.
CSCwe81775	Apple devices are not deleted after sending Extensible Authentication Protocol (EAP) logoff messages.
CSCwh59109	Controller reloads due to critical process WNCd fault.
CSCwf69377	Controller IOSd ends abnormally in **span_db_port_bl_to_port_list** with an ERSPAN source update.
CSCwh68768	Controller fails to create a Flex WLAN using the Basic Wireless Setup in public cloud.
CSCwi03442	Cisco Catalyst 9130 AP does not honor the Unscheduled automatic power save delivery (U-APSD) trigger frame causing real-time protocol (RTP) stream disruption.
CSCwh08625	Cisco Catalyst 9120 APs end abnormally due to kernel panic when PC is at **_raw_spin_unlock**.
CSCwh20334	The change-of-authorization (CoA) server key appears blank in the controller GUI.
CSCwh49406	Cisco Catalyst 9130 AP displays excessive CleanAir syslogs.
CSCwh33190	Cisco Catalyst 9115 AP ends abnormally due to kernel panic.
CSCwi10656	New clients fail to join when IO IDs are exhausted due to high volume of clients in webauth pending state.

Identifier	Headline
CSCwf50558	Disabling dynamic channel allocation (DCA) aggressive in 5-GHz does not take effect.
CSCwh61007	Controller ends abnormally when it provisions multiple APs.
CSCwh33056	Policy tag description are automatically deleted when deleting a WLAN from a location.
CSCwf83515	Inconsistent transmission power levels advertised in Country information of beacon frame causes client-side issue.
CSCwh68219	Clients fail to authenticate via 802.1x using EAP-TLS.
CSCwe58841	Cisco Catalyst 9136 AP does not support Power over Ethernet (PoE) negotiations on both the ports.
CSCwe42200	RADIUS server with fully qualified domain name (FQDN) does not update properly during Domain Name Service (DNS) periodic update.
CSCwf64009	Cisco Aironet 1815 AP leaks RLAN VLAN traffic with looped port.
CSCwh88246	URL filter is not applied after an invalid configuration.
CSCwh45418	Cisco Catalyst 9124 AP sends incorrect duplex information through CDP.
CSCwf60519	Clients performing inter-WNCD roaming using 802.11r fails due to invalid Pairwise Master Key (PMK) ID.
CSCwh76420	Controller ends abnormally when performing an In-Service Software Upgrade (ISSU) upgrade.
CSCwh44793	Cisco Catalyst 9130 AP fails to join the controller and sets Fast Transition data in BSSID after modifying the site tag.
CSCwh20934	Cisco Wave 2 APs reboot repeatedly with Systemd critical process crash.
CSCwe70039	Client gets stuck in authentication loop after an N+1 High Availability switchover.
CSCwf86242	Controller reloads unexpectedly when CAPWAP window size is set to 0.
CSCwi22847	Cisco Catalyst 9800-80 Wireless Controller ends abnormally after receiving analytics from AP.
CSCwh37783	Controller GUI does not load the Lobby Admin page.
CSCwh22981	WNCD process ends abnormally.
CSCwh21092	Controller ends abnormally generating a system report with two core files (cpp_cp_svr and cpp-mcplo-ucode).
CSCwf68612	Controller reloads unexpectedly due to segmentation fault in WNCd process.
CSCwf30701	Cisco Aironet 2800 and Cisco Catalyst 9120 APs as supplicant cannot initiate the Extensible Authentication Protocol (EAP) process without a static IP address.

Identifier	Headline
CSCwh29442	Cisco Catalyst 9800-40 Wireless Controller ends abnormally after In-Service Software Upgrade (ISSU) upgrade to Cisco IOS-XE 17.9.x.
CSCwf83278	Client traffic fails with N+1 when AP sends CLIENT_DEL_STOP_REASSOC.

Resolved Caveats for Cisco IOS XE Cupertino 17.9.4a

Identifier	Headline
CSCwh87343	Cisco IOS XE Software Web UI Privilege Escalation Vulnerability For more information, see Security Advisory: cisco-sa-iosxe-webui-privesc-j22SaA4z.

Resolved Caveats for Cisco IOS XE Cupertino 17.9.4

Identifier	Headline
CSCwf42824	Cisco Catalyst 9105AXW APs do not recover after an upgrade.
CSCwe38431	Controller remarks SIP packets from CS3 to CS0 in upstream or downstream when voice Channel Availability Check (CAC) is configured.
CSCwe87973	Cisco Aironet 3800 AP reloads unexpectedly due to FIQ or NMI reset.
CSCwd46815	Cisco Wave 2 APs: EAP-TLS fails for wired clients behind MAP.
CSCwf34100	When Samsung device (Galaxy Tab S6 Lite - P610K) tries to associate with a Cisco AP, AP sends association rejected with status code 40.
CSCwd79502	Device tracking stale entries are observed when FlexConnect and foreign anchor SSIDs use two different VLANs.
CSCwe92340	Cisco Catalyst 9136I-ROW AP ends abnormally due to kernel panic.
CSCwe82892	Client connected to flexconnect APs with profile policy is assigned to VLAN 1 instead of native VLAN.
CSCwe17593	Cisco Catalyst 9115 AP stops sending traffic to the root AP after 60 seconds from its initial connection.
CSCwf44483	The Cisco Catalyst 9120AXI 5-GHz radio AP remains operationally down when -A domain AP joins the controller for country Panama (PA).
CSCwf04748	AP reloads unexpectedly due to CALLBACK FULL reset radio.
CSCwd60034	Cisco Aironet 3800 AP radio reloads unexpectedly when the beacon is stuck.
CSCwe25446	Controller reboots unexpectedly due to wncd process.
CSCwe85742	Controller clears PMK ID when it fails to ressurect client entry upon N+1 AP failover.

Identifier	Headline
CSCwe14729	Controller might reboot due to memory corruption when processing DHCP Reply option 82.
CSCwe04602	Cisco Wave 2 AP fails to forward traffic to wireless client for about 60 seconds in SDA fabric WLANs.
CSCwe11213	Cisco Catalyst 9130 AP crashes due to radio recovery failure.
CSCwe30473	Cisco Wave 2 AP Radio firmware reloads unexpectedly when RC queue is stuck.
CSCwe49267	Controller does not send GTK M5 packet to Cisco IP Phone 8821 after fast transition roaming between wncds.
CSCwe66216	Cisco Catalyst 9136 AP experiences mac-flap notification when interface speed is set to 1000.
CSCwe73758	Cisco Catalyst 9115AX AP is unable to send beacons in 5-GHz radio.
CSCwe73403	DHCP Option 82 is not added in WLAN with EoGRE tunnel when SVI interface is down.
CSCwe11315	Cisco Catalyst 9164 and 9166 APs running Cisco IOS-XE 17.9.2 experiences DFS detections in all channels.
CSCwe67580	CAWAP DATA tunnel is not formed between OEAP and controller after changing the public IP.
CSCwd91054	Cisco Wave 2 AP do not encrypt EAP_ID_REQ after M1-M4 and update PMKID for dot1x Opportunistic Key Caching (OKC).
CSCwe81552	Transmit Power Control (TPC) does not work as expected in the secondary radio operating in 5-GHz band.
CSCwe56266	RRM crash is observed during bootup in the controller.
CSCwe76818	Cisco Catalyst 9800-80 Wireless Controller - Syslog configuration does not reflect in the AP.
CSCwf29742	Cisco Catalyst 9120 AP: Firmware crashed is observed when multicast and longevity is run with 80+ clients after 12 hours.
CSCwe66515	Cisco Catalyst 9136 AP does not register with M2 response from client.
CSCwe74874	Cisco Catalyst 9120 AP randomly crashes due to kernel panic.
CSCwf33623	Cisco Catalyst 9162I AP radios experiences operational status down when AP is operating in 802.3af (default mode).
CSCwe07802	Cisco Wave 2 APs drop upstream Extensible Authentication Protocol (EAP) packets.
CSCwe01579	wncd reloads when creating an RRM client coverage in a large scale setup.

Identifier	Headline
CSCwe74653	Cisco Wave 2 APs do not send the DELETE reason to the controller resulting in stale entries.
CSCwe18012	Crash is observed in standby controller while saving the QOS table to standby.
CSCwf07605	Cisco Catalyst 9105AXW AP and Cisco Aironet 1815W Flex RLAN AP does not apply VLAN in the ethernet port after AAA VLAN override.
CSCwe66730	Dynamic Channel Assignment (DCA) assigns wrong channels after Dynamic Frequency Selection (DFS) events.
CSCwf15582	AP radio reloads unexpectedly when the beacon is stuck.
CSCwe62694	wncd goes into infinite loop in customer network with 382 APs.
CSCwe91394	Aeroscout T15e tags do not report the temp data due to extra bytes.
CSCwe70970	Need an option to prioritize KeepAlives in the redundancy port for High Availability SSO deployment.
CSCwf44027	The username is randomly missing for wireless 802.1x clients in the controller GUI or console.
CSCwf50177	Cisco Catalyst 9105AXW AP detects large number of bad blocks.
CSCwe39888	RRM process crashes while running Dynamic Channel Assignment (DCA) algorithm.
CSCwf07264	WNCd reloads unexpectedly when accessing the Crimson database.
CSCwe27839	Kernel panic is observed in Cisco Catalyst 9120 AP during Longevity test.
CSCwe67810	Cisco Wave 2 APs in Flexconnect standalone mode disconnects clients on DHCP renewal every 18 minutes.
CSCwe55390	Cisco Aironet 3802 AP experiences buffering when UP6 or voice traffic is less than 500ms after Spectralink phone roam causes audio issues.
CSCwe99957	Controller does not respond to keepalive from AP after an AP disconnect.
CSCwe80617	Wireless clients are unable to connect to Cisco Aironet 1830 AP after input or output error message.
CSCwb51757	High channel utilization on 5-GHz radio when channel bonding is set to 40 MHz.
CSCwf54714	Controller reloads unexpectedly.
CSCwe30429	Cisco Catalyst 9800-L Series Wireless Controller displays last reload reason as 'reload' instead of "Critical process wncd fault".
CSCwe35285	Controller deletes client. This could be triggered by CSCwd91054 fix.
CSCwf71255	Client traffic fails after AP N+1 failover and policy update.
CSCwd72847	Cisco Catalyst 9115 AP stops transmitting multicast traffic downstream.

Identifier	Headline
CSCwf55303	Active controller reboots when RP link comes up.
CSCwe53639	Controller is sending high volume of messages matching 'brain: +(awk|sed)'.
CSCwd56391	Controller is not providing Received Signal Strength (RSSI) location data for some of the RFID tags in database.
CSCwf22225	Cisco Catalyst 9120 AP: Standardize calculation of management frame count across AP chipsets.
CSCwf42629	VLAN group supports static IP clients when dot1x SSID have Security Group Tag (SGT) via AAA override.
CSCwe00848	Cisco Catalyst 9105 AP reloads unexpectedly.
CSCwe15338	Cisco Catalyst 9120 AP: Tx is stuck and AP does not respond to client's probe or authentication.
CSCwe07297	Cisco Catalyst 9120 AP reloads unexpectedly due to radio firmware crash.
CSCwc49970	Channel 165 is not allowed on Cisco Aironet 2800, 3800, 4800 APs.
CSCwe92462	Client Data Rate chart is skewed by management rate rather than data rate.
CSCwf09008	Cisco Catalyst 9800-L Series Wireless Controller crashes with last reload reason: Critical process wNCD fault on rp_0_0 (rc=139).
CSCwe32853	Cisco Catalyst 9124AXI AP is not forwarding Remote LAN (RLAN) traffic to the upstream network.
CSCwd98332	The controller undergoes a reload when the interface ID in the anchor message does not match.
CSCwe71081	macOS Setup Assistant: Guest issue is observed.
CSCwe84267	Cisco Wave 2 AP in flex N+1 failover mode doesn't transmit first CAPWAP data keepalive.
CSCwf67316	The Cisco 2800, 3800, 4800, 1560, IW6300 series APs may not detect radar in the required levels after the CAC time.
CSCwe82287	AP prevents a Protected Management Frame (PMF) Wi-Fi Protected Access Version 3 (WPA3) client from associating after the client initiates self-deauthentication.
CSCwe30572	Cisco Wave 2 AP is leaking Network Address Translation (NAT) IP from iOX app.
CSCwf45495	Cisco Catalyst 9130 AP fails to start CAPWAP as interface is reset every 52s during DHCP process.
CSCwf11117	Cisco Catalyst 9120 AP: Root AP deauthenticates workgroup bridge (WGB) continuously after a roam.

Identifier	Headline
CSCwe95127	Controller is providing incorrect data for certain APs in response to the SNMP query bsnAPIfDot11BSSID.
CSCwe76817	CAPWAP Maximum Transmission Unit (MTU) discovery issue is reported on APs.
CSCwe91264	AP reloads unexpectedly when PC is at get_partial_node.isra.
CSCwd68141	Rogue containment LRAD is not shown in the output of the **show wireless wps rogue ap detail** command.
CSCwe19858	Cisco Catalyst 9130 AP advertises incorrect local power constraint value in management frames.
CSCwe17920	Cisco Catalyst 9124 AP is not forwarding traffic to workgroup bridge (WGB) after a session timeout.
CSCwf14803	Controller web UI menu displays cryptic feature names after upgrade.
CSCwe74895	Controller crashes when running AP packet capture.
CSCwf22788	The **show wireless client summary detail** command output is not showing all IPv6 addresses.
CSCwf88588	The AP manager experiences a crash while performing an ISSU upgrade to version 17.9.3, leading to the controller entering a boot loop.
CSCwd41463	Access points intermittently stop sending Internet Group Management Protocol (IGMP) membership report.
CSCwf09259	AP LED flash is automatically turning on after a reboot.
CSCwf57471	Enabling Application Visibility and Control (AVC) on wireless policy profiles containing special characters results in the web UI entering a hung state.
CSCwe42302	The Inter-Release Controller Mobility (IRCM) client is deleted silently after a profile name mismatch.
CSCwe45553	Revise the error message displayed during one-shot AP Service Pack (APSP) installation to enhance clarity.
CSCwd86288	Load average warning is displayed even when Cisco Catalyst 9800-80 Series Wireless Controller is healthy.
CSCwe18185	Day 0 factory image for new out of the box Cisco Catalyst 9130 AP (VID03) does not contain iox.tar.gz.
CSCwf71906	Controller is not plumbing IPv4 address in IP Source Guard (IPSG) datapath on Central Web Authentication (CWA) SSIDs for clients having single IPv4 address.
CSCwd08068	Cisco Aironet 1815W AP crashes due to Out of Memory (OOM); WCPD is causing Out of Memory in 8.10.171.0 (MR7).
CSCwe63089	The LEDs on the APs are sporadically changing to a white color.

Resolved Caveats for Cisco IOS XE Cupertino 17.9.3

Identifier	Headline
CSCvx32806	COS-APs are stuck in bootloop due to image checksum verification failure.
CSCwb72924	FlexConnect client is intermittently unable to reconnect to an AP.
CSCwc10696	Regular ASR support field is disabled for supporting clients.
CSCwc24994	Cisco Aironet 3800 series AP crashes due to kernel panic (PC is at vfp_reload_hw+0x30/0x44).
CSCwc32182	Cisco Catalyst AP 1852: Radio firmware crash is observed.
CSCwc54410	Controller HA dual active scenario is observed when standby controller is reconnecting to HA pair.
CSCwc55632	Cisco Catalyst 9124 MAP fails to connect to Cisco Aironet 1562 RAP after first reload of MAP.
CSCwc75732	Cisco Aironet 4800 AP: Firmware radio crash is observed.
CSCwc79718	Cisco Catalyst 9166I AP: Multiple cores are reported after image upgrade.
CSCwc81656	Flash file system corruption is observed on AIR-CAP2702E-K-K9.
CSCwc87688	Cisco Catalyst 9120 AP shows very high noise level on 5-GHz radio.
CSCwc89183	Controller crash is observed on libewlc_client_dpath_svc.so.
CSCwc97298	Cisco Catalyst 9166 AP: Radio-2 firmware crash is observed - Thread ID: 0x00000014 Thread name: WLAN_SCHED0;PC: 0x015dc73c.
CSCwd02898	Cisco Catalyst 9300 Series Switch is not flushing remote MAC address after roaming to a local AP.
CSCwd02960	Cisco Catalyst 9166 AP: XoR radio (slot-2); switching between 5-Ghz and 6-Ghz causes kernel panic.
CSCwd03803	Cisco Aironet 1815I AP reboot: PC is at edma_poll / LR is at dma_cache_maint_page.
CSCwd04025	PI 3.10.1: Associated APs with controller is showing interface "Half duplex".
CSCwd04571	Memory leak is observed in wncd process when under load.
CSCwd06001	Linux iosd crash on standby controller during reload of the Cisco Catalyst 9800-L Wireless Controller.

Identifier	Headline
CSCwd06018	802.11r re-auth failed due to invalid Pairwise Master Key ID (PMKID) while doing inter-WNCD roaming.
CSCwd06122	AP Join issues reported due to stale client entries.
CSCwd08678	Timer is not running state client not deleted by controller.
CSCwd10570	Cisco Catalyst 9130 AP: Beacon with incorrect datarates - different rates for same slot on different BSSIDs.
CSCwd12120	Inject path crash is observed on controller switch on IPv6_qos.
CSCwd12754	CAPWAP wireless traffic is getting the same Security Group Tag (SGT) as the corresponding incoming wired traffic.
CSCwd19631	Cisco Catalyst 9120 AP cannot operate in mGig when EEE is enabled on switchport.
CSCwd21996	Cisco Catalyst 9120 AP: CleanAir sensor is crashing.
CSCwd23681	Controller fails to update AP config with error "% Error: no ap_name exists".
CSCwd26693	N+1 HA for FlexConnect is not working.
CSCwd28226	Cisco Catalyst 9136 AP in sniffer mode suffers capwapd crash followed by join/disjoin loop.
CSCwd30828	Cisco Catalyst 9120 AP: Kernel panic crash is observed.
CSCwd32107	Cisco Aironet 2700 AP: Ignore CAPWAP_PAYLOAD: AP_LAN_CONFIG payload having invalid RLAN port enable value.
CSCwd34890	Clients are getting deauth immediately after getting IP address in LWA+LocalSW+CentralAuth.
CSCwd34908	Controller is not following the Dynamic Channel Assignment (DCA) sensitivity threshold.
CSCwd35393	Wireless load balancing affinity incorrectly shows AP site tag as default-site.
CSCwd35577	Redundancy fails during double bit ECC error
CSCwd39605	Cisco Catalyst 9117 AP reloads unexpectedly due to kernel panic at console_unlock+0x320/0x3ac.
CSCwd40731	AP reloads due to kernel panic - not syncing: softlockup: hung tasks.
CSCwd41108	Cisco Catalyst 9130AXE AP with Dart connectors are stuck at channel 36.

Identifier	Headline
CSCwd46091	Cisco Catalyst 9105AXI AP is requesting 30 watts instead of 15.4 watts.
CSCwd46721	IP Theft occurs due to stale client entries in the ODM database.
CSCwd46770	License: Remove reporting interval (fixed 8 hours) and change Sync report to a user action.
CSCwd47741	Controller is failing to update dynamic channel assignment (DCA) channels in radio resource management (RRM) are stuck.
CSCwd49166	Cisco Aironet 3800 AP is consistently reporting high QoS Basic Set Service (QBSS) load.
CSCwd49861	AIRESPACE-WIRELESS-MIB: bsnAPIfType OID documentation incomplete.
CSCwd52385	AP is not initiating gRPC connection to Cisco DNA Center correctly after token expiry.
CSCwd52745	Cisco Aironet 3802 AP: Kernel crash is observed.
CSCwd52938	Wired clients behind workgroup bridge (WGB) are not getting IP address in anchor WLAN.
CSCwd55757	Wave 2 APs: Systemd critical process crash - dnsmasq-host.service failed.
CSCwd56621	Controller GUI logging buffer size display is incorrect.
CSCwd59921	Cisco Catalyst 9130 AP is dropping EAP-TLS frames.
CSCwd60376	Cisco Catalyst 9120 AP: Kernel panic is observed with PC is at pci_generic_config_read+0x34/0xa8.
CSCwd61428	Cisco Catalyst 9136I AP: GRPC crash is observed.
CSCwd63516	Cisco Catalyst 9120 AP fails EAP-TLS port authentication after Plug and Play (PnP) configuration is pushed.
CSCwd63665	Cisco Catalyst 9800-80 Series Wireless Controller shows high CPU utilization in wncd with 200 APS due to WSA.
CSCwd63861	SIGSEGV crash is observed when incrementing roaming statistics.
CSCwd69780	Controller crashes due to netflow watchdog and observed CPU HOG in wncmgrd due to scale netflow.
CSCwd72295	Cisco Catalyst 9136 AP: AP radios are going down if country code is set to RO.
CSCwd74123	Cisco Catalyst 9105 OEAP: Personal SSID is not advertising HE IE in beacon.

Identifier	Headline
CSCwd74571	Wcpd crashes after reusing freed packets.
CSCwd76693	Profile mismatch counter is not increasing.
CSCwd77188	Cisco Aironet 3802 AP: Broadcasts different power values in beacon country IE.
CSCwd77823	Cisco Catalyst 9130 AP: Radio firmware crash is observed.
CSCwd79178	Cisco Aironet 1840 OEAP: Crash is observed due to radio failure.
CSCwd79645	Wireless client are unable to communicate after session timeout when AP dropped once during the session.
CSCwd80290	IOS AP image validation certificate failed/expired, causing AP join issues.
CSCwd81523	Cisco Catalyst 9130 AP is not sending EAP_ID_RESP next assoc-req after PMF client tx deauth in middle of EAP handshake.
CSCwd83840	Cisco Aironet 1830 AP: Wireless clients are unable to connect - "writing to fd 27 failed!".
CSCwd83841	EWC: AP is not sending packets from wired interface to subnet 192.168.129.0/24.
CSCwd90472	Adding static IP MAC binding to device tracking fails.
CSCwd90907	Cisco Catalyst 9164 AP: Crash is observed on Radio 1.
CSCwd90909	Cisco Catalyst 9115 AP: Crash is observed on Radio 1.
CSCwd93773	Controller should not enable 2nd 5Ghz radio for 9124E with PoE+ (30W).
CSCwd96376	Unable to login to controller GUI or CLI with the user created by Day 0 Wizard.
CSCwd99656	The **snmp-server host** command is not filtering characters properly (Fails when name is e.g.TEST\).
CSCwe00248	Poor reassociation behavior is observed between Spectralink 84xx series phones and Cisco Catalyst 9136 APs.
CSCwe06752	Controller GUI cannot configure HA/SSO if wireless mgmt interface is not configured.
CSCwe08688	EWC: Mesh ap factory reset mode cannot be set to EWC after converting it to CAPWAP and factory-reset.
CSCwe11547	Crash is seen on "Critical process rrm fault on rp_0_0 (rc=139)".

Identifier	Headline
CSCwe12057	QoS Page is not loading when access control list (ACL) has double quote special character in the name.
CSCwe18524	AP filter error in the controller GUI when add operation follows edit/view.
CSCwe26846	Console Flood- check_dot1x_feature_status: config change or tams_init_not_done.
CSCwe28717	Certificate failures observed when joining APs to Cisco Catalyst 9800 controller using CMCA III.
CSCwe32728	Cisco Catalyst 9162 AP crashes due to radio failure.
CSCwe38326	Cisco Catalyst 9166 APs are stuck in CAPWAP state.

Resolved Caveats for Cisco IOS XE Cupertino 17.9.2

Caveat ID	Description
CSCwa42620	Cisco Catalyst 9130 Access Point drops packets on-air for Phoenix WinNonlin application.
CSCwa86610	Cisco Aironet 2802 and 3802 Access Points experience kernel panic crash when 8.10.151.0 image is executed.
CSCwc09461	Cisco Catalyst 9120 Access Points send Authentication response frames to clients after long delays.
CSCwc62021	Default credential does not work after factory reset in Cisco Aironet 1815 and 1832 Access Points.
CSCwc75102	Conversion of Mobility Express Access Points from ME to CAPWAP mode using DHCP option 43 does not work.
CSCwc78435	Cisco Catalyst 9130 Access Point sends incorrect channel list in out-of-band DFS event causing client connectivity issues.
CSCwd00751	Cisco Aironet 2802 Access Point reloads unexpectedly on 8.10.171 release version.
CSCwd08259	Cisco Catalyst 9120, 9115, and 9105 Access Points experience radio firmware crash with Cisco IOS-XE 17.3 or later releases.
CSCvv96364	Cisco Aironet 3800 Access Points experience WCPd crash when running 17.3.1 image.
CSCvx80422	An access point fails to forward packets when using 10.128.128.127 or 10.128.128.128 addresses.
CSCvz66623	EAP-TLS clients behind the Mesh Access Point (MAP) experience authentication failure.

Caveat ID	Description
CSCwb08291	Cisco Catalyst 9105AXW Access Point introduces latency when clients use RLAN ports.
CSCwc05350	Cisco Wave 2 Access Points: CAPWAP MTU flapping occurs due to asymmetric MTU between Access Point to controller and vice-versa.
CSCwc10621	CleanAir statistics are not visible in Cisco Catalyst 9130 Access Points when joined to EWC.
CSCwc35321	Cisco Wave 2 Access Points in Local mode sends Address Resolution Protocol (ARP) requests to wireless clients from 10.128.128.128 IP address.
CSCwc38912	Changing an Access Point site or policy tag to a Flex local switching set intermittently causes client connectivity failure to local web auth WLANs.
CSCwc51894	Cisco Catalyst 9117 Access Point reloads unexpectedly due to kernel panic with "dp_print_host_stats" logs.
CSCwc56774	Workgroup Bridge (WGB) with static IP loses IP address after multiple roams.
CSCwc71198	CAPWAP flapping is observed when VRRPv3 is present in the network.
CSCwc73462	Backslash "\" in the end of the RADIUS servers' shared secret is not allowed for FlexConnect groups configuration.
CSCwc81341	Cisco Catalyst 9130 Access Point experiences kernel panic crash in Local mode when full data packet capture is enabled.
CSCwc89719	Cisco Aironet 1832 Access Point crashes due to radio failure.
CSCwc96683	Controller running Cisco IOS-XE 17.3.5a with Cisco Aironet 3800 Access Point in Flex local switching does not forward IP fragmented packets received with DF.
CSCwd07572	Access Point stops transmitting UBPR in 6-GHz when it is active in 2.4-GHz or 5-GHz band.
CSCwc05366	Wireless clients cannot reach each other as ARP resolution fails when performing dynamic VLAN assignment using AAA with SSID.
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 and few Access Points are unable to join the controller.

Caveat ID	Description
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.
CSCwc42784	Client fails to connect when protocol based Quality of Service (QoS) is configured.
CSCwc57227	Controller experiences an unexpected reset resulting in a system report containing a wncd core file.
CSCwc59518	Cisco Catalyst 9800-80 Wireless Controller crashes when using WLAN profile with 32 characters and disabled voice Channel Availability Check (CAC).
CSCwc68682	Cisco Catalyst 9800 Wireless Controller - Link down due to local fault.
CSCwb47040	Controller does not update Radio Frequency Identification (RFID) location properly.
CSCwb78191	The AAA VLAN override is not considered with iPSK authentication and anchor WLAN.
CSCwc17774	Few OIDs in CISCO-ENHANCED-MEMPOOL-MIB display "No instance after switchover" in Cisco IOS-XE 17.6.1.
CSCwc26819	Controller does not send LLC or XID spoofed frames after a mobility event.
CSCwc28408	Controller crashes intermittently due to wncd critical process failure.
CSCwc36125	Radio Resource Management (RRM) startup mode gets triggered on every reboot as the controller does not keep track of the last state.
CSCwc41358	Controller MAC filtering: WLAN profile column displays the WLAN name and description.
CSCwc41903	Syslog "LISP RELIABLE REGISTRATION" needs to be enhanced.
CSCwc57836	Restore configuration by HTTP mode does not work in EWC.
CSCwc62824	Controller does not send LLC or XID spoofed frames after a mobility event.
CSCwc69815	Cisco Catalyst 9300 switch interface generates RUM reports every 8 hours when AIR controller licenses are handled incorrectly.
CSCwc72047	Access Points operate in disabled RF profile channels in Cisco IOS-XE 17.6.2 release version.

Caveat ID	Description
CSCwc74020	Need to increase the 8 IP address limit in the controller datapath.
CSCwc76905	Switch Integrated Security Features (SISF) crash is observed when handling the DHCP messages.
CSCwd17349	Active chassis gets stuck during SSO failover in Cisco IOS-XE 17.9 release version.

Resolved Caveats for Cisco IOS XE Cupertino 17.9.1

Caveat ID	Description
CSCwb52755	Fast Transition capable Apple and Android clients are unable to authenticate with IPSK profile.
CSCwb09248	High latency and packet drops are observed when associated to Cisco Catalyst 9130 AP.
CSCwb76935	Cisco Aironet 1815T AP: OEAP kernel panic crash is observed.
CSCwb97557	Cisco Aironet 3800 AP: Slot0 BSSID beacon frames are received on slot1 radio.
CSCwc04197	Secondary controller crash is observed during redundancy switchover.
CSCwc04328	6 GHz RRM: Channel-aware TPC is always on for 6 GHz TPC.
CSCwc04673	Cisco Wireless 9166 AP crashed at ieee80211_mbssid_del_profile upon flapping WLAN.
CSCwc07014	AP sends empty FlexConnect client cache payload to controller after successful client FT-SAE roam.
CSCwc08770	Cisco Wave 2 AP: Able to do SSH to AP when AP SSH global config is disabled.
CSCwc15229	Cisco Aironet 1832 AP reloads due to radio failure - Beacons are stuck on radio.
CSCwc17898	Observed a crash while joining AP with name that already exists on controller.
CSCwc20929	APP hosting segmentation doesnt work on Cisco Catalyst 9100 AP connected to a controller running 17.6.3.
CSCwc21428	6 GHz radio: Frequent channel changes are observed due to high utilization.
CSCwc27716	Memory leak is observed while deleting and adding mDNS rules.

Caveat ID	Description
CSCwc29238	WGB ping gateway failed after wgb associate to ap in 2.4 GHz and trigger wgbwiredclient get ipv4.
CSCwc29760	Cisco Aironet 3800 AP: Crash is observed due to led_core on ap.
CSCwc31277	6 GHz: Beacon stuck + QBSS 100%; no recovery ap.
CSCwc40483	Transmission power is not getting applied to Slot 1 on AP.
CSCwc43716	Not able to login AP CLI with credentials in site survey mode.
CSCwc46228	Unable to add AP location name on web UI with a space.
CSCwc62021	Cisco Aironet 1815 and 1832 APs: Default credentials are not working after the factory reset.
CSCwa65584	Controller does not accept Cisco Catalyst C91xx Series Access Points as TrustSec capable platform.

Troubleshooting

For the most up-to-date, detailed troubleshooting information, see Troubleshooting TechNotes.

Related Documentation

- Information about Cisco IOS XE
- Cisco Validated Design documents
- MIB Locator to locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets

Cisco Wireless Controller

For more information about the Cisco wireless controller, lightweight APs, and mesh APs, see these documents:

- Cisco Wireless Solutions Software Compatibility Matrix
- Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide
- Cisco Catalyst 9800 Series Wireless Controller Command Reference
- Cisco Catalyst 9800 Series Configuration Best Practices
- In-Service Software Upgrade Matrix
- Upgrading Field Programmable Hardware Devices for Cisco Catalyst 9800 Series Wireless Controllers

The installation guide for your controller is available at:

- Hardware Installation Guides

All Cisco Wireless Controller software-related documentation

Cisco Catalyst 9800 Wireless Controller Data Sheets

- *Cisco Catalyst 9800-CL Wireless Controller for Cloud Data Sheet*
- *Cisco Catalyst 9800-80 Wireless Controller Data Sheet*
- *Cisco Catalyst 9800-40 Wireless Controller Data Sheet*
- *Cisco Catalyst 9800-L Wireless Controller Data Sheet*

Cisco Embedded Wireless Controller on Catalyst Access Points

For more information about the Cisco Embedded Wireless Controller on Catalyst Access Points, see:

https://www.cisco.com/c/en/us/support/wireless/embedded-wireless-controller-catalyst-access-points/tsd-products-support-series-home.html

Wireless Product Comparison

- Compare specifications of Cisco wireless APs and controllers
- Wireless LAN Compliance Lookup
- Cisco AireOS to Cisco Catalyst 9800 Wireless Controller Feature Comparison Matrix

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 the Cisco Trust Portal.

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

Cisco Prime Infrastructure

Cisco Prime Infrastructure Documentation

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.