Release Notes for Cisco Catalyst 9800 Series Wireless Controller, Cisco IOS XE Amsterdam 17.3.x

First Published: 2020-08-10

Last Modified: 2023-10-30

Release Notes for Cisco Catalyst 9800 Series Wireless Controller, Cisco IOS XE Amsterdam 17.3.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 controllers use Cisco IOS XE software 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 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 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 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 controllers are supported by DevNet, either through community-based support or through DevNet developer support. For more information, go to https://developer.cisco.com.

Note For information about the recommended Cisco IOS XE releases for Cisco Catalyst 9800 Series Wireless Controllers, see the documentation at:

https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/214749-tac-recommended-ios-xe-builds-for-wirele.html

What's New in Cisco IOS XE Amsterdam 17.3.8a

There are no new features in this release.

This release only 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 Amsterdam 17.3.8

There are no new features in this release as it is a PSIRT only release.

What's New in Cisco IOS XE Amsterdam 17.3.7

Table 1: New and Modified Software Features

Feature Name	Description and Documentation Link
Secure Data Wipe	This feature allows you to securely erase files from the file system of the Cisco Access Points. For more information, see the chapter Secure Data Wipe.

What's New in Cisco IOS XE Amsterdam 17.3.6

This release includes critical bug fixes relating to scale and stability improvements.

Table 2: Software Features Introduced on Cisco Catalyst 9800 Series Wireless Controllers

Feature Name	Description and Documentation Link
Mesh and Mesh + Flex Support for Cisco Catalyst 9124AXE Outdoor Access Points	Mesh feature and Mesh + Flex feature is supported in Cisco Catalyst 9124AXE outdoor Access Points. For more information, see the chapter Mesh Access Points.
Mesh and Mesh + Flex Support for Cisco Catalyst 9124AXI/D Outdoor Access Points	Mesh feature and Mesh + Flex feature is supported in Cisco Catalyst 9124AXI/D outdoor Access Points. For more information, see the chapter Mesh Access Points.

Important Open issue: Slow TCP downloads and failing EAP-TLS are observed in Cisco IOS XE 17.3.6 - Cisco Aironet 2800, 3800, 4800, 1562, or Cisco Catalyst Industrial Wireless 6300 Heavy Duty Series Access Points (CSCwd37092).

To fix this issue, we recommend that you download APSP2 (CSCwd40096) which includes the above fix along with fixes for CSCvz99036 and CSCwc78435 while upgrading to Cisco IOS XE Amsterdam 17.3.6.

What's New in Cisco IOS XE Amsterdam 17.3.5b

This release includes few critical bug fixes from Cisco IOS XE Amsterdam 17.3.5a to improve stability.

What's New in Cisco IOS XE Amsterdam 17.3.5a

This release includes critical bug fixes relating to scale and stability improvements.

Table 3: Software Features Introduced on Cisco Catalyst 9800 Series Wireless Controllers

Feature Name	Description and Documentation Link
Support for SGT Inline Tagging Over Port-Channel Uplink	SGT inline tagging over port-channel uplink is supported in Cisco IOS XE Amsterdam 17.3.5a for Cisco Catalyst 9800-L Wireless Controller, Cisco Catalyst 9800-40 Wireless Controller, and Cisco Catalyst 9800-80 Wireless Controller. **Note** If you downgrade to the Cisco IOS XE releases that do not support SGT inline tagging over port-channel, the port-channel may be suspended. For more information, see the Cisco TrustSec chapter.
Cisco Catalyst 9124AXE Access Point	Cisco Catalyst 9124AXE Access Point is supported from this release. The supported regulatory domains are A, B, E, and Z.

Important Mesh features are not supported in Cisco Catalyst 9124 series APs, in Cisco IOS XE 17.3.5a and earlier releases.

Important **Known issue**: APs are unable to join the controller because of an invalid path MTU in the AP join request (CSCwb13784).

To fix this issue, apply the mandatory patch that has been released for all deployments having an MTU lower than 1500 bytes (for example, CAPWAP over WANs), regardless of the AP type. This recommendation could apply to local network scenarios. This hot patch does not require a controller reload.

The following are the image names for the SMU update:

- C9800-CL-universalk9.17.03.05a.CSCwb13784.SPA.smu.bin
- C9800-L-universalk9_wlc.17.03.05a.CSCwb13784.SPA.smu.bin
- C9800-universalk9_wlc.17.03.05a.CSCwb13784.SPA.smu.bin

You can download the software from the software download home page at:

https://software.cisco.com/download/home

The following products are supported:

- Catalyst 9800-L Wireless Controller
- Catalyst 9800-80 Wireless Controller
- Catalyst 9800-40 Wireless Controller
- Catalyst 9800-CL Wireless Controller for Cloud

For information about the SMU installation process, see:

https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/17-3/config-guide/b_wl_17_3_cg/m_smu_ewlc.html

What's New in Cisco IOS XE Amsterdam 17.3.4c

This release includes critical bug fixes found in 17.3.3 and 17.3.4 releases. Some of these fixes were previously released through Software Maintenance Upgrade (SMU) and AP Service Pack (APSP).

The supported regulatory domains for Cisco Catalyst 9124AXI/D Access Points are A, B, E, Q, Z, F, and R.

What's New in Cisco IOS XE Amsterdam 17.3.4

Table 4: Software Features Introduced on Cisco Catalyst 9800 Series Wireless Controllers

Feature Name	Description and Documentation Link
Cisco Catalyst 9124 Access Points	• Cisco Catalyst 9124AXD Access Points • Cisco Catalyst 9124AXI Access Points [1]

[1] These APs are supported only in US and Canada from Cisco IOS XE Amsterdam 17.3.4 release.

What's New in Cisco IOS XE Amsterdam 17.3.3

Table 5: Software Feature Introduced in Cisco Catalyst 9800 Series Wireless Controller, Cisco IOS XE Amsterdam, 17.3.3

Feature Name	Description and Documentation Link
Overlapping Client IP Address in Flex Deployment	This feature offers overlapping IP address across various flex sites and provides all the functionalities that are supported in flex deployments. For more information, see the Overlapping Client IP Address in Flex Deployment chapter.
Plug and Play Support for Cisco DNA Center Provisioning	From this release, the controller supports PnP feature, which allows for automated provisioning on DNA Center (DNAC 2.1.2.x release and above).

Feature Name	Description and Documentation Link
Smart Software Manager On-Prem (SSM On-Prem) Support for Smart Licensing Using Policy	SSM On-Prem is an asset manager, which works in conjunction with CSSM. It enables you to administer products and licenses on your premises instead of having to directly connect to CSSM. Here, a product instance is connected to SSM On-Prem, and SSM On-Prem becomes the single point of interface with CSSM. The product instance can be configured to *push* the required information to SSM On-Prem. Alternatively, SSM On-Prem can be set-up to *pull* the required information from a product instance at a configurable frequency. After usage information is available in SSM On-Prem, you must synchronize the same with CSSM, to ensure that the product instance count, license count and license usage information is the same on both, CSSM and SSM On-Prem. Offline and online options are available for synchronization between CSSM and SSM On-Prem. Minimum Required SSM On-Prem Version: Version 8, Release 202102 Minimum Required Cisco IOS XE Version: Cisco IOS XE Amsterdam 17.3.3 For more information, see the Smart Licensing Using Policy chapter and the Command Reference guide.

What's New in Cisco IOS XE Amsterdam 17.3.2a

Table 6: Software Features Introduced on Cisco Catalyst 9800 Series Wireless Controllers

Feature Name	Description and Documentation Link
Assurance and IoT Services Coexistence Without iCAP	From this release onwards, the controller supports deployment of both Cisco DNA Spaces IoT Services and Network Assurance on Cisco DNA Center. However, IoT Services and Intelligent Capture (iCAP) port configuration are still mutually exclusive. For more information, see IoT Services Management chapter.
AP Authorization Using Serial Number	From this release onwards, serial number authorization is applicable to all the access points. When serial-number authorization is enabled, the controller uses the top-assembly serial number for the authorization of the AP. For more information, see *Authorizing Access Points* section in Converting Autonomous Access Points to Lightweight Mode chapter.

Feature Name	Description and Documentation Link
OEAP Personal SSID Support	From this release onwards, the Cisco OfficeExtend Access Point (OEAP) supports personal SSID. This enables a local home client to use the same OEAP for local networking and internet connectivity. For more information, see *OEAP Personal SSID* section in FlexConnect chapter.
Smart Licensing Using Policy	An enhanced version of Smart Licensing, with the overarching objective of providing a licensing solution that does not interrupt the operations of your network, rather, one that enables a compliance relationship to account for the hardware and software licenses you purchase and use. With this licensing model, you do not have to complete any licensing-specific operations, such as registering or generating keys before you start using the software and the licenses that are tied to it. Only export-controlled and enforced licenses require Cisco authorization *before* use. License usage is recorded on your device with timestamps and the required workflows can be completed at a later date. Multiple options are available for license usage reporting – this depends on the topology you implement. You can use the Cisco Smart Licensing Utility (CSLU) Windows application, or report usage information directly to CSSM. A provision for offline reporting for air-gapped networks, where you download usage information and upload to CSSM, is also available. Starting with this release, Smart Licensing Using Policy is automatically enabled on the device. This is also the case when you upgrade to this release. By default, your Smart Account and Virtual Account in CSSM is enabled for Smart Licensing Using Policy. For more information, see the Smart Licensing Using Policy chapter.
Cisco DNA Center Support for Smart Licensing Using Policy	Cisco DNA Center supports Smart Licensing Using Policy functionality starting with Cisco DNA Center Release 2.2.2. The corresponding minimum required Cisco IOS XE Release for this platform is Cisco IOS XE Amsterdam 17.3.2a. Implement the “Connected to CSSM Through a Controller” topology to have Cisco DNA Center manage a product instance. When you do, the product instance records license usage, but it is the Cisco DNA Center that initiates communication with the product instance to retrieve and report usage to Cisco Smart Software Manager (CSSM), and returns the acknowledgement (RUM ACK). In order to meet reporting requirements, Cisco DNA Center provides ad hoc or on-demand reporting, as well as scheduled reporting options. For more information, see the Smart Licensing Using Policy chapter.

What's New in Cisco IOS XE Amsterdam 17.3.1

Table 7: Software Features Introduced on Cisco Catalyst 9800 Series Wireless Controllers

Feature Name	Description and Documentation Link
Access Point Audit Configuration	In this release, AP Audit Configuration feature helps to detect wireless service synchronization issues between the controller and AP. Two methods are implemented to support the AP audit configuration. The following commands were introduced: • **ap audit-report** • **show ap audit-report summary** • **show ap audit-report detail** For more information, see the AP Audit Configuration chapter.
Access Point Image Download Time Enhancement	This feature adds support to multiple sliding windows for control packets going from controller to AP. The following commands were introduced: • **capwap window size** • **show capwap client rcb** **Note** We recommend that you use this feature only for the teleworker solution. For more information, see the AP Image Download Time Enhancement chapter.
Access Point Support Bundle	You can now retrieve the support bundle information of an AP and export it to the controller or an external server. The AP support bundle contains core files, crash files, show run-configuration, configuration commands, msglog, and traplog. Until Cisco IOS XE 17.2.1 Release, you had to login to the AP console to retrieve the AP support-bundle information. The following commands were introduced: • **ap name export support-bundle mode** • **show ap support-bundle summary** For more information about Access Point Support Bundle, see AP Support Bundle chapter.
Application Visibility and Control support	From this release onwards, AVC is supported on Cisco Industrial Wireless 3702 Access Point.

Feature Name	Description and Documentation Link
BLE Management in the Controller	From this release onwards, you can enable the BLE radio configuration globally, manually configure gRPC token on the controller, and manually enable gRPC in the AP profile. The following commands were introduced: • **ap dot15 shutdown** • **ap cisco-dna token** • **cisco-dna grpc** • **show ap ble summary** • **show ap name ble detail** • **show ap grpc summary** • **show ap name grpc detail** For more information about BLE management in the controller, see BLE Management in the Controller chapter.
Cisco DNA Center Assurance Wi-Fi 6 [2]	The Cisco DNA Center Assurance Wi-Fi 6 dashboard provides a visual representation of the wireless network. In this release, commands to troubleshoot this network is introduced. • **statistics traffic-distribution** • **show wireless stats ap name traffic-distribution slot packet-count signal** • **show wireless stats ap name traffic-distribution slot airtime access-category** • **show wireless stats ap name traffic-distribution slot airtime traffic-type** • **show wireless stats ap name traffic-distribution slot latency access-category** For more information, see Cisco DNA Center Assurance Wi-Fi 6 Dashboard chapter.
Client Roaming Across Policy Profile	The controller allows seamless roaming between same WLAN associated with different policy profile. For more information, see The following command was introduced: • **wireless client vlan-persistant**

Feature Name	Description and Documentation Link
Support for Spectrum Intelligence in Cisco Catalyst 9115 AP	From this release, Spectrum Intelligence feature is supported on Cisco Catalyst 9115 Access Points. • **show cleanair interferers** • **show cleanair status** • **debug cleanair major** • **debug cleanair event** • **debug cleanair raw 10** For more information, see Spectrum Intelligence chapter.
Embedded Wireless on Cisco Catalyst 9000 Series Switches for Single Secure Site Deployment (Non-SDA)	The Cisco Integrated Wireless on Cisco Catalyst 9000 Series Switches is the next-generation Wi-Fi solution, combining the most advanced features of the Cisco Catalyst 9800 Series Wireless controller with the Catalyst 9000 series switches, creating a best-in-class wireless experience that provides enterprise-class resiliency, security, and IT simplicity for single site deployments. For more information, see Embedded Wireless on Cisco Catalyst 9000 Series Switches for Single Secure Site Deployment (Non-SDA) chapter.
Enable/Disable IW3702 Heaters	Cisco Industrial Wireless 3702 Access Point has two heaters that are enabled by default and will start to work when the environment temperature is under -20°C. If you determine that the environment temperature where the AP is deployed will never be under -20°C, you can turn off the heaters, which allows the APs to request less power from the device when the AP is powered by PoE+. To display the AP temperature, status, and the heater operational status you can use the following command. • **show ap name temperature**

Feature Name	Description and Documentation Link
Enhanced Certificate Management Through GUI	The Public Key Infrastructure (PKI) Management page now displays the following tabs: **Trustpoints** tab: Used to add, create or enroll a new trustpoint. This also displays the current Trustpoints configured on the controller and other details of the trustpoint. You can also see if the trustpoint is in use for any of the features. **CA Server** tab: Used to enable or disable the Certificate Authority (CA) server functionality on the controller. The CA server functionality should be enabled for the controller to generate a Self-Signed Certificate (SSC). **Key Pair Generation** tab: Used to generate key pairs. **Certificate Management** tab: Used to generate and manage certificates, and perform all certificate related operations, on the controller. For more information about certificate management, see Certificate Management chapter.
Enhanced Mesh Convergence	Mesh convergence allows MAPs to reestablish connection with the controller, when it loses backhaul connection with the current parent.
Ethernet Daisy Chain on Cisco Industrial Wireless 3702	The Cisco Industrial Wireless 3702 Access Points have the capability to daisy chain APs when they function as MAPs. The daisy chained MAPs can either operate the APs as a serial backhaul, allowing different channels for uplink and downlink access, thus improving backhaul bandwidth, or extend universal access. The following command was introduced: • **ssid broadcast persistent**
External Modules	External module enables traffic to flow in and out from the Cisco Aironet Developer Platform module, when an AP is in both local and flex connect mode. In this release, the following command was introduced: • **remote-lan rlan-profile policy rlan-policy ext-module** For more information on configuring external modules, see RLAN External Module chapter.

Feature Name	Description and Documentation Link
Flexible Antenna Port Configuration for Cisco Industrial Wireless 3702	The presence of multiple antennas on the transmitters and the receivers of APs results in better performance and reliability of the APs. The following commands were introduced: • **ap name antenna-band-mode** • **show ap general config** For more details, see Cisco Flexible Antenna Port chapter.
gNMI Configuration Persistence	The gNMI Configuration Persistence feature ensures that all successful configuration changes made through gNMI SET persists in the configuration after a device restart.
Hotspot 2.0 Updates	The Hotspot 2.0 R3 has added options such as new ANQP elements, Terms & Conditions, and integration of OSEN security and WPA2 security on the same SSID: The following commands were introduced: • **advice-charge** • **eap-method** • **inner-auth-eap** • **inner-auth-non-eap** • **nai-realm** • **plan** • **terms-conditions** • **tunneled-eap-credential** • **url** • **vlan-name** • **vlan-id** • **vlan encryption osen** For more information on the Hotspot 2.0 feature enhancements, see Hotspot 2.0 chapter.

Feature Name	Description and Documentation Link
HTTP and HTTPS Requests for Web Authentication	From Cisco IOS XE Amsterdam 17.3.1 onwards, to control the HTTP and HTTPS requests sent to the web authentication module, new commands that are listed below are introduced under the global parameter map parameters. The following commands were introduced: • **secure-webauth-disable** • **webauth-http-enable** For more information, see Configuring HTTP and HTTPS Requests for Web Authentication section.
IoT Module Management in the Controller	The IoT Module Management solution uses the USB interface on the Cisco Catalyst 9105AXI, 9105AXW, 9115AX, 9117AX, 9120AX, and 9130AX series Access Points, to connect to the IoT connector. These APs host the third party application software components, that act as containers. Cisco DNAC helps in the provisioning, deployment, and in controlling the container applications on the APs. The controller and the APs are managed by Cisco DNAC. You can connect the USB modules to the APs, then login to the controller and run the commands to enable the USB and Cisco IOx application to the APs associated in the AP profile group. The following commands were introduced: • **ap dot15 shutdown** • **ap cisco-dna token** • **cisco-dna grpc** • **show ap ble summary** • **show ap name ble detail** • **show ap grpc summary** • **show ap name grpc detail** For more information, see IoT Module Management in the Controller chapter.
Mesh - 2.4 GHz Mesh Backhaul	In certain countries, you might prefer to use 2.4 GHz radio frequencies to achieve much larger mesh or bridge distances. For more information, see Mesh Access Points chapter.
Mesh Off Channel Background Scanning	This release supports off channel background scanning for Mesh APs. For more information, see Mesh Access Points chapter.

Feature Name	Description and Documentation Link
Multicast Filtering	In this release, the Multicast Filtering feature is supported on Layer 3 for IPv6. When you enable this feature, the APs will stop forwarding multicast packets to the clients. For more information, see the Multicast Filtering chapter.
Address Resolution Protocol (ARP) and Neighbor Discovery (ND) Proxy	Neighbor Discovery (ND) Proxy is the ability of the controller to respond to the Neighbor Solicitation packet destined to the wireless clients. The following commands were introduced: • **ipv4 arp-proxy** • **ipv6 nd proxy** For more information, see the IPv6 Client IP Address Learning chapter.
OFDMA in Cisco Catalyst 9130 APs	Both Uplink and Downlink Orthogonal frequency-division multiple access (UL OFDMA and DL OFDMA) features are supported in Cisco Catalyst 9130 APs in this release. • Currently limited to support eight users in a DL OFDMA or UL OFDMA transmission. • In this release, 37 users are supported in the 80-MHz and 160-MHz bandwidths.
Retain Client for 10 seconds after delete	The controller retains client session for 10 seconds instead of immediately deleting for few clients. This feature is applicable for run state clients, if any client status shows as controller IPLEARN or Authenticating, that client entry will be removed from the controller and only run state clients will be moved to idle state. This is supported on central authentication with local and flex mode enabled. You must execute the following commands to view the clients in idle state. • **show wireless stats client detail** • **show wireless client summary**

Feature Name	Description and Documentation Link
Rogue Containment and AP Impersonation Detection based on AP Authentication	In Cisco IOS XE Amsterdam 17.3.1 Release, a rogue device that is enabled with 802.11w Protected Management Frames (PMF) is not contained. Instead, the rogue device is marked as *Contained Pending* and a wireless service assurance (WSA) alarm is raised to inform about the event. As the device containment is not performed, AP resources are not consumed unnecessarily. The AP Authentication feature allows you to detect AP impersonation. When you enable this feature, the controller creates an AP domain secret and shares it with other APs in the same network. This allows the APs to authenticate each other. Also, this is enhanced using two other methods: • Checking channel of the rogue in the DS Parameter set and matching it with Managed APs channels. • Using Infrastrucure MFP to check the message integrity check. The following command was introduced: • **show wireless wps rogue ap detailed** For more information, see Managing Rogue Devices chapter.
Standby Monitoring	Standby Monitoring feature allows to monitor the Health of the Standby controller directly from the Standby, without going through the Active controller. The following commands are introduced: • **show processes cpu** • **show environment summary** For more information, see the High Availability chapter.
Support for Cisco Catalyst 9105 Series APs	Support is added for Cisco Catalyst 9105I and 9105W APs in this release.
Support for Configuring SR-IOV for KVM and VMware ESXi Environments	Starting with this release, SR-IOV can be configured on KVM and ESXi environments. For more information on configuring SR-IOV for KVM and ESXi, see the following sections: • Installing the Controller in KVM Environment • Installing Controller in VMware Environment

Feature Name	Description and Documentation Link
Cisco User Defined Network (UDN) Mobile Application	The Cisco User Defined Network (UDN) mobile application helps create a user defined network and restrict access to devices unless they are invited to share the network. For more information, see User Guide for Cisco User Defined Network Mobile Application.
Support for Configuring High Throughput Templates on Cisco Catalyst 9800-CL Cloud Wireless Controller	From 17.3 release onwards, high throughput templates can be configured on the Cisco Catalyst 9800-CL Cloud Wireless Controller private cloud instances. With this enhancement, the throughput can be raised from 2 Gbps to 5 Gbps. For information on the supported templates and hardware requirements, see Table 9: Supported Templates and Hardware Requirements.
Syslog Support for Client State Change	The Syslog Support for Client State Change feature enables you to track the client details such as IP addresses, AP names, and so on. The following commands was introduced: • **wireless client syslog-detailed**
Support for Direct-Sequence (DS) Parameter Set	The managed APs will now have additional information about the DS Parameter Set of the detected Rogue AP, in the Rogue AP reports. If an impersonation attack is detected, the controller checks if the reported DS channel matches with one of the recent channels used by the managed APs. If a match is not found, a DS channel attack alarm is raised through the wireless service assurance (WSA) impersonation alarm.
Tri-Radio (Dynamic)	Support for Dual Radio role is added to the Tri-Radio feature. This feature enables FRA to dynamically choose between dual radio and tri-radio mode and determine the radio role as client-serving or monitor for the individual radios. For more information, see Cisco Access Points with Tri-Radio chapter.

Feature Name	Description and Documentation Link
Uplink MU-MIMO in Cisco Catalyst 9130 APs	Uplink Multi-user multiple-input and multiple-output (UL MU MIMO) feature is supported in Cisco Catalyst 9130 APs in this release. • Conceptually similar to Downlink MU-MIMO, which is already supported in Cisco Catalyst 9130 APs. • Allows multiple clients to send traffic simultaneously, thus saving air time. • Controller by AP through triggers sent to clients. • Supported in 20-MHz, 40-MHz, and 80-MHz bandwidths, but not supported in the 160-MHz bandwidth. • Supported only in the 5-GHz band. • Currently limited to support three users. When more than three users are connected, UL MU-MIMO scheduling does not occur, and the AP falls back to single-user (SU) transmission.
User Defined Network	A user defined network (UDN) is a solution that is aimed at providing secure and remote on-boarding of devices in shared service environments like dormitory rooms, resident halls, class rooms and auditoriums. For more information, see the User Defined Network chapter.
WIPS: Advanced Security Enhancements	The following WIPS alarms were included in this release: • Denial-Of-Service Attack: Request-To-Send Flood • Denial-Of-Service Attack: Clear-To-Send Flood

[2] In conjunction with DNA Center version 2.1.2

Table 8: Web UI Features Introduced or Modified on Cisco Catalyst 9800 Series Wireless Controllers

Feature Name	Web UI Path
Dark Mode option	You can enable Dark Mode in the GUI. Dark Mode (screen with light text in a dark background) is best suited for reducing eye strain, especially in low-light conditions. Screen glare and flickering is also reduced. Click the Preferences icon (the gear icon) > Dark Mode option
Download AP support bundle from the GUI	Configuration > Wireless > Access Points > Edit AP

Feature Name	Web UI Path
Enhanced Certificate Management Through the GUI	Configuration > Security > PKI Management
Embedded Wireless on Cisco Catalyst 9000 Series Switches for Single Secure Site Deployment (Non-SDA)	Configuration > Embedded Wireless Setup
Open Roaming	Configuration > Wireless > Hotspot/OpenRoaming
Software Upgrade page enhancement	Administration > Software Management > Software Upgrade
Tracking of appliance temperature in the System Information dashlet	Cisco Catalyst 9800 Wireless Controller GUI Dashboard
Tri-Radio (Dynamic)	• Configuration > Radio Configurations > Network • Configuration >Wireless > Access Points

Table 9: Supported Templates and Hardware Requirements

Model Configuration	Small (Low Throughput)	Medium (Low Throughput)	Large (Low Throughput)	Small (High Throughput)	Medium (High Throughput)	Large (High Throughput)
Minimum number of vCPUs (Hyperthreading is not supported)	4	6	10	7	9	13
Minimum CPU Allocation (MHz)	4,000	6,000	10, 000	4000	6000	10,000
Minimum Memory (GB)	8	16	32	8	16	32
Required Storage (GB)	16	16	16	16	16	16
Virtual NICs (vNIC) (*) 3rd NIC for High Availability	2/(3)*	2/(3)*	2/(3)*	2/(3)*	2/(3)*	2/(3)*

MIBs

The following MIBs were modified.

- CISCO-LWAPP-AP-MIB.my
  - Added the following scalar objects:
    - cLApGlobalAPAuditReport
    - cLApGlobalAPAuditReportInterval
  - Added following objects to the cLApProfileEntry table:
    - cLApProfilePersistentSsidBroadcastEnable
    - cLApProfileDhcpFallback
- CISCO-LWAPP-DOT11-CLIENT-CALIB-MIB.my
- CISCO-LWAPP-DOT11-CLIENT-MIB.my

- CISCO-LWAPP-DOT11-MIB.my
- CISCO-LWAPP-WLAN-SECURITY-MIB.my
- CISCO-WIRELESS-HOTSPOT-MIB.my
- CISCO-LWAPP-REAP-MIB.my
- CISCO-LWAPP-WLAN-MIB.my
  - cLWlanWifiDirectPolicyStatus: The following policy value was added.
    - xconnectNotAllow

Compliance with Pyang

Some models are not fully compliant with all IETF guidelines as exemplified by running the pyang tool with the `--lint` flag. The errors and warnings exhibited by running pyang with the `--lint`flag are currently deemed to be non-critical as they do not impact the semantic of the models or prevent the models being used as part of tool chains. A script has been provided, "check-models.sh", that runs pyang with `--lint` validation enabled, but ignoring certain errors. This allows the developer to determine what issues may be present.

As part of the model validation for this release we are ignoring "LEAFREF_IDENTIFIER_NOT_FOUND" and "STRICT_XPATH_FUNCTIONS" error types. Reason being that the missing leafref reference errors are due to pyang bug which needs to be fixed and some of the XPATH function errors are false positives which are handled in the newer version of pyang (2.3.2)

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.

Behavior Change

- From Cisco IOS XE Amsterdam 17.3.5a onwards, rate limiting is performed for ARP packets for each client to prevent a denial-of-service attack. If a client sends an ARP storm, then the client is excluded. To configure rate limiting, use the **ip arp-limit rate** command at the policy profile level.
- Cisco CleanAir feature is supported on the Cisco Catalyst 9120AXE Access Points from Cisco IOS XE Amsterdam Release 17.3.x.
- In-Service Software Upgrade (ISSU) feature is supported officially from this release.
- If a switchover occurs while performing Rolling AP Upgrade during ISSU, the Rolling Upgrade process will restart automatically after the switchover.
- From Cisco IOS XE Amsterdam 17.3.1 onwards, 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.
- From Cisco IOS XE Amsterdam 17.3.1 onwards, higher number of port channels are supported on the following Cisco Catalyst 9800 Series Wireless Controllers:
  - Cisco Catalyst 9800-80 Wireless Controller: From 1-40 to 1-64
  - Cisco Catalyst 9800-40 Wireless Controller: From 1-4 to 1-16
  - Cisco Catalyst 9800-L Wireless Controller: From 1-6 to 1-14

  If you downgrade from Cisco IOS XE Amsterdam 17.3.1 to an earlier release, the port channels that are configured with higher range will disappear.
- From Cisco IOS XE Amsterdam 17.3.1 onwards, the AP name can only be up to 32 characters.
- When EoGRE AAA-proxy is used, AAA ports are set to 1645 and 1646 by default. To change this port configuration, use the following command: **tunnel eogre interface** *tunnel-intf* **aaa proxy key** *key key-name* **auth-port** *auth_port* **acct-port** *acct_port*
- Mobility Tunnel will go down and come up if SSO is triggered due to gateway check failure.
- Adding support for the LED blink in Cisco Catalyst 9800 Wireless Controllers.
- Log viewer window added to the GUI, to view radioactive trace logs.

- New field is added to display AP configuration state in the GUI.
- Column header in rogue detection changed from MFP Required to PMF Required.
- The **Central Forwarding** field that was present in the **EoGRE** > **Tunnel Profiles** > **Edit Tunnel Profile** > **General** tab, has been removed.
- From Cisco IOS XE Amsterdam 17.3.1, the LED Flash configuration under AP profile is deprecated. The following command is deprecated: **ledflash** { **duration** | **indefinite** }. To enable or disable LED Flash, use the **ap name led flash** command in the Privileged EXEC mode.
- From Cisco IOS XE Amsterdam 17.3.1 onwards, the command **ap country** is deprecated and renamed as **wireless country** *<1 country code>*, where you can enter country codes for more than 20 countries. Although the existing command **ap country** is still functional, it is recommended that you use the **wireless country** *<1 country code>* command.
- Windows 10 cannot be connected using Intel chipset series such as 260, 9560, AX200, AX201, and AX210 to a WLAN configured with security WPA3 or WPA2 with Protected Management Frames (PMF) requirements. This is a limitation in Windows and is only fixed in Windows version 21H2.
- To migrate public IP address from 16.12.x to 17.x. ensure that you configure the **service internal** command. Failing to do so will not carry forward the IP address.

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 12: Supported PIDs and Ports, on page 24 for the list of supported modules.)

Table 10: 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 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 1-rack unit space and provides four 1-GE or 10-GE uplink ports.

Platform	Description
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 ESXi, KVM, Microsoft Hyper-V, and NFVIS on ENCS hypervisors), or in the public cloud as Infrastructure as a Service (IaaS) in Amazon Web Services (AWS) and Google Cloud Platform (GCP) marketplace.
Cisco Catalyst 9800 Embedded Wireless Controller for Switch	The Catalyst 9800 Wireless Controller software for the Cisco Catalyst 9000 switches bring the wired and wireless infrastructure together with consistent policy and management. This deployment model supports only SD Access, which is a highly secure solution for small campuses and distributed branches.
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.

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

Table 11: Supported Host Environments for Public and Private Cloud

Host Environment	Software Version
VMware ESXi	• VMware ESXi vSphere 6.0, 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, 8.2, and 8.5 • Ubuntu 14.04.5 LTS, Ubuntu 16.04.5 LTS
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)

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 RP port of C9800-80-K9 and C9800-40-K9.

Table 12: 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. The following SFPs are supported: • GLC-BX-D • GLC-BX-U • GLC-EX-SMD • GLC-LH-SMD • GLC-SX-MMD • GLC-ZX-SMD • GLC-TE
	The following enhanced SFPs are supported: • SFP-10G-AOC1M • SFP-10G-AOC2M • SFP-10G-AOC3M • SFP-10G-AOC5M • SFP-10G-AOC7M • SFP-10G-AOC10M • SFP-10G-SR • SFP-10G-SR-S • SFP-10G-SR-X • SFP-10G-ER • SFP-10G-ZR • SFP-H10GB-ACU7M • SFP-H10GB-ACU10M • DWDM-SFP10G-30.33 • DWDM-SFP10G-61.41

Controller Model	Description
	The following QSFP+s are supported: • QSFP-40G-SR4 • QSFP-40G-LR4 • QSFP-40GE-LR4 • QSFP-40G-ER4 • QSFP-40G-SR4-S • QSFP-40G-LR4-S • QSFP-40G-SR-BD • QSFP-40G-BD-RX • QSFP-100G-SR4-S • QSFP-100G-LR4-S
C9800-40-K9	Four 1/10-Gigabit Ethernet SFP or SFP+ ports and two power supply slots The following SFPs are supported: • GLC-BX-D • GLC-BX-U • GLC-LH-SMD • GLC-SX-MMD • GLC-EX-SMD • GLC-ZX-SMD • GLC-TE

Controller Model	Description
	The following enhanced SFPs are supported: • SFP-10G-AOC1M • SFP-10G-AOC2M • SFP-10G-AOC3M • SFP-10G-AOC5M • SFP-10G-AOC7M • SFP-10G-AOC10M • SFP-10G-SR • SFP-10G-SR-S • SFP-10G-SR-X • SFP-10G-ER • SFP-10G-ZR • SFP-H10GB-ACU7M • SFP-H10GB-ACU10M • DWDM-SFP10G-30.33 - DWDM-SFP10G-61.41
C9800-L-C-K9	• 4x2.5/2-Gigabit ports • 2x10/5/2.5/1-Gigabit ports The following SFPs are supported: • GLC-BX-D • GLC-BX-U • GLC-LH-SMD • GLC-SX-MMD • GLC-ZX-SMD • GLC-TE

Controller Model	Description
C9800-L-F-K9	• 4x2.5/2-Gigabit ports • 2x10/1-Gigabit ports The following SFPs are supported: • GLC-BX-D • GLC-BX-U • GLC-SX-MMD • GLC-ZX-SMD • GLC-TE • SFP-10G-SR • SFP-10G-SR-S • SFP-10G-SR-X • SFP-H10GB-ACU7M • SFP-H10GB-ACU10M

Optics Modules

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

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 17.3.6
  - VID 03 or earlier - supported in all 17.3.x releases
- Cisco Catalyst 9105AXW Access Points
  - VID 02 or later - supported from 17.3.6
  - VID 01 or earlier - supported in all 17.3.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 17.3.6
  - VID 06 or earlier - supported in all 17.3.x releases
- Cisco Catalyst 9120AXP Access Points
- Cisco Catalyst 9130AX (I/E) Access Points
  - VID 03 or later - supported from 17.3.6
  - VID 02 or earlier - supported in all 17.3.x releases

(For information about Cisco Catalyst 9105, 9120, or 9130 Access Points version support, see the Field Notice 72424.)

- Cisco Aironet 1700 Series Access Points
- Cisco Aironet 1800I, 1815 (I/W), 1830 (I), 1840 (I), and 1850 (I/E) Access Points
- Cisco Aironet 2700 Series Access Points
- Cisco Aironet 2800 (I/E) Series Access Points
- Cisco Aironet 3700 Series Access Points
- Cisco Aironet 3800 (I/E/P) Series Access Points
- Cisco Aironet 4800 Series Access Points

Outdoor Access Points

- Cisco Aironet 1540 Access Points
- Cisco Aironet 1560 Series Access Points
- Cisco Aironet 1570 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 9124AXI Access Points - supported from 17.3.4
- Cisco Catalyst 9124AXD Access Points - supported from 17.3.4
- Cisco Catalyst 9124AXE Access Points - supported from 17.3.5a

Note Do not enable Efficient Image Download feature on controllers running Cisco IOS XE Amsterdam 17.3.x when there are Cisco Catalyst 9124AX and Cisco Catalyst 9130AX APs in the same group.

Integrated Access Points

- Integrated Access Point on Cisco 1100 ISR

Network Sensor

- Cisco Aironet 1800s Active Sensor

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. For more information, see Cisco Wireless Solutions Software Compatibility Matrix

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 CMX
Amsterdam 17.3.8	3.1 3.0 2.7 2.6 2.4	3.10.1 3.9.1 3.9 3.8.1	8.10.196.0 8.10.190.0 8.10.185.0 8.10.171.0 8.10.162.0 8.10.160.0 8.10.151.0 8.10.142.0 8.10.130.0 8.8.130.0 8.8.125.0 8.8.120.0 8.8.111.0 8.5.182.104 8.5.176.2 8.5.164.216	See Cisco Catalyst Center Compatibility Information	10.6.2 10.6 10.5.1

Cisco Catalyst 9800 Series Wireless Controller Software	Cisco Identity Services Engine	Cisco Prime Infrastructure	Cisco AireOS-IRCM Interoperability	Cisco Catalyst Center	Cisco CMX
Amsterdam 17.3.7	3.1 3.0 2.7 2.6 2.4	3.10.1 3.9.1 3.9 3.8.1	8.10.171.0 8.10.162.0 8.10.160.0 8.10.151.0 8.10.142.0 8.10.130.0 8.8.130.0 8.8.125.0 8.8.120.0 8.8.111.0 8.5.182.104 8.5.176.2 8.5.164.216	See Cisco Catalyst Center Compatibility Information	10.6.2 10.6 10.5.1
Amsterdam 17.3.6	3.1 3.0 2.7 2.6 2.4	3.10.1 3.9.1 3.9 3.8.1	8.10.171.0 8.10.162.0 8.10.160.0 8.10.151.0 8.10.142.0 8.10.130.0 8.8.130.0 8.8.125.0 8.8.120.0 8.8.111.0 8.5.182.104 8.5.176.2 8.5.164.216	See Cisco Catalyst Center Compatibility Information	10.6.2 10.6 10.5.1

Cisco Catalyst 9800 Series Wireless Controller Software	Cisco Identity Services Engine	Cisco Prime Infrastructure	Cisco AireOS-IRCM Interoperability	Cisco Catalyst Center	Cisco CMX
Amsterdam 17.3.5b	3.1 3.0 2.7 2.6 2.4	3.10.1 3.9.1 3.9 3.8.1	8.10.171.0 8.10.162.0 8.10.160.0 8.10.151.0 8.10.142.0 8.10.130.0 8.8.130.0 8.8.125.0 8.8.120.0 8.8.111.0 8.5.182.104 8.5.176.2 8.5.164.216 8.5.164.0	See Cisco Catalyst Center Compatibility Information	10.6.2 10.6 10.5.1
Amsterdam 17.3.5a	3.1 3.0 2.7 2.6 2.4	3.10.1 3.9.1 3.9 3.8.1	8.10.171.0 8.10.162.0 8.10.160.0 8.10.151.0 8.10.142.0 8.10.130.0 8.8.130.0 8.8.125.0 8.8.120.0 8.8.111.0 8.5.182.104 8.5.176.2 8.5.164.216 8.5.164.0	See Cisco Catalyst Center Compatibility Information	10.6.2 10.6 10.5.1

Cisco Catalyst 9800 Series Wireless Controller Software	Cisco Identity Services Engine	Cisco Prime Infrastructure	Cisco AireOS-IRCM Interoperability	Cisco Catalyst Center	Cisco CMX
Amsterdam 17.3.4c	3.0 2.7 2.6 2.4	3.9.1 3.9 3.8.1	8.10.171.0 8.10.162.0 8.10.160.0 8.10.151.0 8.10.142.0 8.10.130.0 8.8.130.0 8.8.125.0 8.8.120.0 8.8.111.0 8.5.176.0 8.5.164.0	See Cisco Catalyst Center Compatibility Information	10.6.2 10.6 10.5.1
Amsterdam 17.3.4	3.0 2.7 2.6 2.4	3.9.1 3.9 3.8.1	8.10.171.0 8.10.162.0 8.10.160.0 8.10.151.0 8.10.142.0 8.10.130.0 8.8.130.0 8.8.125.0 8.8.120.0 8.8.111.0 8.5.176.0 8.5.164.0	See Cisco Catalyst Center Compatibility Information	10.6.2 10.6 10.5.1

Cisco Catalyst 9800 Series Wireless Controller Software	Cisco Identity Services Engine	Cisco Prime Infrastructure	Cisco AireOS-IRCM Interoperability	Cisco Catalyst Center	Cisco CMX
Amsterdam 17.3.3	2.7 2.6 2.4	3.9 3.8.1	8.10.171.0 8.10.162.0 8.10.151.0 8.10.142.0 8.10.130.0 8.8.130.0 8.8.125.0 8.8.120.0 8.8.111.0 8.5.164.0 8.5.182.104 8.5.152.103 8.5.164.216 8.5.176.2	See Cisco Catalyst Center Compatibility Information	10.6.2 10.6 10.5.1
Amsterdam 17.3.2a	2.7 2.6 P6 2.4	3.8.1	8.10.171.0 8.10.162.0 8.10.151.0 8.10.142.0 8.10.130.0 8.8.130.0 8.8.125.0 8.8.120.0 8.8.111.0 8.5.164.0 8.5.182.104 8.5.152.103 8.5.164.216 8.5.176.2	See Cisco Catalyst Center Compatibility Information	10.6.2 10.6 10.5.1

Cisco Catalyst 9800 Series Wireless Controller Software	Cisco Identity Services Engine	Cisco Prime Infrastructure	Cisco AireOS-IRCM Interoperability	Cisco Catalyst Center	Cisco CMX
Amsterdam 17.3.1	2.7 2.6 P6 2.4	3.8.1	8.10.171.0 8.10.162.0 8.10.142.0 8.10.130.0 8.10.122.0 8.10.121.0 8.10.113.0 8.10.112.0 8.10.105.0 8.9.111.0 8.9.100.0 8.8.125.0 8.8.120.0 8.8.111.0 8.5.164.0 8.5.182.104 8.5.152.103 8.5.164.216 8.5.176.2	See Cisco Catalyst Center Compatibility Information	10.6.2 10.6 10.5.1

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[3]	512 MB[4]	256	1280 x 800 or higher	Small

[3] We recommend 1 GHz.

[4] 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:

- When you upgrade from Cisco IOS XE Dublin 17.12.3 to 17.12.4 or Cisco IOS XE 17.15.1, the Cisco Catalyst Wi-Fi 6 APs fail to upgrade the AP image.

  Workaround:

  - Reboot the impacted APs through the power cycle.

  For more information, see CSCwm08044

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, 17.14.x, and 17.15.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.

- The controller reloads automatically when a cold patch is applied using web UI. This behavior is applicable to 17.3.x and 17.6.x releases.
- 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 the Cisco Catalyst 9800-80 Wireless Controller to Cisco IOS XE Amsterdam 17.3.4 using BUNDLE mode, ensure that the ROMMON version is 16.12.5r. Otherwise, the controller gets stuck in a boot loop. We recommend that you upgrade the ROMMON version to 16.12.5r, even for the INSTALL mode upgrade. Note that this recommendation is not applicable to other versions of the Cisco Catalyst 9800 Wireless Controller.

  For information about how to upgrade the ROMMON, see the "Upgrading Field Programmable for Cisco Catalyst 9800-80 Wireless Controller" section of the Upgrading Field Programmable Hardware Devices for Cisco Catalyst 9800 Series Wireless Controllers 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.

- If you have configured FIPS mode, ensure that you remove the **security wpa wpa1 cipher tkip** command configuration from WLANs before upgrading to Cisco IOS XE Amsterdam 17.3.x from an earlier version. Failure to do so will set the WLAN security to TKIP, which is not supported in FIPS mode. After the upgrade, reconfigure WLAN with AES.
- The Cisco Catalyst 9800 devices running Cisco IOS XE Amsterdam 17.3.1 can either support the BLE solution with Cisco Spaces, or the Network Assurance solution with Cisco DNA Center. The Network Assurance (including iCAP) and BLE solution are mutually exclusive. That is, if Network Assurance or iCAP has to be enabled on a device, the BLE solution cannot be deployed. In the same way, if the BLE solution has to be enabled on a device, Network Assurance and iCAP cannot be deployed.
- 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.
- When you configure the Cisco Catalyst 9800 Series Wireless controllers with Cisco Aironet 3700 Series Access Points through IPv6, and then connect the IPv6-capable clients, the IP addresses of all the IPv6 clients are not updated on the controller.
- 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
    - HTTP
    - HTTPS
    - Licensing for Smart Licensing feature to communicate with CSSM
    - SSH
- 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.

- The Cisco Catalyst 9800 Wireless Controller might reload if downgraded from 17.x to 16.12.4a. To avoid this, we recommend that you downgrade to Cisco IOS XE Gibraltar 16.12.5 instead of 16.12.4a.

Note It is recommended to do the following:

- Disable Spectrum Intelligence on Cisco Catalyst 9115 Access Points.
- Disable BSS colouring feature on the controller.

- It is not possible to shut down the WLAN policy profile when you downgrade from Cisco IOS XE Amsterdam 17.3.x (supporting local switching IPv6 AVC) to Cisco IOS XE Gibraltar 16.12.x (where local switching IPv6 AVC is not supported). In such instances, we recommend that you delete the existing WLAN policy profile and create a new one.
- The following access points may encounter stability issues when you upgrade to Cisco IOS XE Amsterdam 17.3.4:
  - Cisco Aironet 1562 APs
  - Cisco Aironet 2800 Series APs
  - Cisco Aironet 3800 Series APs
  - Cisco Aironet 4800 Series APs
  - Cisco Catalyst IW6300 DC Heavy Duty Access Point

  To avoid stability issues, we recommend you upgrade to Cisco IOS XE Amsterdam 17.3.4 and install AP Service Pack (APSP). For more information, see the *Information About Per Site or Per AP Model Service Pack* section in Software Maintenance Upgrade chapter.

Note The AP stability issue is not applicable to Cisco IOS XE Amsterdam 17.3.7 and later releases.

- 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 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 Amsterdam 17.3.x

Table 15: Upgrade Path to Cisco IOS XE Amsterdam 17.3.x Release

Current Software	Upgrade Path to Cisco IOS XE Amsterdam 17.3.x Release
16.10.x	Upgrade first to 16.12.5 and then to 17.3.x.

Current Software	Upgrade Path to Cisco IOS XE Amsterdam 17.3.x Release
16.11.x	Upgrade first to 16.12.5 and then to 17.3.x.
16.12.x	You can upgrade directly to 17.3.x.
17.1.x	You can upgrade directly to 17.3.x.
17.2.x	You can upgrade directly to 17.3.x.

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 Amsterdam 17.3.x
- **Image**: Universal
- **File Name**: C9800-universalk9_wlc.17.3.x.SPA.bin

Software Installation Commands

Cisco IOS XE Amsterdam 17.3.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

This section provides information about the licensing packages for the features that are available in the Cisco Catalyst 9800 Series Wireless Controller.

The software features that are available on the controller fall under these license categories:

- AIR DNA Essentials (AIR-DNA-E)
- AIR DNA Advantage (AIR-DNA-A) (Includes the features that are available with the Cisco DNA Essentials license and more.)

Note The controller starts with *AIR-DNA-A* as the default. Any change in the license level requires a reboot.

Note After adding new license in the Cisco Smart Software Manager (CSSM) for customer virtual account, run the **license smart renew auth** command on the controller to get the license status changed from Out OF Compliance to Authorized.

Base Licenses

Base licenses are perpetual licenses and can be used even after the expiry of *Air-DNA-A* and *AIR-DNA-E*. Base licenses include:

- AIR Network Essentials (AIR-NE)
- AIR Network Advantage (AIR-NA) (Includes the features that are available in the Network Essentials license.)

License Term

The licenses are available for a three, five, or seven-year periods.

For a more detailed overview on Cisco Licensing, go to 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 Amsterdam 17.3.x
Cisco Wireless Controller	See Supported Hardware, on page 22
Access Points	See Supported APs, on page 27.
Radio	• 802.11ax • 802.11ac • 802.11a • 802.11g • 802.11n
Security	Open, PSK (WPA2-AES), 802.1X (WPA2-AES) (EAP-FAST, EAP-TLS) 802.11ax
RADIUS	See Compatibility Matrix, on page 29.

Hardware or Software Parameter	Hardware or Software Type
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
Wi-Fi 6 Devices (Mobile Phone and Laptop)	
Apple iPhone 11	iOS 14.1
Apple iPhone SE 2020	iOS 14.1
Dell Intel AX1650w	Windows 10 (21.90.2.1)
Dell Latitude 5491 (Intel AX200)	Windows 10 Pro (21.40.2)
Samsung S20	Android 10
Samsung S10 (SM-G973U1)	Android 9.0 (One UI 1.1)
Samsung S10e (SM-G970U1)	Android 9.0 (One UI 1.1)
Samsung Galaxy S10+	Android 9.0
Samsung Galaxy Fold 2	Android 10
Samsung Galaxy Flip Z	Android 10
Samsung Note 20	Android 10
Laptops	
Acer Aspire E 15 E5-573-3870 (Qualcomm Atheros QCA9377)	Windows 10 Pro (12.0.0.832)
Apple Macbook Air 11 inch	OS Sierra 10.12.6
Apple Macbook Air 13 inch	OS Catalina 10.15.4
Apple Macbook Air 13 inch	OS High Sierra 10.13.4
Macbook Pro Retina	OS Mojave 10.14.3
Macbook Pro Retina 13 inch early 2015	OS Mojave 10.14.3
Dell Inspiron 2020 Chromebook	Chrome OS 75.0.3770.129
Google Pixelbook Go	Chrome OS 84.0.4147.136
HP chromebook 11a	Chrome OS 76.0.3809.136
Samsung Chromebook 4+	Chrome OS 77.0.3865.105
Dell Latitude 3480 (Qualcomm DELL wireless 1820)	Win 10 Pro (12.0.0.242)

Client Type and Name	Driver or Software Version
Dell Inspiron 15-7569 (Intel Dual Band Wireless-AC 3165)	Windows 10 Home (18.32.0.5)
Dell Latitude E5540 (Intel Dual Band Wireless AC7260)	Windows 7 Professional (21.10.1)
Dell XPS 12 v9250 (Intel Dual Band Wireless AC 8260)	Windows 10 (19.50.1.6)
Dell Latitude 5491 (Intel AX200)	Windows 10 Pro (21.40.2)
Dell XPS Latitude12 9250 (Intel Dual Band Wireless AC 8260)	Windows 10 Home (21.40.0)
Lenovo Yoga C630 Snapdragon 850 (Qualcomm AC 2x2 Svc)	Windows 10 (1.0.10440.0)
Lenovo Thinkpad Yoga 460 (Intel Dual Band Wireless-AC 9260)	Windows 10 Pro (21.40.0)
Note For clients using Intel wireless cards, we recommend that you to update to the latest Intel wireless drivers if the advertised SSIDs are not visible.	
Tablets	
Apple iPad Pro	iOS 13.5
Apple iPad Air2 MGLW2LL/A	iOS 12.4.1
Apple iPad Mini 4 9.0.1 MK872LL/A	iOS 11.4.1
Apple iPad Mini 2 ME279LL/A	iOS 12.0
Microsoft Surface Pro 3 – 11ac	Qualcomm Atheros QCA61x4A
Microsoft Surface Pro 3 – 11ax	Intel AX201 chipset. Driver v21.40.1.3
Microsoft Surface Pro 7 – 11ax	Intel Wi-Fi chip (HarrisonPeak AX201) (11ax, WPA3)
Microsoft Surface Pro X – 11ac & WPA3	WCN3998 Wi-Fi Chip (11ac, WPA3)
Mobile Phones	
Apple iPhone 5	iOS 12.4.1
Apple iPhone 6s	iOS 13.5
Apple iPhone 8	iOS 13.5
Apple iPhone X MQA52LL/A	iOS 13.5
Apple iPhone 11	iOS 14.1
Apple iPhone SE MLY12LL/A	iOS 11.3
ASCOM SH1 Myco2	Build 2.1
ASCOM SH1 Myco2	Build 4.5

Client Type and Name	Driver or Software Version
ASCOM Myco 3 v1.2.3	Android 8.1
Drager Delta	VG9.0.2
Drager M300.3	VG2.4
Drager M300.4	VG2.4
Drager M540	DG6.0.2 (1.2.6)
Google Pixel 2	Android 10
Google Pixel 3	Android 11
Google Pixel 3a	Android 11
Google Pixel 4	Android 11
Huawei Mate 20 pro	Android 9.0
Huawei P20 Pro	Android 9.0
Huawei P40	Android 10
LG v40 ThinQ	Android 9.0
One Plus 8	Android 10
Oppo Find X2	Android 10
Redmi K20 Pro	Android 10
Samsung Galaxy S7	Andriod 6.0.1
Samsung Galaxy S7 SM - G930F	Android 8.0
Samsung Galaxy S8	Android 8.0
Samsung Galaxy S9+ - G965U1	Android 9.0
Samsung Galaxy SM - G950U	Android 7.0
Sony Experia 1 ii	Android 10
Sony Experia xz3	Android 9.0
Xiaomi Mi10	Android 10
Spectralink 8744	Android 5.1.1
Spectralink Versity Phones 9540	Android 8.1
Vocera Badges B3000n	4.3.2.5
Vocera Smart Badges V5000	5.0.4.30
Zebra MC40	Android 5.0
Zebra MC40N0	Android 4.1.1
Zebra MC92N0	Android 4.4.4

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

Issues

Issues describe unexpected behavior in Cisco IOS releases 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 Amsterdam 17.3.8a

Identifier	Headline
CSCvg70549	Error propagation from wncd back to manageability agent through wncmgrd.
CSCwe38431	Controller is remarking SIP packets from CS3 to CS0 in upstream/downstream when voice cac is configured.
CSCwd93773	Controller should not enable second 5-Ghz radio for 9124E with PoE+ (30W).
CSCwe22625	Controller GUI goes blank after logging in if username has '&'.
CSCwc97298	Cisco Catalyst 9166 AP: Radio-2 firmware crash is observed.
CSCwb84844	Cisco Catalyst OEAP 9105w CAPWAP DTLS session closed for AP, due to DTLS shutdown.
CSCvz18045	Cisco Catalyst 9130 AP: Probe suppression for Macro-Micro cell client steering is not supported.
CSCvy92773	Cisco Catalyst 9117 AP: Crash is observed on Slot 1.
CSCwe55494	Cisco Aironet 1832 AP is not sending packets to radio.
CSCwe11747	Cisco Catalyst 9130AX APs are decoding Extensible Authentication Protocol (EAP) request ID incorrectly.
CSCwd49861	AIRESPACE-WIRELESS-MIB: bsnAPIfType OID documentation incomplete.
CSCvz78407	Tx power mismatch on RAP & MAP even though same power is set on RAP & MAP
CSCwd96484	Controller is reloading unexpectedly generating "wncd" core files.
CSCvz16109	Cisco Catalyst 9105w Office Extend Access Points (OEAP) is crashing due to kernel panic.
CSCvz99564	Cisco APs are not assigned up with IPv6 addresses after upgrade from 17.6.1 to 17.6.2 or 17.7.1.
CSCvz16102	Cisco Catalyst 9105i OEAP is crashing due to kernel panic.
CSCwe53573	Cisco Aironet 1815W AP: Kernel panic with radio stats crash.
CSCwe44991	Cisco Catalyst 9105AX AP: Kernel panic crash is observed.
CSCwd16419	Cisco Catalyst 9800-CL-K9 unexpectedly reloads and generates pubd core.
CSCwe31030	Cisco Catalyst 9105AXW APs are crashing.

Identifier	Headline
CSCwa11312	Cisco Catalyst 9124E AP: Max transmit power is being capped for some domains resulting in 3 to 4dB less power.
CSCwe00248	Poor reassociation behavior is observed between Spectralink 84xx series phones and Cisco Catalyst 9136 APs.
CSCwe17593	Cisco Catalyst 9115 AP in workgroup bridge (WGB) stops sending traffic to the root AP after about 60 seconds from its initial connection.
CSCvw59760	ECDHE ciphers are not listed when WLAN Common Criteria (WLAN CC) is enabled.
CSCwc62824	Controller does not send LLC or XID spoofed frames after a mobility event.
CSCwe25446	Unexpected reboot due wncd.
CSCvw51315	Cisco Catalyst 9120 AP: Kernel panic is seen on AP when client is disconnected and connected back with Target Wake Time (TWT) session.
CSCwe30473	Radio firmware reloads unexpectedly due to a frozen RC queue.
CSCwe11315	Cisco Catalyst 9164 and 9166 APs running Cisco IOS-XE 17.9.2 is facing Dynamic Frequency Selection (DFS) detections in all channels.
CSCwc61347	Cisco Catalyst 9136I AP: Kernel crash is observed.
CSCwc10696	Regular ASR support field is disabled for supporting clients.
CSCwd90742	Cisco Catalyst 9120AX AP kernel crash - PC is at rhb_del_interface+0xc.
CSCwe43294	Cisco Catalyst 9105AXW AP and Cisco Aironet 1815W Flex RLAN AP does not apply VLAN in the ethernet port after AAA vlan override.
CSCwd73783	Cisco Catalyst 9800-L Series Controller: Observed qfp-ucode-wlc crash.
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.
CSCvy16422	Cisco Catalyst 9115 and 9120 APs are crashing: WL_REINIT_RC_MQ_ERROR.
CSCwe45970	Cisco Catalyst 9105 AP is stuck in U-BOOT.

Identifier	Headline
CSCwc95496	Cisco Catalyst 9130 AP: Radio crash is observed.
CSCvy89508	The primary member displays "standby hot" even though the standby is in recovery mode.
CSCwe45894	Cisco AP is not forwarding IGMPv3 query to wireless clients.
CSCvw64170	After changing channel and bandwidth of AP (with SIA), antenna shows incorrect legal/configured gain.
CSCwa38528	Cisco Catalyst 9105w OEAP: CAPWAP DTLS session is closed for AP due to DTLS server session shutdown.
CSCwc86955	Dual DFS stats on AP do not match controller information.
CSCwe45300	Cisco Catalyst 9120 AP: Sending Msg:2 in mode:2 to hostapd failed.
CSCvz59428	Unclear reason for radio reset due to role change sent from controller to Cisco DNA Center.
CSCvx03815	Cisco Catalyst 9120AX AP+SIA-DART: Initial configuration for slot 0 show configured gain value as 0.
CSCvz82490	WPA3-Suite B: Incorrect APUT response to STA incorrect TLS authentication parameters.
CSCwb38948	Cisco Catalyst 9124 AP: MAPs are no longer able to join RAP due to security failures.

Open Caveats for Cisco IOS XE Amsterdam 17.3.8

Identifier	Headline
CSCvg70549	Error propagation from wncd back to manageability agent through wncmgrd.
CSCwe38431	Controller is remarking SIP packets from CS3 to CS0 in upstream/downstream when voice cac is configured.
CSCwd93773	Controller should not enable second 5-Ghz radio for 9124E with PoE+ (30W).
CSCwe22625	Controller GUI goes blank after logging in if username has '&'.
CSCwc97298	Cisco Catalyst 9166 AP: Radio-2 firmware crash is observed.
CSCwb84844	Cisco Catalyst OEAP 9105w CAPWAP DTLS session closed for AP, due to DTLS shutdown.
CSCvz18045	Cisco Catalyst 9130 AP: Probe suppression for Macro-Micro cell client steering is not supported.

Identifier	Headline
CSCvy92773	Cisco Catalyst 9117 AP: Crash is observed on Slot 1.
CSCwe55494	Cisco Aironet 1832 AP is not sending packets to radio.
CSCwe11747	Cisco Catalyst 9130AX APs are decoding Extensible Authentication Protocol (EAP) request ID incorrectly.
CSCwd49861	AIRESPACE-WIRELESS-MIB: bsnAPIfType OID documentation incomplete.
CSCvz78407	Tx power mismatch on RAP & MAP even though same power is set on RAP & MAP
CSCwd96484	Controller is reloading unexpectedly generating "wncd" core files.
CSCvz16109	Cisco Catalyst 9105w Office Extend Access Points (OEAP) is crashing due to kernel panic.
CSCvz99564	Cisco APs are not assigned up with IPv6 addresses after upgrade from 17.6.1 to 17.6.2 or 17.7.1.
CSCvz16102	Cisco Catalyst 9105i OEAP is crashing due to kernel panic.
CSCwe53573	Cisco Aironet 1815W AP: Kernel panic with radio stats crash.
CSCwe44991	Cisco Catalyst 9105AX AP: Kernel panic crash is observed.
CSCwd16419	Cisco Catalyst 9800-CL-K9 unexpectedly reloads and generates pubd core.
CSCwe31030	Cisco Catalyst 9105AXW APs are crashing.
CSCwa11312	Cisco Catalyst 9124E AP: Max transmit power is being capped for some domains resulting in 3 to 4dB less power.
CSCwe00248	Poor reassociation behavior is observed between Spectralink 84xx series phones and Cisco Catalyst 9136 APs.
CSCwe17593	Cisco Catalyst 9115 AP in workgroup bridge (WGB) stops sending traffic to the root AP after about 60 seconds from its initial connection.
CSCvw59760	ECDHE ciphers are not listed when WLAN Common Criteria (WLAN CC) is enabled.
CSCwc62824	Controller does not send LLC or XID spoofed frames after a mobility event.
CSCwe25446	Unexpected reboot due wncd.
CSCvw51315	Cisco Catalyst 9120 AP: Kernel panic is seen on AP when client is disconnected and connected back with Target Wake Time (TWT) session.

Identifier	Headline
CSCwe30473	Radio firmware reloads unexpectedly due to a frozen RC queue.
CSCwe11315	Cisco Catalyst 9164 and 9166 APs running Cisco IOS-XE 17.9.2 is facing Dynamic Frequency Selection (DFS) detections in all channels.
CSCwc61347	Cisco Catalyst 9136I AP: Kernel crash is observed.
CSCwc10696	Regular ASR support field is disabled for supporting clients.
CSCwd90742	Cisco Catalyst 9120AX AP kernel crash - PC is at rhb_del_interface+0xc.
CSCwe43294	Cisco Catalyst 9105AXW AP and Cisco Aironet 1815W Flex RLAN AP does not apply VLAN in the ethernet port after AAA vlan override.
CSCwd73783	Cisco Catalyst 9800-L Series Controller: Observed qfp-ucode-wlc crash.
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.
CSCvy16422	Cisco Catalyst 9115 and 9120 APs are crashing: WL_REINIT_RC_MQ_ERROR.
CSCwe45970	Cisco Catalyst 9105 AP is stuck in U-BOOT.
CSCwc95496	Cisco Catalyst 9130 AP: Radio crash is observed.
CSCvy89508	The primary member displays "standby hot" even though the standby is in recovery mode.
CSCwe45894	Cisco AP is not forwarding IGMPv3 query to wireless clients.
CSCvw64170	After changing channel and bandwidth of AP (with SIA), antenna shows incorrect legal/configured gain.
CSCwa38528	Cisco Catalyst 9105w OEAP: CAPWAP DTLS session is closed for AP due to DTLS server session shutdown.
CSCwc86955	Dual DFS stats on AP do not match controller information.
CSCwe45300	Cisco Catalyst 9120 AP: Sending Msg:2 in mode:2 to hostapd failed.
CSCvz59428	Unclear reason for radio reset due to role change sent from controller to Cisco DNA Center.
CSCvx03815	Cisco Catalyst 9120AX AP+SIA-DART: Initial configuration for slot 0 show configured gain value as 0.

Identifier	Headline
CSCvz82490	WPA3-Suite B: Incorrect APUT response to STA incorrect TLS authentication parameters.
CSCwb38948	Cisco Catalyst 9124 AP: MAPs are no longer able to join RAP due to security failures.

Open Caveats for Cisco IOS XE Amsterdam 17.3.7

Identifier	Headline
CSCvg70549	Error propagation from wncd back to manageability agent through wncmgrd.
CSCwe38431	Controller is remarking SIP packets from CS3 to CS0 in upstream/downstream when voice cac is configured.
CSCwd93773	Controller should not enable second 5-Ghz radio for 9124E with PoE+ (30W).
CSCwe22625	Controller GUI goes blank after logging in if username has '&'.
CSCwc97298	Cisco Catalyst 9166 AP: Radio-2 firmware crash is observed.
CSCwb84844	Cisco Catalyst OEAP 9105w CAPWAP DTLS session closed for AP, due to DTLS shutdown.
CSCvz18045	Cisco Catalyst 9130 AP: Probe suppression for Macro-Micro cell client steering is not supported.
CSCvy92773	Cisco Catalyst 9117 AP: Crash is observed on Slot 1.
CSCwe55494	Cisco Aironet 1832 AP is not sending packets to radio.
CSCwe11747	Cisco Catalyst 9130AX APs are decoding Extensible Authentication Protocol (EAP) request ID incorrectly.
CSCwd49861	AIRESPACE-WIRELESS-MIB: bsnAPIfType OID documentation incomplete.
CSCvz78407	Tx power mismatch on RAP & MAP even though same power is set on RAP & MAP
CSCwd96484	Controller is reloading unexpectedly generating "wncd" core files.
CSCvz16109	Cisco Catalyst 9105w Office Extend Access Points (OEAP) is crashing due to kernel panic.
CSCvz99564	Cisco APs are not assigned up with IPv6 addresses after upgrade from 17.6.1 to 17.6.2 or 17.7.1.
CSCvz16102	Cisco Catalyst 9105i OEAP is crashing due to kernel panic.

Identifier	Headline
CSCwe53573	Cisco Aironet 1815W AP: Kernel panic with radio stats crash.
CSCwe44991	Cisco Catalyst 9105AX AP: Kernel panic crash is observed.
CSCwd16419	Cisco Catalyst 9800-CL-K9 unexpectedly reloads and generates pubd core.
CSCwe31030	Cisco Catalyst 9105AXW APs are crashing.
CSCwa11312	Cisco Catalyst 9124E AP: Max transmit power is being capped for some domains resulting in 3 to 4dB less power.
CSCwe00248	Poor reassociation behavior is observed between Spectralink 84xx series phones and Cisco Catalyst 9136 APs.
CSCwe17593	Cisco Catalyst 9115 AP in workgroup bridge (WGB) stops sending traffic to the root AP after about 60 seconds from its initial connection.
CSCvw59760	ECDHE ciphers are not listed when WLAN Common Criteria (WLAN CC) is enabled.
CSCwc62824	Controller does not send LLC or XID spoofed frames after a mobility event.
CSCwe25446	Unexpected reboot due wncd.
CSCvw51315	Cisco Catalyst 9120 AP: Kernel panic is seen on AP when client is disconnected and connected back with Target Wake Time (TWT) session.
CSCwe30473	Radio firmware reloads unexpectedly due to a frozen RC queue.
CSCwe11315	Cisco Catalyst 9164 and 9166 APs running Cisco IOS-XE 17.9.2 is facing Dynamic Frequency Selection (DFS) detections in all channels.
CSCwc61347	Cisco Catalyst 9136I AP: Kernel crash is observed.
CSCwc10696	Regular ASR support field is disabled for supporting clients.
CSCwd90742	Cisco Catalyst 9120AX AP kernel crash - PC is at rhb_del_interface+0xc.
CSCwe43294	Cisco Catalyst 9105AXW AP and Cisco Aironet 1815W Flex RLAN AP does not apply VLAN in the ethernet port after AAA vlan override.
CSCwd73783	Cisco Catalyst 9800-L Series Controller: Observed qfp-ucode-wlc crash.
CSCwe31270	Clients stop passing traffic when there is a missing bandwidth limit AAA attribute on the controller.

Identifier	Headline
CSCwe32005	Cisco Catalyst 9130 AP: Packet loss is observed on Digital Signage device.
CSCvy16422	Cisco Catalyst 9115 and 9120 APs are crashing: WL_REINIT_RC_MQ_ERROR.
CSCwe45970	Cisco Catalyst 9105 AP is stuck in U-BOOT.
CSCwc95496	Cisco Catalyst 9130 AP: Radio crash is observed.
CSCvy89508	The primary member displays "standby hot" even though the standby is in recovery mode.
CSCwe45894	Cisco AP is not forwarding IGMPv3 query to wireless clients.
CSCvw64170	After changing channel and bandwidth of AP (with SIA), antenna shows incorrect legal/configured gain.
CSCwa38528	Cisco Catalyst 9105w OEAP: CAPWAP DTLS session is closed for AP due to DTLS server session shutdown.
CSCwe22861	Observing AID leak in Cisco Wave 2 APs in FlexConnect mode.
CSCvv18443	In-Service Software Upgrade (ISSU) build issue.
CSCwe39039	Traceback is seen after provisioning controller from Cisco DNA Centre.
CSCwa13091	Tx power changes are not getting applied to the AP.
CSCwc86955	Dual DFS stats on AP do not match controller information.
CSCwd22364	Unexpected error messages flooding in RA logs for successful client joins.
CSCwe45300	Cisco Catalyst 9120 AP: Sending Msg:2 in mode:2 to hostapd failed.
CSCvz59428	Unclear reason for radio reset due to role change sent from controller to Cisco DNA Center.
CSCwe54482	Cisco Catalyst 9120 AP is dropping DHCP offer in click. Not forwarding to wireless interface.
CSCvx03815	Cisco Catalyst 9120AX AP+SIA-DART: Initial configuration for slot 0 show configured gain value as 0.
CSCwe44216	Cisco AP reloads unexpectedly due to kernel panic.
CSCvz82490	WPA3-Suite B: Incorrect APUT response to STA incorrect TLS authentication parameters.
CSCwb38948	Cisco Catalyst 9124 AP: MAPs are no longer able to join RAP due to security failures.

Open Caveats for Cisco IOS XE Amsterdam 17.3.6

Caveat ID	Description
CSCwd37092	Slow TCP downloads and failing EAP-TLS are observed in Cisco IOS XE 17.3.6 - Cisco Aironet 2800, 3800, 4800, 1562, or Cisco Catalyst Industrial Wireless 6300 Heavy Duty Series Access Points.
CSCvw70260	Cisco Aironet 1572EAC Access Point does not respond to the Canadian EIRP regulation.
CSCvz59428	The reason for radio reset is unclear due to role change sent from controller to Cisco DNAC.
CSCwa25735	Cisco Aironet 1832 Access Point does not forward packets to radio.
CSCwa68709	Cisco Catalyst 9115 Access Point reports Dynamic Frequency Selection (DFS) in channels incorrectly: "blocked list due to be cleared".
CSCwa75050	Factory reset using a physical button does not work always.
CSCwb32300	Cisco Catalyst 4800 Series Access Point in local mode running 8.10.171.0 experiences radio coredump.
CSCwc78435	Cisco Catalyst 9130 Access Point sends incorrect channel list in out-of-band DFS event causing client connectivity issues.
CSCwc28757	Cisco Catalyst 3800 Access Point radio reloads unexpectedly in Slot 0 ap-17.9.0.135.
CSCwc32182	Cisco Aironet 1852 Access Point experiences radio firmware crash.
CSCwc61347	Cisco Catalyst 9136I Access Point experiences kernel crash in ap-17.9.1.7.
CSCwc75732	Firmware radio crash is observed in Cisco Catalyst 4800 Access Point in Cisco IOS-XE 17.3.5b release.
CSCvw28085	Access Point **show logging** is flooded with "syslog: parse_tx_bcn: Bcn payload is NULL" syslog messages.
CSCvz90902	Cisco Catalyst 9130 Access Point: Probe suppression for macro-micro cell client steering does not work.
CSCwb08291	Cisco Catalyst 9105AXW Access Point introduces latency when clients use RLAN ports.
CSCwb23886	Mac and Android OS clients are not able to pass traffic when connected to Cisco Aironet 1810W Access Point RLAN ports.
CSCwc15898	CleanAir data is missing for 2.4-GHz in few Cisco Catalyst 9120 or 9130 Access Points.

Caveat ID	Description
CSCwc30521	Workgroup bridge (WGB) breaks in Pre-Shared Key (PSK) with key length of 63.
CSCwc38912	Changing an AP site or policy tag to a Flex local switching set intermittently causes client connectivity failure to local web auth WLANs.
CSCwc42728	Cisco Access Point reloads unexpectedly due to system critical process crash.
CSCwc49970	5-GHz channel 165 cannot be selected in Cisco Aironet 2800, 3800, and 4800 Access Point models.
CSCwc59814	Burst beacon is enabled by default for 11ac Cisco Wave 2 QCA Access Points.
CSCwc72194	Cisco Catalyst 9120 Access Point: Radio Core Dump: wl0: wlc_check_assert_type HAMMERING.
CSCwc73462	Backslash "\" in the end of the RADIUS servers' shared secret is not allowed for FlexConnect groups configuration.
CSCvy89508	The primary member displays "standby hot" even though the standby is in recovery mode.
CSCwa44734	wncd crash is observed at wsa_clt_evt_cache_update during client join with Cisco DNAC auth rate testing.
CSCwc68682	Cisco Catalyst 9800 Wireless Controller - Link down due to local fault.
CSCvu49930	Changing channel to 165 or width 20 fails when an Access Point is configured with channel width 40.
CSCvz81889	Cisco Catalyst 9500-32C and 9500-32QC missing air license related XML entries.
CSCwa93208	FlexConnect WLAN VLAN mapping disappears when VLAN name is defined in the FlexProfile.
CSCwc26819	Controller does not send LLC or XID spoofed frames after a mobility event.
CSCwc72047	Access Points operate in disabled RF profile channels in Cisco IOS-XE 17.6.2 ESW01.
CSCwc74020	Need to increase the 8 IP address limit in the controller datapath.
CSCwc76905	SISF crash is observed when handling the DHCP messages.
CSCwc77604	Access Point does not join the controller due to CAPWAP data tunnel plumb failure.

Open Caveats for Cisco IOS XE Amsterdam 17.3.5b

Caveat ID	Description
CSCvz82509	The AVC page does not load in the GUI under **Configuration** > **Services** > **AVC**.
CSCvy89508	The primary controller displays "standby hot" even though the standby controller is in recovery mode.
CSCvt99760	Crash occurs when Btrace modules exceed the initial maximum number of registrations.
CSCwa37701	The controller standby chassis shows Cisco Unknown Power Supply and the same serial number in the **show inventory** command output.
CSCvz98800	Cisco Aironet 1542 Series APs are not listed while adding to the Floor Map.
CSCwa25291	Configures the APs workflow to Resume or Cancel errors.
CSCwa14744	Cisco Catalyst 9130AX AP reloads unexpectedly when PC is at __qdf_bug+0x0/0x8 osif_delete_vap_wait_and_free.
CSCwa26814	Cisco Aironet 3800 Series AP does not pass Address Resolution Protocol (ARP) requests when configured in Custom Flex Group.
CSCwa33348	AIR-AP1815I-H-K9: AP abnormal reboot without crash or core file.
CSCwa33917	Cisco Catalyst 9130AXI AP changes the Domain Name System (DNS) information from the Dynamic Host Configuration Protocol (DHCP) offer packet.
CSCwa48644	The FortyGigabitEthernet interfaces in Cisco Catalyst 9800-80 Wireless Controller gets stuck in the down state after repeated High Availability (HA) failovers.
CSCwa49815	CleanAir status down reported by multiple APs in controller running 8.10.151.0.
CSCwa52440	Cisco Catalyst 9117AX AP reloads unexpectedly due to radio failure (radio recovery failed) when beacons are stuck in Radio 1.
CSCwa54223	Incorrect campus maps information is observed in Cisco CMX 10.6.2-89.
CSCwa61087	Cisco Aironet 1562 Series AP acts as Work Group Bridge (WGB) but unable to pass multicast traffic to passive client behind it.
CSCwa64749	Cisco Catalyst 9130 Series AP driver declines authorization request causing 802.11w client join issues.

Caveat ID	Description
CSCwa65318	Clients are unable to join the Cisco Catalyst 9130 AP slot 2 when transmission power is set to the lower power level (-2dbm or -4dbm).
CSCwa65713	Cisco Aironet 4800 AP crash: Unable to handle kernel NULL pointer dereference at virtual address.
CSCwa71189	Cisco Catalyst 9130 Series AP crashes on CAPWAP after joining the controller.
CSCwa75901	Radio failure (radio recovery failed) due to Cisco Catalyst 9117 Series AP Beacon stuck.
CSCvy72750	Wireless controller is unable to use the **wireless broadcast vlan X** command.

Open Caveats for Cisco IOS XE Amsterdam 17.3.5a

Caveat ID	Description
CSCvz82509	The AVC page does not load in the GUI under **Configuration** > **Services** > **AVC**.
CSCvy89508	The primary controller displays "standby hot" even though the standby controller is in recovery mode.
CSCvt99760	Crash occurs when Btrace modules exceed the initial maximjm number of registrations.
CSCwa37701	The controller standby chassis shows Cisco Unknown Power Supply and the same serial number in the **show inventory** command output.
CSCvz98800	Cisco Aironet1542 Series APs are not listed while adding to the Floor Map.
CSCwa25291	Configures the APs workflow to Resume or Cancel errors.
CSCvw70260	Cisco Aironet 1572EAC AP does not respond to the Canadian EIRP regulation.
CSCvz96924	Cisco Catalyst 9130 series AP does not send M1 over the air.
CSCwa14744	Cisco Catalyst 9130 Series AP crash - PC is at __qdf_bug+0x0/0x8 osif_delete_vap_wait_and_free.
CSCwa26814	Cisco Aironet 3800 Series AP not passing Address Resolution Protocol (ARP) requests when configured on Custom Flex Group.
CSCwa31596	Cisco Catalyst 9130 Series high channel utilization and client lags with 9 or more clients using MS Teams.
CSCwa33348	AIR-AP1815I-H-K9: AP abnormal reboot without crash/core file.

Caveat ID	Description
CSCwa33917	Cisco Catalyst 9130AXI AP changes the Domain Name System (DNS) information from the Dynamic Host Configuration Protocol (DHCP) offer packet.
CSCwa48644	The FortyGigabitEthernet interfaces on Cisco Catalyst 9800-80 Wireless Controller gets stuck in the down state after repeated High Availability (HA) failovers.
CSCwa49815	Multiple CleanAir Sensor Status: 'Down' - Controller 8.10.151.0
CSCwa52440	Cisco Catalyst 9117 Series APs crashes due radio failure (radio recovery failed) Beacons stuck on Radio 1.
CSCwa54223	Incorrect campus maps information on CMX 10.6.2-89.
CSCwa61087	Cisco Aironet 1562 Series AP acts as Work Group Bridge (WGB) but unable to pass multicast traffic to passive client behind it.
CSCwa64749	Cisco Catalyst 9130 Series AP driver declines authorization request causing 11w client join issues.
CSCwa65318	Tx power for Microcell created by AP for slot 2 of Cisco Catalyst 9130 Series AP.
CSCwa65713	Cisco Aironet 4800 AP crash: Unable to handle Kernel NULL pointer dereference at virtual address.
CSCwa71189	Cisco Catalyst 9130 Series AP crashes on CAPWAP after joining with the controller.
CSCwa75901	Cisco Catalyst 9117 Series AP Beacon Struck - crash due to radio failure (radio recovery failed).
CSCvy67650	Controller does not send TCP SYN or ACK for web redirect once TCP SYN is received and punted to CPU.

Open Caveats for Cisco IOS XE Amsterdam 17.3.4c

Caveat ID	Description
CSCvh82161	WGB loses connectivity to the controller.
CSCvs77557	Cisco Aironet 3802 AP is not able to acknowledge EAP frames (EAP-TLS).
CSCvw70260	Cisco Aironet 1572EAC Access Point does not respond to the Canadian EIRP regulation.
CSCvx67724	Cisco 1815 AP ends abnormally on the controller due to Out of Memory.
CSCvx84524	Cisco Aironet 1570 AP does not display the RRM neighbors.

Caveat ID	Description
CSCvx99197	Cisco Catalyst 9120 Access Point experiences crash after upgrading to 8.10.158.38.
CSCvy30091	Cisco Catalyst 9120 AP stops transmitting frames to Macbook after a session reauthetication.
CSCvy48917	When Samsung tries to join the WPA3 AES-802.1x or SHA256 WLAN, AP sends corrupted assoc response.
CSCvy52874	Cisco Catalyst 9115 AP crashes after loading the 17.3.3 ES6 image.
CSCvy67650	Controller does not send TCP SYN or ACK for web redirect once TCP SYN is received and punted to CPU.
CSCvy72750	Wireless controller is unable to use the "wireless broadcast vlan X".

Open Caveats for Cisco IOS XE Amsterdam 17.3.4

Caveat ID	Description
CSCvh82161	WGB loses connectivity to the controller.
CSCvs77557	Cisco Aironet 3802 AP is not able to acknowledge EAP frames (EAP-TLS).
CSCvw70260	Cisco Aironet 1572EAC Access Point does not respond to the Canadian EIRP regulation.
CSCvx67724	Cisco 1815 AP ends abnormally on the controller due to Out of Memory.
CSCvx84524	Cisco Aironet 1570 AP does not display the RRM neighbors.
CSCvx99197	Cisco Catalyst 9120 Access Point experiences crash after upgrading to 8.10.158.38.
CSCvy30091	Cisco Catalyst 9120 AP stops transmitting frames to Macbook after a session reauthetication.
CSCvy48917	When Samsung tries to join the WPA3 AES-802.1x or SHA256 WLAN, AP sends corrupted assoc response.
CSCvy52874	Cisco Catalyst 9115 AP crashes after loading the 17.3.3 ES6 image.
CSCvy62022	AP stops forwarding RTP packets to clients.
CSCvy66944	Cisco Catalyst 9120AX Series Access Point does not forward downstream packets to the device.
CSCvy67650	Controller does not send TCP SYN or ACK for web redirect once TCP SYN is received and punted to CPU.

Caveat ID	Description
CSCvy72750	Wireless controller is unable to use the "wireless broadcast vlan X".

Open Caveats for Cisco IOS XE Amsterdam 17.3.3

Caveat ID	Description
CSCvx94722	Cisco IOS XE Gibraltar 16.12.5 version generates jumbo frames for dot1x packets.
CSCvr71247	Process "pubd" uses large amount of memory in case of many subscriptions to large amounts of data.
CSCvs73917	Zero session-timeout from AAA or policy-profile.
CSCvs77557	Cisco Aironet 3802 AP is not able to acknowledge EAP frames (EAP-TLS).
CSCvv01775	Wired Clients behind non-Cisco WGB does not get IP on the controller.
CSCvv52618	Cisco Aironet 2800 and 3800 APs exhibit choppiness during the multicast voice call.
CSCvw07137	No validation on unsupported channel configuration in the controller.
CSCvw10039	Cisco Aironet 2802 AP reloads unexpectedly due to kernel panic.
CSCvw55697	AP cannot join the controller - Dropping client hello received with zero MAC.
CSCvw69665	VLANs are not being marked dirty and stuck in ip learn.
CSCvw70285	Cisco Catalyst 9120 APs cannot send ACK over the air during EAP negotiation.
CSCvw99347	Controller drops AP DTLS connection.
CSCvx06998	Cisco Catalyst 9800-CL Cloud Wireless Controller running Hyper-V stops responding intermittently.
CSCvx17425	DFS detection optimization to avoid false DFS detection in Cisco Catalyst 9115 Series APs.
CSCvx19602	Cisco Catalyst 9120 Series AP beacon gets stuck after moving from channel UNII 1 to UNII 2.
CSCvx35811	CWA clients are not moved back to webauth after CoA reauth is sent when client is in RUN.

Caveat ID	Description
CSCvx44338	802.11r retried Auth packet forwarded to controller causes duplicate Auth responses sent to client.
CSCvw25812	AP does not send an ADDTS response when PMF enabled.
CSCvw65861	MAC Filtering: Description not imported properly from a CSV file.
CSCvw88389	Check if the AP-COS crash files print complete information.
CSCvw94907	The client data rate displays incorrectly on the GUI or CLI.
CSCvx12253	Observed Cisco C9800-L Wireless Controller downgrade rommon after upgrading hw-programmable phy.
CSCvx24622	The controller produces an error when RA trace is generated on the GUI or CLI.
CSCvx27626	The Apple clients fail to pass M2 EAPOL when 802.11r is enabled after a switchover.
CSCvx29110	PMF Optional - Protecting frames for NON-PMF clients.
CSCvx31952	C9115/9120 reading /sys/class/thermal/thermal_zone0/temp failed [2]: No such file or directory logs.
CSCvx34926	AP admin enable doesn't work on slow systems when page is submitted immediately after a click action.
CSCvx41454	The **show wireless client detail** command displays the old or incorrect IP address.
CSCvx52078	Cisco Aironet 2802 series Access Point suddenly drops in transmission power level.
CSCvx43345	Cisco Aironet 3802 series access points crashes on Radio 1 in FlexConnect mode.
CSCvx51502	ASR1K platform crashes when applying a hierarchical QoS policy on the tunnel interface.

Open Caveats for Cisco IOS XE Amsterdam 17.3.2a

Caveat ID	Description
CSCvr16233	Cisco Aironet 2802 AP beacon loss issue.
CSCvs77557	Cisco Aironet 3802 AP is not able to acknowledge Extensible Authentication Protocol (EAP) frames.
CSCvu58210	Cisco Aironet 3800 and 4800 APs are dropping from the controller.

Caveat ID	Description
CSCvu66043	Cisco Aironet 9130 APs are not sending DHCP messages over the air.
CSCvu84745	Wired clients are not able to access HTTP/HTTPS through Remote LAN (RLAN).
CSCvv01775	Wired clients behind a non-Cisco workgroup bridge (WGB) is not getting IP address.
CSCvv28658	Wave 2 AP crashed due to FIQ/NMI reset.
CSCvv34443	Controller is not accepting href parameters on web support bundle.
CSCvv39947	Dual-Band (XOR) radio operating in monitor mode exists as part of 5 GHz band emulated radio table.
CSCvv50570	WNCD crash is observed after MAB fails to allocate memory.
CSCvv52578	Inconsistent configuration options to enable 5 GHz single band antennas on external antenna APs.
CSCvv52618	Cisco Aironet 2800 and 3800 APs exhibit choppiness during the multicast voice call.
CSCvv64647	Wave 2 APs are not able to negotiate power with SG350 switches.
CSCvv68017	Controller platform error: %IOSXE-2-PLATFORM: Chassis 1 R0/0: kernel: EXT2-fs (sda1): error.
CSCvv68091	Controllers fails to save configuration with with EXT2-fs (sdb1) errors.
CSCvv74729	Controller is unable to classify Google pixel mobile phones.
CSCvv77141	Gateway MAC address is being learned from Cisco 1815 AP switchport.
CSCvv78264	MESH: Cisco Aironet 1542 Outdoor Access Point does not converge to Cisco Aironet 1572 Outdoor Access Point.
CSCvv78719	Cisco Aironet 2800, 3800, 4800, 1560, and 6300 APs fail to transmit data frame to the client from the radio interface.
CSCvv79700	Fault tolerance is broken in Flex APs.
CSCvv80531	Flexconnect CA+LS 11w clients may disjoin during standalone to connected transition
CSCvv84296	Stale client entry leads to client disconnection and association problems.
CSCvv91973	Transport mode is not persisting across high-availability after upgrade with smart licensing registered.

Caveat ID	Description
CSCvv93995	Cisco Catalyst 9115 Series Wi-Fi 6 Access Point: Clients are unable to connect due to persistent Tx error on radio.
CSCvv95733	Some commands are not applied while using iosxe_config.txt to load configuration to Cisco Catalyst 9800-CL Wireless Controller using KVM.
CSCvv95806	Remove unsupported VXLAN-EVPN commands from the controller.
CSCvv97156	Cisco Catalyst 9130AX Series Access Points are dropping some uplink packets from macbooks.
CSCvv97807	Netconf and Netconf-YANG are not enabled on the external nodes as part of PnP configuration.
CSCvv97823	YANG requests from Cisco DNA-C to IoT devices related to device licensing are failing.
CSCvv99213	Cisco Catalyst 9130AXE Series Access Points are not taking RF tag power settings on slot 2.
CSCvw01612	Cisco Catalyst 9130AX Series Access Points are not sending M1 over the air.
CSCvw02981	Cisco Aironet 2802 Access Point shows sudden drop in TX power level.
CSCvw06580	CAC shown as running for non-DFS channels and even on 2.4GHz band on controller.
CSCvw08444	Flex: Client is stuck in excluded state after modifying the VLAN to default.
CSCvw08559	APs are not broadcasting SSID after disabling mobility anchor using web interface.
CSCvw10013	Cisco Aironet 1852 Access Point: Radio hangs are causing packets drops.
CSCvw10308	Cisco Catalyst 9130AX Series Access Point is dropping packets and the AP is not able to push packet to click module.
CSCvw13174	AP location string is truncated during join.
CSCvw15298	Cisco Embedded Wireless Controller for an AP is not forwarding downstream traffic after active AP failover.
CSCvw16305	Wncd core is seen when client is getting blacklisting flag from WLAN policy.
CSCvw16414	Cisco Catalyst 9130 Series Access Point: Repeated log entries are showing dual radio failure.

Caveat ID	Description
CSCvw16701	AQI value is coming as 0 for slot_index:1.
CSCvw19807	Warn users if a configuration is not applied correctly and remedial steps are to be performed
CSCvw19820	Controller is unable to push SSIDs while doing a configuration change on policy profile.
CSCvw20567	Kernel crash seen in the hardware controllers during upgrade.
CSCvw25488	Interface speed for the AP is showing a wrong value in Cisco Prime.
CSCvw27530	Data DTLS with IPv6 tunnel is not established after reloading controller.
CSCvw27949	Client goes to excluded state till timeout expires when changing vlan-id-mapping in both in both flex and policy profile.
CSCvw30043	Cisco Aironet 3800 Access Point is randomly not sending traffic to client queue 0 after dot1x session-timeout.
CSCvw30340	The output of the **show license authorization** command is incorrect.
CSCvw31638	Make messages such as \"kernel: HANET: ip_local_out send failed\" customer readable or suppress them.
CSCvw31786	CAPWAP multiwindow feature: AP disconnects after stateful switchover (SSO) while AP image predownload is in progress.
CSCvw32098	Cisco switches connected to Wave2 APs generate CDP-4-DUPLEX_MISMATCH.
CSCvw35589	Controller displays incorrect antenna gain.
CSCvw67128	Smart Liensing Policy: Purchase information should be protected and shouldn't be able to erase.

Open Caveats for Cisco IOS XE Amsterdam 17.3.1

Caveat ID	Description
CSCvr96755	Support for three-step install upgrade with ap image predownload is required.
CSCvs62309	Device is crashing while executing the **copy flash:< >.cfg running-config** command.
CSCvt35141	Disallow Webauth WLANs from being tagged to authentication servers with load-balancing enabled.
CSCvu17521	Interface speed for the AP is showing as *None* in Cisco Prime Infrastructure.

Caveat ID	Description
CSCvu22410	The dot11n and dot11ac are disabled and configuration is saved. When the controller reloads, they are enabled again.
CSCvu40188	Configuration slot 0 output is updating wrong values for XOR radio when mapped to the custom rf-profile.
CSCvu40529	Radio objects are missing from the RRMradSlot table if AP tag is in mis-configured state.
CSCvu41319	Cisco Aironet 1570 APs are not allowing clients to connect in 5 GHz.
CSCvu53070	AP kernel panic crash (PC is at vfp_reload_hw).
CSCvu58082	Cisco Aironet 3800 AP with data DTLS encryption disconnects from the controller due to CAPWAP keepalive after rx PMTU discovery.
CSCvu65440	CAPWAP multi-window support: AP disconnects post switchover when AP image predownload is in progress.
CSCvu69426	Auto-contain doesn't resume after rogue-client is removed.
CSCvu70630	Rogue rule created is overridden with latest priority.
CSCvu73873	Cisco Catalyst 9800-80 Controller is sending client traffic out of the AP manager interface.
CSCvu76954	Client is connected through dot11n or dot11n even when dot11 options are disabled.
CSCvu89996	AP disjoins after client connects to SSID using LDAP with secure mode.
CSCvu91948	The show command for AP tri-radio Feature is not available in Cisco Embedded Wireless Controller on Catalyst Access Points.
CSCvu92134	Cisco Aironet 2800 AP: Wpa2-psk-aes WLAN client is getting disturbed when AP moves from flex.
CSCvu95179	Spectrum intelligence interference detected by AP is not seen on the controller.
CSCvv01407	Small VM install of controller loses its management trustpoint after every reboot.
CSCvv02099	AP is not rejecting incorrect Fast Transition Auth request.
CSCvv02121	AP is not sending reassociation response.
CSCvv02670	Controller is showing incorrect AP cisco discovery protocol (CDP) information.

Caveat ID	Description
CSCvv03370	Cisco Embedded Wireless Controller on Catalyst Access Points: AP image predownload status is empty for most of the APs.
CSCvv03668	Cisco Aironet 3800h AP: Jitter issue with MS-Teams application.
CSCvv04072	Cisco Catalyst 9105 AP: LED is turned off by default.
CSCvv04911	Last switchover reason is shown as *active unit removed* during ISSU upgrade.
CSCvv09143	Private Pre-Shared-Key (PSK) Pairwise Master Key (PMK) is retained resulting in client delete. Controller is crashing with scaled PPSK join.
CSCvv14121	Cisco DNA-Centre: When AP fails to pre-download image; further attempts to pre-download are getting stuck.

Resolved Caveats for Cisco IOS XE Amsterdam 17.3.8a

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 Amsterdam 17.3.8

Identifier	Headline
CSCwf67316	Cisco Wave 2 Access Points may not detect radar on the required levels after Channel Assessment Time (CAC).

Resolved Caveats for Cisco IOS XE Amsterdam 17.3.7

Identifier	Headline
CSCvv96364	Cisco Aironet 3800 Access Points experienceWCPd crash when running 17.3.1 image.
CSCvw20363	Cisco Aironet 2800 and 3800 APs: WGB fails to connect via PEAP if client certificate is not installed.
CSCvx32806	Cisco Wave 2 APs stuck in bootloop due to image checksum verification failure.
CSCvx72883	Controller does not remove 802.1X clients after session-timeout.
CSCvx80422	AP drops packets addressed to 10.128.128.127 or 10.128.128.128.

Identifier	Headline
CSCvy69496	Remote address attribute missing when accessing controller through GUI using TACACS+ credentials.
CSCvz94649	Controller sends new Access-Requests using previous packet id.
CSCwa21431	Controller unexpectedly reloads on DMI authentication task with **guestshell** enabled.
CSCwa48702	Kernel panic crash in Cisco Catalyst 9130AX Series APs.
CSCwa68709	Cisco Catalyst 9115 AP reports DFS on channels incorrectly: "Blocked list due to be cleared".
CSCwa93884	Cisco iOX app installation fails during app activation phase with the following error: "Error while creating app start up script".
CSCwb08291	Cisco Catalyst 9105AXW AP is introducing latency when clients are using RLAN ports.
CSCwb23886	Cisco Aironet 1810W AP: RLAN DHCP issues with certain client models.
CSCwb34231	Cisco Catalyst 9115 AP: Power saving client state on radio.
CSCwb41815	AP is not copying DHCP ACK packets to the controller after enable "cts manual" on the switch.
CSCwb51757	High channel utilization on 5-GHz radio with 40Mhz.
CSCwb59227	Cisco Catalyst 9105w AP is crashing due to kernel panic.
CSCwb82694	Cisco Catalyst 9105/9115/9120 series APs are unable to handle out of order packets.
CSCwb96560	AppHost: App install fails when USB state is disabled in the AP Join profile.
CSCwc02477	Cisco Catalyst 9130 AP does not transmit EAP identity request.
CSCwc05366	Wireless AAA dynamic VLAN assignment: The wireless clients cannot reach each other.
CSCwc15898	Cisco Catalyst 9120 and 9130 APs: Missing CleanAir data for 2.4GHz.
CSCwc15944	Multicast data not sent to clients; some APs may be unable to join the controller.
CSCwc31331	Cisco Catalyst 9130 AP unexpectedly reload in run_timer_softirq.
CSCwc32182	Radio firmware crashes in Cisco Aironet 1850 Series Access Points.

Identifier	Headline
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.
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.
CSCwc57227	Controller experiences an unexpected reset resulting in a system report containing a wncd core file.
CSCwc67729	Cisco Aironet 1840 OEAP crashed due to radio failure.
CSCwc68682	Link connecting the controllers goes down due to local fault.
CSCwc69815	Catalyst 9300 switches generate RUM reports every 8 hours.
CSCwc72194	Cisco Catalyst 9120 AP: Radio core dump.
CSCwc73462	For FlexConnect group configuration, do not use backslash (\) at the end of the radius servers shared secret.
CSCwc75732	Cisco Aironet 4800 AP: Firmware radio crash is observed.
CSCwc76905	Switch Integrated Security Features (SISF) crash is observed when handling the DHCP messages.
CSCwc78435	Cisco Catalyst 9130 AP sends incorrect channel list on the "out of band" DFS event, causing client connectivity issues.
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.
CSCwc89719	Cisco Aironet 1832 AP reloads unexpectedly due to radio recovery failure.
CSCwc93198	Cisco Catalyst 9800-L Wireless Controller does not receive HWDIB down message when RP port goes down in HA, preventing WMI from sending GARP.
CSCwc94898	AP WGB stuck in EAPOL state.
CSCwc99823	Fman crash seen in SGACL@ fman_sgacl_calloc.
CSCwd00711	WPA3 and OWE transition enabled: Non-WPA3 clients get network access in "webauth-pending" state.

Identifier	Headline
CSCwd00751	Cisco Aironet 2802 AP reloads unexpectedly.
CSCwd02898	Cisco Catalyst 9300 Series Switch is not flushing remote MAC address after roaming to a local AP.
CSCwd03803	Cisco Aironet 1815 APs reboot - PC is at edma_poll or LR is at dma_cache_maint_page.
CSCwd04025	PI 3.10.1: Associated APs with controller displays interface mode type as "Half duplex".
CSCwd04571	Memory leak is observed in wncd process when under load.
CSCwd05593	Cisco Catalyst 9120 AP: TX is stuck due to data block PS and AP radio crash.
CSCwd06001	Linux iosd crash on standby controller during reload of the Cisco Catalyst 9800-L Wireless Controller.
CSCwd06018	802.11r re-auth failed due to invalid Pairwise Master Key ID (PMKID) while doing inter-WNCD roaming.
CSCwd08165	Controller is accounting wrong class attribute in accounting packets.
CSCwd08259	Cisco Catalyst 9120, 9115, and 9105 Access Points experience radio firmware crash with Cisco IOS-XE 17.3 or later releases.
CSCwd08678	Clients not deleted by the controller after session-timeout ("Timer not running" state).
CSCwd08926	Cisco Catalyst 9162 AP: Client connection failure with BLE configured as native scan.
CSCwd10570	Cisco Catalyst 9130 Access Point displays different beacon data-rates for different Basic Service Set Identifiers (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.
CSCwd16409	User-agent details needs to be truncated to string length 234 in WSA to prevent vstring corruption.
CSCwd17349	Active chassis gets stuck during SSO failover in Cisco IOS-XE 17.9 release version.
CSCwd19631	Cisco Catalyst 9120 AP cannot operate in Multigigabit Ethernet (mGig) when Energy Efficient Ethernet (EEE) is enabled on switchport.
CSCwd21996	Cisco Catalyst 9120 AP: CleanAir sensor reloads unexpectedly.

Identifier	Headline
CSCwd23681	Controller fails to update AP configuration with error `% Error: no ap_name exists` .
CSCwd30578	Wired guest client are stuck at IP_LEARN with DHCP packets not forwarded out of the foreign to anchor.
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 does not follow the DCA sensitivity threshold.
CSCwd35393	Wireless load balancing affinity incorrectly shows AP site tag as default-site.
CSCwd35577	Double bit ECC error causes the standby controller to reload.
CSCwd36552	Cisco Catalyst 9120 AP reloads unexpectedly due to kernel panic.
CSCwd37092	Cisco Aironet 2800, 3800, 4800, 1562, and 6300 series APs: Slow TCP downloads, failing EAP-TLS.
CSCwd38925	Cisco Catalyst 9105 AP reloads unexpectedly multiple times.
CSCwd39605	Cisco Catalyst 9117 AP reloads unexpectedly due to kernel panic at console_unlock+0x320/0x3ac.
CSCwd40731	AP reloads due to kernel panic.
CSCwd41108	Multiple Cisco Catalyst 9130AXE APs with DART connectors stuck at channel 36.
CSCwd46721	Controller stays in the IP_THEFT state indefinitely 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.
CSCwd46815	EAP-TLS is failing for the wired clients behind MAP for Cisco 2800, 3800, 4800, 1562, 6300 series APs.
CSCwd47384	Cisco Catalyst 9130 AP: Radio 1 is crashing.
CSCwd47741	Controller fails to update DCA channels as RRM is stuck.
CSCwd49166	Cisco Aironet 3800 AP consistently reports high QBSS load.

Identifier	Headline
CSCwd52745	Cisco Aironet 3802 AP: Kernel crash is observed.
CSCwd52938	Wired clients behind WGB do not get IP addresses for anchor WLAN.
CSCwd55757	Wave 2 APs reloads unexpectedly due to "Systemd critical process crash - dnsmasq-host.service failed" error.
CSCwd56391	Controller does not provide RSSI location data for some of the RFID tags in the database.
CSCwd56434	Service insertion fails after CSR1Kv hub in Azure is rebooted.
CSCwd56621	Controller GUI logging buffer size display is incorrect.
CSCwd58182	Cisco Aironet 3800 series AP reloads unexpectedly due to kernel panic.
CSCwd59423	Unexpected reload on the controller caused by WNCd process after removing a VLAN from a VLAN-GROUP.
CSCwd59921	Cisco Catalyst 9130 AP is dropping EAP-TLS frames.
CSCwd60034	Cisco Aironet 3800 AP: Radio reloads unexpectedly due to a stuck beacon.
CSCwd60376	Cisco Catalyst 9120 AP: Kernel panic is observed.
CSCwd63861	SIGSEGV crash is observed when incrementing roaming statistics.
CSCwd69780	Controller crashes due to NetFlow watchdog. Observed CPU hog in the wncmgrd process due to NetFlow scale.
CSCwd72847	Cisco Catalyst 9115 APs intermittently stop transmitting multicast traffic downstream.
CSCwd74571	Wcpd crashes after reusing freed packets.
CSCwd77823	Cisco Catalyst 9130 AP radio firmware reloads unexpectedly.
CSCwd79178	Cisco Aironet 1840 OEAP crashes due to radio failure.
CSCwd80290	Cisco Wave 1 AP image validation certificate failure or expiry causes 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!".
CSCwd86288	Load average warning is displayed even when Cisco Catalyst 9800-80 Series Controller is healthy.

Identifier	Headline
CSCwd90380	Access point page shows Power Mode as unknown power.
CSCwd90472	Adding static IP MAC binding to device tracking fails.
CSCwd90909	Cisco Catalyst 9115 AP radio 1 crashes.
CSCwd91054	Cisco Wave 2 APs do not encrypt EAP_ID_REQ after M1-M4, and does not update PMKID for dot1x OKC.
CSCwd98332	Controller crashes after failing to match the interface ID in the anchor message.
CSCwe04602	COS AP fails to forward traffic to wireless client for about 60 seconds in SDA Fabric WLANs.
CSCwe07297	Cisco Catalyst 9120 AP reloads unexpectedly due to radio firmware crash.
CSCwe07802	Cisco APs such as 2800, 3800, 4800, and 1562 are dropping upstream EAP packets.
CSCwe11476	Cisco Catalyst 9130 AP: Kernel panic with filp_close and do_close values.
CSCwe11547	Crash is seen on "Critical process rrm fault on rp_0_0 (rc=139)".
CSCwe12057	Controller QoS page does not load when ACL has double quotes as special character in the name.
CSCwe14729	Controller reloads due tomemory corruption when processing DHCP Reply Option82.
CSCwe18012	Standby controller crashes while saving tbl QoS table.
CSCwe18185	Day 0 factory image for a new out-of-the-box Cisco Catalyst 9130 AP (VID 03) does not contain `iox.tar.gz`.
CSCwe19858	Cisco Catalyst 9130 APs advertise incorrect Local Power Constraint value in management frames.
CSCwe35906	Cisco Catalyst 9117 AP: Radio firmware crash is observed.
CSCwe55390	Spectralink Versity 9553 phones experience sporadic delay and robotic voice.
CSCwa81938	Cisco Catalyst 9130 AP experiences kernel unresponsiveness while recovering from the radio reset.

Resolved Caveats for Cisco IOS XE Amsterdam 17.3.6

Caveat ID	Description
CSCwa26814	Cisco Aironet 3800 Access Point does not pass Address Resolution Protocol (ARP) requests in central WLAN when configured in custom flex group.
CSCwa31596	Cisco Catalyst 9130AX Access Point experiences high channel utilization and client lags with 9 or more clients using MS Teams.
CSCwa42620	Cisco Catalyst 9130 Access Point drops packets On-Air for Phoenix WinNonlin application.
CSCwa54943	Cisco Wave 2 Access Points with RLAN port connected to device running LLDP reboots due to Out-of-Memory.
CSCwa68439	Cisco Aironet 3800 Access Point sends a burst of deauthentication frames after each session timeout for each Access Point in PSK WLAN.
CSCwa75901	Cisco Catalyst 9117 beacon stuck reloads unexpectedly due to radio failure (radio recovery failed).
CSCwa77205	Cisco Aironet 1832, 1852, or 1815: Kernel panic is observed at **wlan_handle_napi**.
CSCwa81190	Cisco Catalyst 9120 Access Point crashes with Null pointer dereference in **wlc_wnm_is_wnmsleeping**.
CSCwa82660	Cisco Aironet 2800 or 3800 Access Points only update the **QBSS_AAC** sent by the controller after radio reset when CAC is configured.
CSCwa86015	Cisco Catalyst 9120 Access Point experiences kernel panic crash when PC is at __kmalloc+0x5c/0x140.
CSCwa86610	Cisco Aironet 2802 and 3802 Access Points experience kernel panic crash when 8.10.151.0 image is executed.
CSCwa88621	Cisco Catalyst 9120AXI Access Point - capwapd.service failed.
CSCwa90871	Cisco Catalyst 9120 Access Point running Cisco IOS-XE 17.7.1.11 experiences wcpd.service failure software crash in wcpd process.
CSCwa96198	Central Web Authentication (CWA) clients with RUN state cannot go online even though it is in RUN state.
CSCwa96429	Cisco Wave 2 Access Point disconnects from the controller after a CTS switchport configuration.
CSCwa97033	Cisco Catalyst 9120 Access Point experiences kernel crash while bringing up the slot1 radio.

Caveat ID	Description
CSCwb05556	Cisco Catalyst 9120 Access Point does not send multicast data till it snoops IGMPv2.
CSCwb07125	Access Points detect its own MAC addresses as rogue in slot1 or slot3 intermittently with an empty SSID.
CSCwb08755	Cisco Catalyst 9130 and 9120 Access Points in FlexConnect mode does not send SA query.
CSCwb09248	High latency and drops are observed when associated to Cisco Catalyst 9130 Access Point.
CSCwb09642	Enhanced diagnostics is required to determine why Cisco Catalyst 9130 Access Point reloads unexpectedly with "PC is at run_timer_softirq".
CSCwb11711	Cisco Catalyst 9120 and 9130 Access Points in FlexConnect mode sends Assoc reject after a first successful connection.
CSCwb19448	Cisco Catalyst 9117 Access Point reloads unexpectedly due to kernel panic in "cisco_wlan_crypto_decap".
CSCwb23976	Cisco Catalyst 9117 Access Point reloads unexpectedly due to kernel panic "dp_print_host_stats".
CSCwb28006	Cisco Aironet 3800 Access Point plumbs client to VLAN 1 instead of native VLAN 0 causing ARP drops "OUTER_UCAST_VLAN_BLOCK".
CSCwb30993	Cisco Catalyst 9117AXI-E Access Point reports kernel panic crash.
CSCwb32121	Cisco Aironet 1832 Access Point reloads due to radio failure - Beacon Stuck- reset radio for recovery.
CSCwb34215	Cisco Catalyst 9115AXI-E Access Point crashes after upgrading to Cisco IOS-XE 17.3.5a.
CSCwb34231	Cisco Catalyst 9115 Access Point: Power saving client state in radio.
CSCwb36531	Cisco Catalyst 9130 Access Point does not process fragmented Extensible Authentication Protocol (EAP) frames from client when doing EAP-TLS.
CSCwb53348	Cisco Catalyst 9130 Access Points generate radio coredumps.
CSCwb62329	Cisco Catalyst 9120 Access Point does not send the Aggregate MAC Protocol Data Unit (AMPDUs) for WPA1 AES clients in WPA1 and WPA2 mixed modes.
CSCwb68720	Cisco Catalyst 9120 or 9130 Access Points send Address Resolution Protocol (ARP) packet without VXLAN encapsulation.

Caveat ID	Description
CSCwb70757	Cisco Catalyst 9130 Access Point reloads unexpectedly due to kernel panic.
CSCwb71679	Cisco Aironet 4800 Series Access Point in 8.10.171.0 crashes due to FIQ or NMI reset.
CSCwb76935	Cisco Aironet 1815-T OEAP kernel panic crash is observed in Cisco IOS-XE 17.8.1 CCO.
CSCwb94209	Cisco Catalyst 9115 Access Point: The Mode reset button does not clear the CC mode and console blocking configuration.
CSCwb95980	Cisco Catalyst 9130 Access Point experiences kernal crash when PC is at _ZN10CACMetrics25accumulate.
CSCwb97557	SJC Alpha Cisco Aironet 3800 Access Points in Cisco IOS-XE 17.9.1 EFT2 Slot 0 BSSID beacon frames are received in Slot 1 radio.
CSCwc06293	Cisco Catalyst 9120 Access Point stops beaconing.
CSCwc07421	Cisco Aironet 4800 Access Point displays its own MAC address in the NDP neighbor list.
CSCwc09461	Cisco Catalyst 9120 Access Points send Authentication response frames to clients after long delays.
CSCwc15229	Cisco Aironet 1832 Access Point reloads due to radio failure - Beacons are stuck in radio.
CSCwc20929	APP hosting segmentation does not work in Cisco Catalyst 9100 Acces Point and Cisco Catalyst 9800 controller running Cisco IOS-XE 17.6.3.
CSCvv20610	Workgroup bridge (WGB) does not support the pre-shared key (PSK) with 63 characters.
CSCvw10013	Cisco Aironet 1852 Access Point radio hangs causing packets drops.
CSCvz66623	Clients with EAP-TLS behind the Mesh Access Point (MAP) fails.
CSCwa05828	Cisco Catalyst 9105 Access Point does not respond to controller's Discovery Response: Error connecting Transport Layer Security (TLS) context.
CSCwa33537	Cisco Catalyst 9117AX Access Point radio reloads unexpectedly due to partial command issues.
CSCwa36216	Cisco Catalyst 9120AXI Access Point sends weaker beacons than Cisco Aironet 2802I Access Point.
CSCwa49086	Cisco Aironet 3802 FQI or NMI reset: LocateAddr & extStaDb_GetStaInfo.

Caveat ID	Description
CSCwa53727	Cisco Catalyst 9117AX Access Point reloads unexpectedly at cmnos_thread.c:3493.
CSCwa59673	Cisco Aironet 3802 FQI or NMI reset at rb_next+0xc.
CSCwa61087	Cisco Aironet 1562 Access Point acting as Workgroup bridge (WGB) is unable to pass multicast traffic to the passive client behind it.
CSCwa73820	Cisco Aironet 4800 Access Point does not get full 31or 32 Watt power while negotiating with UPOE SW.
CSCwa77633	Cisco Aironet 1832 Access Point reloads unexpectedly due to kernel panic.
CSCwa79564	Cisco Aironet 2800 and 3800 Access Points in 8.10.162: Incorrect Power Type is displayed when static power is set to 15.4W.
CSCwa85088	Wired client behind Cisco WGB does not consider the DHCP IP address.
CSCwa95705	Cisco Aironet 2802 Access Point reloads unexpectedly due to FIQ or NMI reset.
CSCwb02488	Cisco Catalyst 9120 Access Point experiences kernel crash when PC is at number.isra and LR is at vsnprintf.
CSCwb05569	Cisco Catalyst 9130 Access Point does not transmit beacons randomly.
CSCwb08956	Cisco Aironet 2800 Access Points changes the TID for Extensible Authentication Protocol (EAP) over LAN (EAPOL) packets from 6 to 0 after changing the RF profile in the controller.
CSCwb11854	Low throughput is observed in Cisco Aironet 1852 Access Point.
CSCwb19680	Incorrect kernel assertion is observed while checking invalid timer objects.
CSCwb19993	Cisco Wave 2 Access Point looses configuration after an upgrade.
CSCwb45599	Cisco Access Point reloads unexpectedly with ppr_create_prealloc+0xbc.
CSCwb73294	Cisco Catalyst 9105 Access Point experiences low throughput with AX clients with adjacent channel interference in 2.4-GHz radio.
CSCwb76882	Cisco Catalyst 9130 Access Point detects its own BSSID as rogue in 5-GHz channel.
CSCwb98247	Cisco Access Point reloads unexpectedly in "wlan_objmgr_peer_release_ref" running Cisco IOS-XE 17.3.5.

Caveat ID	Description
CSCwc04079	Cisco Wave 2 Access Point in WGB mode running 8.10.171.4 is unable to assign a static IP with subnet mask other than /24.
CSCwc05350	Cisco Wave 2 Access Points: CAPWAP MTU flapping occurs due to asymmetric MTU between Access Point to controller and vice-versa.
CSCwc07002	Access Point crash is observed due to kernel panic - pci_generic_config_read CS00012247092.
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.
CSCwc51428	Cisco Catalyst 9130 Access Point: Kernel panic. __dma_inv_range+0x20/0x50.
CSCwc51894	Cisco Catalyst 9117 Access Point reloads unexpectedly due to kernel panic with "dp_print_host_stats" logs.
CSCwc54470	The **config boot crashkernel enable** Cisco Wave 2 Access Point command does not generate kernel core to USB.
CSCwc56774	WGB with Static IP loses IP address after multiple roams.
CSCwc60528	Assert crash is observed in Cisco Catalyst 9120 Access Point.
CSCwc71198	CAPWAP flapping is observed when VRRPv3 is present in the network.
CSCwb13784	Access Points are unable to join the controller due to invalid path MTU in the Access Point Join request.
CSCvu37120	Dataplane classification error is observed in WLCLIENT-IF interface.
CSCvx17641	Cisco Catalyst 9105 Access Point experiences wncd traceback followed by wncd crash.
CSCvx28901	C9800:"% TDL error: thrown while configuring clients under manual exclusion list in Cisco IOS-XE 17.6.1.
CSCvy30606	Cisco Catalyst 9800 Wireless Controller fails to update sdn-network-infra-iwan key after a year.
CSCvy53756	Pubd crash is observed with tdl_get_manifested_type_info_ptr_mem in 200 Access Points mesh configuration with telemetry subscriptions.
CSCvy63924	Telemetry: Cisco IOS-XE controller crashes after using **show telemetry ietf subscription all** command.

Caveat ID	Description
CSCvz82509	GUI does not load the AVC page from **Configuration** > **Services** > **AVC**.
CSCwa10377	Cisco Catalyst 9800-80 Wireless Controller in SSO running 17.03.04 with APSP and SMU crashes causing unexpected HA failure.
CSCwa50929	Controller crashes within 10 minutes after starting the pure intra wnc roam at 600 Clients Per Second.
CSCwa64326	Controller crashes due to memory leak in Simple Network Management Protocol (SNMP) process.
CSCwa67566	Controller rejects clients with wrong PMKID when changing AKM from FT to dot1x and FT again.
CSCwa69631	Controller crashes during webauth AAA routines generating wncd core.
CSCwa70649	Improve serviceability to figure out the reason for blacklisting 802.11w client.
CSCwa73179	SSDP does not function across VLANs for wireless clients in the same UDN domain.
CSCwa73294	17.3.5: The show commands, HTTPS, and SNMP stops working in Cisco Catalyst 9800-80 Wireless Controller when DBM process CPU stays high at 100%.
CSCwa76898	WLAN stopped broadcasting after a configuration change in the WLAN profile.
CSCwa77214	Controller crashes at ewlc_wlanmgr_wlan_ref_count_cleanup_timer_cb.
CSCwa78384	Segfault is seen when updating the 802.11 client parameters.
CSCwa79968	SNMP MIB at times does not return all data or no data at all for SNMP walk with high client count.
CSCwa82644	Controller displays incorrect available bandwidth calculations for QBSS_AAC with voice CAC and FlexConnect AP.
CSCwa88790	Controller crashes during mobility routines generating wncd core.
CSCwa99904	Controller deletes the client when DHCP RELEASE is sent by the client during Posture.
CSCwb05014	Controller crashes in WNCd when changing the "mac ip binding" configuration.
CSCwb09214	Controller sends QBSS_AAC with zero available bandwidth after DEL TS.

Caveat ID	Description
CSCwb15700	Intermittent crash is observed in the active controller with Port channel in QoS code.
CSCwb21141	Cisco Catalyst 9800 Wireless Controller related WLAN configuration is not pushed to APs during a specific wncd.
CSCwb24037	Client gets stuck in **Authenticating** state after failing the Broadcast key rotation process.
CSCwb27940	Client gets deleted due to VLAN failure after performing L3 roaming when VLAN persistency is enabled.
CSCwb31335	Standby controller goes to standby recovery when Gateway Failover is enabled.
CSCwb35196	High CPU utilization is observed in wncd due to continuous log in ra_trace "WebAuth info not found while termin".
CSCwb37940	Clients randomly gets excluded in the Controller with the "CO_CLIENT_DELETE_REASON_EXCLUDE_VLAN_FAIL" reason.
CSCwb39307	AAA server does not mark as UP, even reachable, and client does not authenticate through the server.
CSCwb42717	Cisco Catalyst 9800-80 Wireless Controller crashes due to "ewlc_capwapmsg_free_msgbuf_internal".
CSCwb45089	The controller HTTPS access is broken after an upgrade to Cisco IOS-XE 17.3.5a.
CSCwb47046	"wncmgrd" process memory leak is observed in Cisco IOS-XE 17.8.
CSCwb57391	Controller deletes client after roaming with "CO_CLIENT_DELETE_REASON_IP_DOWN_NO_IP" reason.
CSCwb65356	Controller reloads with the reason "Critical process wncd fault on rp_0_0 (rc=139)".
CSCwb69531	Controller initiates EAPOL retries for the client in **RUN** state.
CSCwb73136	Clients in RUN state are unable to pass traffic after Change of Authorization (CoA) is completed.
CSCwb80500	Memory leak is observed in the WNCD process due to Unknown responses from the RADIUS server.
CSCwc01644	Cisco Wave 2 Access Points use native VLAN instead of VLAN used in the Policy Profile.
CSCwc04197	Secondary controller crash is observed during redundancy switchover.

Caveat ID	Description
CSCwc14629	GUI takes a long time to display the initial page due to http request wirelessDeviceSummary.
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.
CSCwc32226	Zebra RF Gun clients are unable to get the IP address and gets stuck in IPLEARN STATE.
CSCwc34322	Controller deletes client due to DELETE_REASON_MOBILITY_FAILURE triggered by WEBAUTH_ON_MAB_FAILURE_ROAM.
CSCwc42784	Client fails to connect when protocol based Quality of Service (QoS) is configured.
CSCwc59518	Cisco Catalyst 9800-80 Wireless Controller crashes with reason Critical process wncd fault on rp_0_3 (rc=134).
CSCvx84936	Cisco IOS-XE controller sends SNMP client intance in SNMP wireless client traplogs.
CSCvy69694	Access Point network icon is missing in the 17.5.1 GUI for Privilege Level 1 users instead you get to view the config icon.
CSCwa51748	Cisco Catalyst 9800 Wireless Controller generates cpp-mcplo-ucode cpp_fatal_internal in 17.7.1 image.
CSCwa52721	Access Point does not assign native VLAN when there is no vlan-id configured in the Policy Profile.
CSCwa56574	"Band Selection" does not change from 2.4-GHz to 5-GHz when performing the operation using 2.4-GHz radios.
CSCwa74884	Controller sends wrong payload information to AP when mesh RRM is enabled or disabled.
CSCwa76445	SNMP cLMobilityGroupMembersOperEntry table is not working.
CSCwa77027	RADSEC counter always remain zero.
CSCwa82133	Controller crashes with "Critical process nmspd fault on rp_0_0 (rc=1)".
CSCwa94092	ARP Broadcast in GUI is shown as DISABLED for some VLANs even though it is enabled in VLAN configuration.
CSCwa95336	Static workgroup bridge (WGB) client does not move to RUN state in the controller.

Caveat ID	Description
CSCwa99102	The controller GUI does not display trustpoints in the PKI Management Trustpoints tab.
CSCwb05825	MAC authentication bypass (MAB) client does not move to exclude state during a MAB failure.
CSCwb15031	Client is unable to pass traffic after roaming using WPA2 Opportunistic Key Caching (OKC).
CSCwb15884	Memory depletion and high WAN latency is observed in FlexConnect deployment.
CSCwb17280	Japanese GUI displays wrong Mesh information.
CSCwb19227	Interim update is not sent to AAA during client reassociation or roam in GA.
CSCwb22347	Image download profile special character support.
CSCwb22867	WNCD process crash is observed when applying Cisco ATF profiles.
CSCwb26543	Ethernet over GRE (EoGRE) client traffic stops working after an SSO.
CSCwb28057	Cisco Catalyst 9800-CL Cloud Wireless Controller crashes after updating the WLAN configuration.
CSCwb35119	Invalid logging level is observed for Locator ID Separation Protocol (LISP) log.
CSCwb35761	Incorrect VLAN is assigned to initiate SIP when SIP and AAA override combination is used.
CSCwb37457	Standby controller crashes when the controller is configured in RMI+RP High Availability mode and wired guest feature.
CSCwb39675	AP XOR radio role mismatch between GUI and CLI.
CSCwb43261	Dropping the packets in Cisco Catalyst 9800-CL Cloud or Cisco Catalyst 9800-L Wireless Controller when the call snooping is enabled and call cannot be established.
CSCwb45549	Controller Web UI does not allow WPA-TKIP only configuration.
CSCwb47040	Controller does not update radio frequency identification (RFID) location properly.
CSCwb58100	Unable to map SSID with spaces in it on an attribute list.
CSCwb63861	WLAN clear refcount command does not accept WLAN names with special characters.

Caveat ID	Description
CSCwb64761	Controller discards the location updates from radio frequency identification (RFID) tags.
CSCwb67450	The **show process cpu platform sorted** command is required in **show tech wireless**.
CSCwb78191	The AAA VLAN override is not considered with iPSK authentication and anchor WLAN.
CSCwb93513	Stale client entries are not deleted and stuck in device-tracking database.
CSCwb99793	CRL verification failure results in 400 Bad Request with DigiCert.
CSCwc17774	Few OIDs in CISCO-ENHANCED-MEMPOOL-MIB display No instance after switchover in Cisco IOS-XE 17.6.1.
CSCwc28408	Controller crashes intermittently due to wncd critical process failure.
CSCwc41358	Controller MAC filtering: WLAN profile column displays the WLAN name and description.
CSCwc41903	Syslog "LISP RELIABLE REGISTRATION" needs to be enhanced.
CSCwc57312	L2VNID number in the controller command line and GUI are different.
CSCvt66135	Verify traffic flow in RP port similar to Internet Control Message Protocol (ICMP) displaying RTT drops and "show int" command.
CSCvt66147	Controller needs to display the counters of devshell in ethtool -S ha_port.
CSCvw19807	Warn users if a configuration is not applied correctly and remedial steps are to be performed.

Resolved Caveats for Cisco IOS XE Amsterdam 17.3.5b

Caveat ID	Description
CSCwb13784	APs are unable to join the controller due to invalid Maximum Transmission Unit (MTU) in AP join request.
CSCvu37120	Traceback is observed when QoS policy is removed in CPP, client is unbound from the policy, and Address Resolution Protocol (ARP) is still flowing.
CSCvz96924	Cisco Catalyst 9130 Access Point does not send M1 over the Air.
CSCwa31596	Cisco Catalyst 9130AX AP: High channel utilization and client lags are observed with 9 or more clients using MS TEAMS.

Caveat ID	Description
CSCwa50929	Controller crashes within 10 minutes after starting the pure intra wnc roam at 600 Clients Per Second.
CSCwa77214	Controller crashes at ewlc_wlanmgr_wlan_ref_count_cleanup_timer_cb.
CSCwb05556	Cisco Catalyst 9120 AP does not send multicast data till it snoops the IGMPv2.
CSCwb15700	Intermittent crash is observed in the active controller in Quality of Service (QoS) code with Port channel.
CSCwb45089	HTTPS access is broken after the controller is upgraded to 17.3.5a.
CSCwb68720	AP sends Address Resolution Protocol (ARP) packet without VXLAN encapsulation.
CSCwa53592	Cisco Catalyst 9120AX APs in 17.3.4c release show Flexible Radio Assignment (FRA) as not capable although FRA is enabled.
CSCwb05569	Cisco Catalyst 9130 Access Point does not transmit beacons randomly.
CSCwb64761	Controller discards the location updates from RFID tags.
CSCwb52379	AP randomly changes CAPWAP next-hop MAC due to irrelevant Address Resolution Protocol (ARP).
CSCwa92678	Controller crashes due to leak in mobilityd causing invalid ID when controller runs out of IDs.
CSCvy67650	Controller does not send TCP SYN or ACK for web redirect once TCP SYN is received and punted to CPU.

Resolved Caveats for Cisco IOS XE Amsterdam 17.3.5a

Caveat ID	Description
CSCwb13784	APs are unable to join the controller due to invalid path MTU in AP join request.
CSCwa12204	Controller does not send the correct association ID (AID), causing APs to reject new client associations.
CSCvz89976	The controller crashes due to Work Group Bridges (WGBs), in the 17.3.4 version.
CSCwa23632	Cisco Catalyst 9800-80 Wireless Controller crashes on 17.3.4ES9 version.
CSCvx43471	OEAP authentication failure is observed on the controller running 17.3.3EFT4.

Caveat ID	Description
CSCvx64169	The **request platform software trace archive** command throws an error.
CSCvx71141	Cisco Catalyst 9800-80 Wireless Controller crashes due to a CPU hog in the Radio Resource Management (RRM) process.
CSCvx81815	Controller does not send server hello packets to AP when enabling the Data Datagram Transport Layer Security (DTLS) encryption.
CSCvy73244	Cisco Catalyst 9800-80 Wireless Controller: Application visibility configuration page does not load when 99 or more policy profiles have the Cisco Application Visibility and Control (AVC) enable.
CSCvy73730	Controller may experience a crash in the cpp-ucode process due to a misaligned DesignatedTransit List (DTL).
CSCvy73836	Cisco Catalyst 9800-80 Controller goes to ROMMON after multiple failovers due to power cycling.
CSCvy82035	Controller deauthenticates client when receiving DHCP release from the client (17.3.3).
CSCvy84153	Crash is observed in the controller when the AP location name is greater than 32 characters.
CSCvy89423	'WNCMGRD' process crashes due to segmentation fault in the controller.
CSCvy90646	Controller drops the incoming CAPWAP keepalive for random APs.
CSCvy99116	A crash is observed when a wireless client attempts to connect and the connection times out.
CSCvz06544	Controller crashes when enabling the RMI+RP in WebUI before bringing High Availability (HA) connectivity up first.
CSCvz08303	Controller reloads unexpectedly in the dBm process when DBAL batch stops executing.
CSCvz11154	Continuous memory leak with multiple table entries is observed in FMAN database.
CSCvz15015	Cisco Catalyst 9130AX AP loses its WLAN configuration after moving between controllers.
CSCvz28378	Memory leak observed in WNCD process running 17.3.3 of around 200MB per day.
CSCvz37723	Cisco Catalyst 9800-80 Wireless Controller: Crash in mobilityd mcfsm_decrement_client_count.

Caveat ID	Description
CSCvz45305	Controller is missing fields in the access-request when sending it for a sleeping client.
CSCvz45488	Memory leak is observed in EWLC_OPERATIONAL_DB causing dbm crash.
CSCvz45576	Rogue telemetry updates need to be throttled as the controller sends lot of Rogue reports to Cisco DNA Center (DNAC).
CSCvz52851	Single Sign-On (SSO) switchover does not re-establish LISP sessions to the CPs.
CSCvz52986	Crash observed in C9800-80-K9 while the running 17.3.4 version.
CSCvz54928	Client gets stuck in IP learn due to stale entry.
CSCvz56650	Configuration changes in WLAN or policy profile causes Service Set Identifier (SSID) to stop the broadcast.
CSCvz59495	Accounting requests messages sent in a stream causes issues in the RADIUS server.
CSCvz60614	WNCD core seen on 17.3.3 CCO image with assert failures observed.
CSCvz63742	Controller does not provide cLApAdminStatus info through SNMP when forensic AWIPS is configured.
CSCvz64802	Controller reloaded due to a memory corruption in WNCD.
CSCvz67166	Controller drops CAPWAP connections due to high WNCD CPU.
CSCvz67806	Central DHCP configuration is not propagated on AP correctly.
CSCvz68857	Optimize bsnMobileData OID query to improve performance.
CSCvz77768	IOS AP brings the radio down after encountering DFS event even when non-DFS channels are available.
CSCvz78859	Flexible NetFlow (FNF): cpp ucode core and reload after invalid access to internal hash table.
CSCvz80697	Controller does not remove old NMSP entries when new probes are received in a different slot.
CSCvz81043	Controller crash after AP session closes.
CSCvz84691	Controller crashes due to WNCD process when learning an IP address for a client.
CSCvz89741	Cisco DNA Center experiences performance issue. Controller sends a large number of events for new clients associating with the AP having maximum number of clients.

Caveat ID	Description
CSCvz95745	The CleanAir interference devices are not merged in clusters.
CSCvz97915	Controller standby reloads with device-classifier configuration and the **write memory** command execution, parallelly.
CSCwa07257	Cisco Wave 2 APs stop authenticating clients using Flex Local Authentication.
CSCwa20681	FRA change is needed from from the controller.
CSCwa23659	Controller stops accepting APs to join - No response after DTLS Client Hello received from AP.
CSCwa26602	Controller adds universal._sub._ipp and universal._sub._ipps to the default-mdns-service list.
CSCwa27041	Controller performs an unexpected reboot with Network Mobility Services Protocol (NMSP).
CSCwa29446	VLAN Trunk Protocol (VTP) is broken on the controller. VLAN information is not propagated to the controller.
CSCwa30458	High CPU provked by "rif_mgr"process.
CSCwa33929	Contoller drops DHCP after reboot.
CSCvr58932	ZTP overwrites *http* authentication aaa/not applying VTY authorization and accounting settings.
CSCvv15144	SNMP objects missing for AP neighbor and radio stats information missing on the controller.
CSCvv94885	The **show ap cdp neighbors** command displays the name of the switch instead of the domain name.
CSCvx94276	%CRIMSON-3-DATABASE_MEMLEAK: Database memory leak detected in /tmp/rp/tdldb/0/IOS_PRIV_OPER_DB.
CSCvy15384	Datapath state mismatch strands are observed in wireless clients after roaming.
CSCvy53122	AP Tag summary page shows incorrect status in the RF section.
CSCvy72750	Wireless controller is unable to use the **wireless broadcast vlan** command.
CSCvy74904	AP authorization related RADIUS request does not include the calling station ID and NAS port type.
CSCvy76922	Switch stack with Cisco IOS XE 17.3.2a displays high memory alerts.

Caveat ID	Description
CSCvy87749	Controller sends DHCP as relay proxy even after removing ip helper from the client SVI interface.
CSCvy94284	Controller crashes when running the **clear wlan id** command.
CSCvz05555	DCA channel Dwell Times gets updated even when there is no channel change seen on the AP.
CSCvz17623	Memory leak is observed in emulated database and AP join.
CSCvz39749	Client location probe displays error when probe request parsing fails.
CSCvz53408	FT IE is sent as 0 in M3 after session timeout.
CSCvz60451	Memory leak is observed in C9800-CL due to native telemetry.
CSCvz67033	Controller sends an extra accounting interim update to AAA when client re-associates to same BSSID.
CSCvz72172	The status of the **snmp trap link-status** command not change after reload.
CSCvz76229	Cisco C9500-48Y4C misses air licenses.
CSCvz82335	Install/ISSU state is not cleared after the **clear install state** command is issued.
CSCvz97359	FlexConnect roaming issue occurs due to PMKID mismatch at controller.
CSCwa05238	Controller GUI does not delete the hotspot configuration correctly.
CSCwa08842	Cisco Wave 1 APs are shown in downloading state because of MD5 Mismatch running the code 17.3.4.
CSCwa10594	MAC Address entry not saved on the GUI when mapped to WLAN profile with spaces.
CSCwa12806	Controller has stale AP entries that stop further AP configuration.
CSCwa16467	Controller needs cleanup of client entry authentication when client is in RUN state on any controller in the network.
CSCwa23606	Controller does not present full certificate in web admin.
CSCwa32317	The Timezone configuration in the GUI does not work. The 'show clock' displays incorrect timezone.
CSCwa35309	High Availibility: Standby CAPWAP plumb failure.
CSCwa39002	AP channel width configuration from GUI is not taking effect but displays successful message.

Caveat ID	Description
CSCwa52109	Vendor OUI mismatch prints wrong message for disassociation request and denying client association.
CSCvz30883	Cisco Catalyst 9120 APs running 17.3.4ES2 gets stuck and does not acknowledge any of the received frames.
CSCvw70285	Cisco Catalyst 9120 APs cannot send acknowledgement over the air during EAP negotiation.
CSCvy59897	Cisco Wave 2 APs detect its own BSSID as rogue.
CSCvy62022	Roaming client stops receiving IP multicast in a new Cisco Aironet 3800 AP.
CSCvy75868	Cisco Wave 2 APs crash due to kernel panic.
CSCvy79320	Increased ping loss after two days of reboot.
CSCvy85178	Cisco Catalyst 4800 APs in the ELM and Local mode, on same controller and same RF group detect each other as honeypot.
CSCvz05686	Cisco Aironet 2802 or Cisco Aironet 3802 AP fails to bring up its radios and continuously logs messages.
CSCvz09846	Cisco Catalyst 9130 AP stale clients in the radio driver table causes associations to fail.
CSCvz09942	Cisco Catalyst 9120AXI AP displays kernel panic in Cisco IOS XE 17.3.4.30.
CSCvz21627	Cisco Aironet 3800 Series or 4800 Series WIPS AP does not list few BSSIDs in the RRM neighbor list causing false honeypot alarms.
CSCvz24841	802.11r retried auth packet forwarded to the controller causes duplicate auth responses sent to client.
CSCvz25183	Cisco Wave 2 AP's fragmenting CAPWAP discovery packets are unable to join the controller.
CSCvz34172	Cisco Aironet 1832 Series AP experiences kernel panic while setting client ACL.
CSCvz46237	Cisco Catalyst 9130 Series AP crashes on Cisco IOS XE 17.3.4 CCO version.
CSCvz49187	Cisco Catalyst 9120 Series AP sends packets with QoS TID when WMM is disabled on WLAN.
CSCvz55681	Cisco Catalyst 9120AXI-B APs crash when joining Cisco Catalyst 9800-CL wireless controllers running Cisco IOS XE 17.6.1.

Caveat ID	Description
CSCvz64239	Cisco Aironet 1815 Series AP crashes and the radio does not come up.
CSCvz66798	Cisco Catalyst 9120 Series AP in FlexConnect mode drops ARP request from the client to the gateway after a WLAN change (Local to Central).
CSCvz69441	Cisco Catalyst 9115 Series AP experiences crash due to kernel panic PC.
CSCvz89108	Cisco Catalyst 9120 Series AP - NDP received frames from neighbour AP with RSSI that is lower than the configured RxSOP.
CSCvz94267	Cisco Catalyst 9130Series APs crash after upgrading to 17.3.4 and applying the ESW7 image.
CSCvz95929	PSM microcode watchdog fired (in seconds) with Cisco Catalyst 9120 Series APs.
CSCwa01142	Cisco Catalyst 9120 Series APs not responding to client association requests.
CSCwa06321	Cisco Catalyst 9120 Series APs - Change parameter under WLAN resets Cisco Catalyst 9120 Series AP radio.
CSCwa18545	Cisco Catalyst 9120 Series AP - PS PRETEND changes the client to Power Save mode even when the client is replying to QoS Null sent by the AP.
CSCwa20219	Cisco Catalyst 9120 Series AP radio 1 gets stuck in TX.
CSCwa26257	Cisco Catalyst 9120 Series AP kernel crash.
CSCwa30802	TCQ stuck due to MU sounding errors.
CSCwa50159	Cisco Catalyst 9120 Series APs show high client count while the neighboring APs have very few clients associated.
CSCwa53266	Cisco Catalyst 9120 Series AP randomly retains 11w client though it is deleted from the controller.
CSCwa57967	Cisco Catalyst 9130 Series AP Slot 2 Mode changes to local when the AP is on FlexConnect mode.
CSCvu75017	Cisco Wave 2 APs and 11AX APs syslog only seen when using the "Kern" facility value in AP join profile.
CSCvw93936	Cisco DNA Center Assurance's Client 360 window shows the wireless client SNR value as 0 for Cisco Catalyst 9115 Series APs and Cisco Catalyst 9120 Series APs.
CSCvx37663	Cisco Aironet 1832 AP displays `/usr/sbin/capwapd: writing to fd 17 failed!: Input/Output error`.

Caveat ID	Description
CSCvx96224	Numerous core dumps are observed in Cisco Aironet 2800 Series APs and Cisco Aironet 3800 APs slot 1 radios.
CSCvy11334	The Non-WiFi Channel Utilization section displays 41 instead of BLE Beacon.
CSCvy13594	Cisco Catalyst 9130 Series AP experiences radio firmware crash on Radio 1, multiple times in a day.
CSCvy30091	Cisco Catalyst 9120 Series AP stops transmitting to MacBook after a session re-authentication.
CSCvy48763	Cisco Catalyst 9130 Series AP crashes due to kernel panic after N+1 failover or fallback.
CSCvy91441	Cisco Aironet 2802 AP experiences radio crash.
CSCvy94725	Cisco Aironet 2800 APs and Cisco Aironet 3800 APs experience Kernel Panic Driver crash when PC is at wlRxRingCleanup.
CSCvy95264	Workgroup bridge (WGB) cannot associate when PSK password contains special characters.
CSCvy95842	Connected AP with non-EWC image undergoes factory reset after reload when DHCP option 43 is set.
CSCvz02579	Cisco Catalyst 9130AXI AP cannot connect to the controller after shut or no shut on a Cisco Catalyst 9300 Series (C9300-48H) switch interface.
CSCvz06937	Cisco Catalyst 9120 Series AP FW crash is observed in Radio 1.
CSCvz18980	Opportunistic Key Caching (OKC) is not pushed from the controller to the AP when applied in the CLI.
CSCvz40749	Cisco Wave 2 AP probe filter to limit unwanted probes from the AP to the controller does not work.
CSCvz44787	Cisco Catalyst 9120AXE AP displays incorrect PID and description for Self Identifying Antenna.
CSCvz56061	Mobility Express cannot input WLAN user information CSV file on the GUI.
CSCvz57427	When the AP is disassociated due to link failure, AP reports the reason as 'AP crash'.
CSCvz58365	Cisco Catalyst 9130 Series APs unexpectedly reboot due to kernel panic.
CSCvz58499	Cisco Catalyst 9120 Series APs reload unexpectedly due to kernel panic on 2.4-GHz band.

Caveat ID	Description
CSCvz59574	Cisco Catalyst 9130 Series APs: Radio operates on channel 128 and publishes in channel 56.
CSCvz79327	Cisco Aironet 1832 Series AP crashes due to radio failure: Beacon Stuck - reset radio for recovery.
CSCvz87088	Cisco Catalyst 9120 Series APs in monitor mode cannot update the neighbor list causing false honeypot alarms.
CSCvz94692	Cisco Catalyst 9130 Series AP crashes due to radio failure (too many radio failures).
CSCvz99449	APs make too many connections to Identitymgmt causing Cisco DNA Center Identitymgmt to crash.
CSCvz99492	Cisco Catalyst 9130 Series AP unexpectedly reloads with a kernel panic.
CSCwa12278	Cisco Catalyst 9115 Series AP crashes due to kernel panic - not syncing: Fatal exception.
CSCwa20827	Controller shows that all 11AX clients are connected on 1 spatial stream.
CSCwa34136	Cisco Aironet 3802 Series AP in local mode reboots unexpectedly (FQI/NMI reset at rb_next+0xc).
CSCwa35428	Cisco Catalyst 9120 Series AP drops CAPWAP connection when running a debug client.
CSCwa45075	AP crashes at FW assert at ar_wal_peer.c:1553.
CSCwa45081	Cisco Catalyst 9130 Series AP crashes: KP at dp_rx_frag_handle+0x8c/0x8e0 [wifi_3_0].

Resolved Caveats for Cisco IOS XE Amsterdam 17.3.4c

Caveat ID	Description
CSCvu22886	Cisco Catalyst 9130 AP is displaying the message "unlzma: write: No space left on device" while upgrading to 17.7.x.
CSCvw70285	Cisco Catalyst 9120 APs cannot send acknowledgement over the air during EAP negotiation.
CSCvz30708	Controller stops sending RADIUS packets to the RADIUS server when accounting is enabled.
CSCvx71141	Cisco Catalyst 9800-80 Wireless Controller crashes due to a CPU hog in the RRM process.

Caveat ID	Description
CSCvy59897	Cisco Aironet 4800 Series AP in ELM mode detects its own BSSID as rogue.
CSCvy62022	Roaming client stops receiving IP multicast in a new Cisco Aironet 3800 AP.
CSCvy73836	Cisco Catalyst 9800-80 Controller goes to ROMMON after multiple failovers due to power cycling.
CSCvy90646	Controller drops the incoming CAPWAP keepalive for random APs.
CSCvz08303	Controller reloads unexpectedly in dbm process when DBAL batch stops executing.
CSCvz45488	Memory leak is observed in EWLC_OPERATIONAL_DB causing dbm crash.
CSCvz45576	Rogue telemetry updates need to be throttled as the controller sends lot of Rogue reports to DNAC.
CSCvz46237	Cisco Catalyst 9130 AP crashes on 17.3.4 CCO version.
CSCvz56650	Configuration changes in WLAN or policy profile causes SSID to stop broadcasting.
CSCvz59495	Accounting Requests messages sent in a stream causes issues in the RADIUS server.
CSCvz64239	Cisco Aironet 1815 APs experience crash in Cisco IOS-XE 17.3.4 ES image.
CSCvz68857	Optimize bsnMobileData OID query to improve performance.
CSCvz94267	Cisco Catalyst 9130 APs crash after upgrading to 17.3.4 and applying the ESW7 image.
CSCvx96224	Numerous core dumps are observed in Cisco Aironet 2800 and 3800 APs slot 1 radios.
CSCvy15384	Datapath state mismatch strands are observed in wireless clients after roaming.
CSCvz58365	Cisco Catalyst 9130 APs unexpectedly reboot due to kernel panic.
CSCvz58499	Cisco Catalyst 9120 AP reloads unexpectedly due to kernel panic on 2.4-GHz band.
CSCvz59574	Cisco Catalyst 9130 AP: Radio operates in channel 128 and publishes in channel 56.
CSCvz67033	Controller sends an extra accounting interim update to AAA when client re-associates to same BSSID.

Caveat ID	Description
CSCvz99492	Cisco Catalyst 9130 AP unexpectedly reloads with a kernel panic.

Resolved Caveats for Cisco IOS XE Amsterdam 17.3.4

Caveat ID	Description
CSCvx39497	WNCD process reloads unexpectedly due to Traffic Distribution Statistics.
CSCvv80531	Flex central auth + local switching 11w clients disjoin during Standalone to Connected transition.
CSCvv84296	Stale client entry leads to client disconnects and association problems.
CSCvw32545	Stale MAC entry in the member switch causes connectivity issues.
CSCvw55275	Controller reloads when AP sends frequent CDP updates and WNCD process ends abnormally.
CSCvw55697	AP cannot join the controller due to zero MAC received by a dropping client hello.
CSCvw69665	VLANs are not marked as dirty and client is in ip learn when client roams frequently between WNCD.
CSCvw93611	Incorrect accounting stop class attribute is observed while roaming with non-FT clients.
CSCvx35811	CWA clients are not moved back to webauth after CoA reauthentication is sent when client is in RUN.
CSCvx36012	AP disconnects after an SSO when CAPWAP multi window feature is enabled.
CSCvx37499	Controller reloads with the reason "Critical process wncd fault on rp_0_0 (rc=139)".
CSCvx44040	Cisco Catalyst 9800-40 WNCD utilises 100 percent of CPU due to local EAP authentication loop.
CSCvx44618	Devices get stuck when the controller consumes ICMP randomly from 8821 phones.
CSCvx44757	Controller in Fabric mode does not support VNID Override on web authentication.
CSCvx50248	Dot1x clients are unable to get IP intermittently while roaming.
CSCvx50299	APs are unreachable in the Inventory even though they are joined to the controller.

Caveat ID	Description
CSCvx69997	SNMP output displays only 27 WiFi clients from the controller.
CSCvx77928	RRM ends abnormally while executing the Grouping Flush pending list.
CSCvy11981	Controller ends abnormally due to WNCD (AP name length greater and equal to 32 characters).
CSCvy17995	Device-tracking doesn't change interface as the controller drops ARP request after roam and IP theft.
CSCvy20300	Primary controller in HA frequently ends abnormally.
CSCvy36594	Controller running EWA ACLs are lost after toggling HTTP or HTTPS server configuration from GUI.
CSCvy46043	Controller ends abnormally for SISF heap pointer to l2_socket_counter record.
CSCvv56712	AAA or RADIUS must fragment packets to the required size based on the MTU settings.
CSCvw45917	License command is not applied on bootup when loading config to C9800-CL using KVM bootstrap.
CSCvw88389	Check if the AP-COS crash files print complete information.
CSCvx16484	GUI does not display all locations configured in Wireless setup.
CSCvx27626	Apple clients fail to pass EAPOL M2 when 802.11r is enabled after a switchover.
CSCvx34926	The enable ap admin command does not work on slow systems when submitting a page after click action.
CSCvx58947	Controller sends "In Progress" status while making tunnel10 gateway down in the controller.
CSCvx80829	Ignore false positive reports managed by local or other controllers in the mobility group.
CSCvy02120	Cisco C9130 AP fails to send reassociation response to roaming clients randomly and deletes client.
CSCvy05019	The “show platform software system all" output does not display interfaces greater than 10.
CSCvy14956	Controller sends DHCP as relay proxy even when the client SVI interface is shutdown.
CSCvy16204	The allowed VLANs in an interface cannot be modified or viewed in the controller GUI.

Caveat ID	Description
CSCvy31684	WNCD table records in pending destroy are not being cleaned up.
CSCvy58934	Controller does not send the CAPWAP restart payload when filter is applied and AP name is changed.
CSCvx35154	Cisco 9105, 9115, or 9120 APs have hard time connecting and passing traffic in 2.4 GHz.
CSCvp88559	Cisco Aironet 1810W Access Point reloads unexpectedly due to kernel panic.
CSCvu71917	Cisco Aironet 1852 and 3802 APs experiences kernel panic during Flex suite run.
CSCvv66853	Transmission power levels in Cisco C9120 AP do not change when power levels are changed at 2.4 GHz.
CSCvv72100	Controller ends abnormally with /tmp at 100% when nginx process consumes space.
CSCvw10039	Cisco Aironet 2802 AP reloads unexpectedly due to kernel panic.
CSCvw83639	Cisco Aironet 2800 Series AP running release 8.10.130 reloads unexpectedly due to FIQ or NMI reset.
CSCvw84512	Cisco Aironet 3800 APs detects its own BSSID as rogue in slots 0 and 1.
CSCvx13166	Cisco Aironet 3802I running release 8.10.130.9 reloads unexpectedly due to kernel panic.
CSCvx18273	Cisco Catalyst 9120AX Series APs send reassembled fragmented packets in the uplink direction.
CSCvx19602	Cisco Catalyst 9120 Series AP beacon is stuck after moving from channel UNII 1 to UNII 2.
CSCvx27345	Cisco Catalyst 9800-CL Wireless Controller displays Neighbor APs as Rogue in 2.4 GHz band.
CSCvx29799	Configuration synchronisation fails between HA pairs in Cisco 8540 Wireless Controller.
CSCvx42772	Cisco Aironet 1832 AP ends abnormally due to kernel panic.
CSCvx43180	Controller running 8.10.130.0 in AP SSO mode ends abnormally due to "broffu_SocketReceive" Task Name.
CSCvx44338	802.11r retried auth packet forwarded to controller causes duplicate auth responses sent to client.
CSCvx47191	Client are stuck in Authenticating state after multiple roams across Cisco Catalyst 9130 APs.

Caveat ID	Description
CSCvx48238	Cisco 4800 AP is in a continuous boot loop when an unsupported code is pushed to AP in pre-download.
CSCvx52078	Cisco Aironet 2802 Series Access Point suddenly drops in transmission power level.
CSCvx56223	Cisco Catalyst 9120AX AP stops allowing new associations on any of the configured SSIDs.
CSCvx56259	FlexConnect central-auth 11r client roaming fails after Cisco AireOS is upgraded to 8.10.142.0.
CSCvx71577	Controller sends MDIE to IOS APS when WLAN is configured for adaptive FT enabled Flex Local Auth/SW.
CSCvx92866	Cisco Catalyst 9115AX Series APs frequently ends abnormally after the controller upgrades to 17.3.3.
CSCvx98447	AP ends abnormally with a crash file indicating Hostapd.service failed during boot.
CSCvy00017	Cisco Catalyst 9120 APs drop downstream packets of WGB clients.
CSCvy06837	Static IP address does not change when IP failover is toggled.
CSCvy14143	Cisco Catalyst 9115AX AP reloads unexpectedly on 17.3.3.26 image.
CSCvy21906	Roaming client delete due to dot1x timer expiry and EAPOL discards message with aa:aa:03:00:00:00.
CSCvy24126	Cisco Catalyst 9105, 9115, or 9120 Series APs display 100% channel utilization.
CSCvy24397	Local mode AP deletes client if there is no response to EAP request within 30 seconds.
CSCvy35021	Cisco Catalyst 9120 and 9105 APs reload unexpectedly during regular operation due to kernel panic.
CSCvy55727	Cisco Aironet 1832 AP ends abnormally due to "translation fault".
CSCvu89997	Wireless clients are unable to connect to Cisco 1830 AP after an input or output error message log.
CSCvv63863	Clients behind WGB faces limited connectivity after a second failover (HA SSO).
CSCvw25812	AP does not send Add Traffic Stream (ADDTS) response when Protected Management Frame is enabled.
CSCvw69941	RLAN ports get blocked when Cisco Aironet 1815T AP joins back the controller.

Caveat ID	Description
CSCvw72516	Cisco DNA Center Assurance's Client 360 page shows the wireless client's SNR value as zero.
CSCvw86121	PMKID roaming fails when configuring a WLAN with WPA3 - Enterprise - GCMP256 and SUITE192-1X - PMKID.
CSCvw89461	Controller reloads unexpectedly with snmp_trap_msg_task system crash as observed in the crash file.
CSCvw94907	The client data rate is displayed incorrectly in the GUI and CLI.
CSCvx29110	Controller with PMF Optional protects the management frames for NON-PMF clients.
CSCvx31952	C9115/9120 displays /sys/class/thermal/thermal_zone0/temp failed [2]: No such file or directory logs.
CSCvx37875	Transmission power discrepancies observed in Cisco Catalyst 9130AX and 9117AX Series APs.
CSCvx44661	Cisco Aironet 4800 APs send wrong number of element count in the MIC control field.
CSCvx51232	Cisco Catalyst 9130 AP displays trace print junk characters while running AP traces.
CSCvx52228	AP fallback does not work when disabled and changed to enabled.
CSCvx53493	Clients are not able to connect to specific Cisco C9130AXI APs due to 4-way handshake time-out.
CSCvx53590	HA configuration sync failure occurs when configuring AP specific antenna monitoring.
CSCvx53862	Cisco Aironet 2802 AP radio0 reloads unexpectedly due to Exception Path.
CSCvx58704	Host does not receive the ARP response in FlexConnect when VLAN tagging and ARP caching are enabled.
CSCvx68417	Lobby Ambassador user accounts have full privilege once "lobbyadmin" term is removed from the URL.
CSCvx73528	APs join the least-loaded controller instead of the primary-base controller.
CSCvx89490	Cisco Catalyst 9130 Series Access Point ends abnormally on 17.3.2.32 build.
CSCvx90730	Cisco Aironet 2802 APs with WIPS reloads unexpectedly after the controller upgrades to 8.10.151.0.

Caveat ID	Description
CSCvx96663	Cisco Aironet 3802 AP takes a long time to skip the PnP after an upgrade from 8.5 to 8.10.
CSCvx97906	Wave 2 APs flood the syslog server with lat_client_add failure errors.
CSCvx99417	C9130AX AP connected client is randomly stuck in IP learning state when BSS coloring is enabled.
CSCvy00817	Only 2.4 GHz clients cannot connect the WLAN to band select enabled and broadcast ssid disabled.
CSCvy11314	The non-WiFi channel utilization does not display anything in 5 GHz even when CleanAir is enabled.
CSCvy15021	Cisco Aironet 3800 Series APs do not provide the ethernet port statistics or status.
CSCvy21584	GUI displays incorrect tagged VLAN data & throws incorrect error message when changing channel width.
CSCvy23582	Cisco Aironet 1810W AP ends abnormally due to kernel panic BUG: soft lockup.
CSCvy24040	Cisco Aironet 2802 AP radio 0 ends abnormally due to command timeout.
CSCvy31207	Cisco Catalyst 9130 AP radio ends abnormally while running WiFi statistics on dev shell.
CSCvy44800	AP forgets its TAG after a second reboot or CAPWAP restart.
CSCvy54374	Controller sends Association Response with status 53 for Apple iPhoneXS iPhoneX.
CSCvv01775	Wired Clients behind non-Cisco WGBs do not get the IP addresses on the controller.
CSCvx14179	Static IP on Non-Cisco WGB does not work - Stuck in IP Learn.
CSCvx83965	WNCD ends abnormally at rrm_client_coverage_hole_algorithm.
CSCvv41817	Policy Profile ACL is not consistently applied on FlexConnect Local auth and local switched client.
CSCvx62420	The external webauth redirect URL does not encode the WLAN special character properly when appended.
CSCvx97611	AP resets the CAPWAP while configuring the same name if the filter is tag source.
CSCvx40586	The controller does not sort the RFID RSSI received from APs before sending 16 APs to the connector.

Resolved Caveats for Cisco IOS XE Amsterdam 17.3.3

Caveat ID	Description
CSCvv56712	AAA or RADIUS must fragment packets to the required size based on the MTU settings.
CSCvf16302	The flash on lightweight Cisco Wave 1 APs get corrupted.
CSCvh08020	Some APs get stuck on AP after an upgrade.
CSCvi84734	Clients may not be able to connect to AP when AAA override SSID performs dynamic VLAN assignment.
CSCvv00630	AP crashes after several hours of processing CAPWAP fragmented data packets.
CSCvv13142	Cisco Catalyst 9117 Access Point radio reloads unexpectedly after disabling MU-MIMO.
CSCvv33955	NBAR crashes when CAPWAP programs the client flows as part of AVCRoam.
CSCvv34695	Wave 2 APs reload unexpectedly when upgrading the controller to a version higher than 8.5.x.
CSCvv64647	Cisco Wave 2 APs cannot negotiate power with Cisco SG350 switches.
CSCvv68021	Prime Infrastructure 3.9: Lightweight AP template fails with object not found in device error.
CSCvv77899	WNCD crash observed after provisioning Cisco Catalyst 9800 Series Wireless Controller in Cisco DNAC.
CSCvv78264	Cisco Aironet 1542 Access Point does not converge to Cisco Aironet 1572 Access Point.
CSCvv78719	Cisco Aironet 2800, 3800, 4800, 1560, or 6300 Series APs fail to transmit data frame to the client.
CSCvv82719	The **show aaa servers detailed** command displays zero value for most of the authentication details.
CSCvv84296	Stale client entry leads to client disconnects and association problems.
CSCvv86518	Cisco Catalyst 9800-L Wireless Controller: Observed WNCD crash due to assertion failure.
CSCvv92583	APs do not forward or drop ARP response when performing Split Tunneling.
CSCvv93995	Clients cannot connect to Cisco Catalyst 9115 Access Points due to transmission error on radio.

Caveat ID	Description
CSCvv95806	Remove unsupported EVPN commands from Cisco Catalyst 9800 Series Wireless Controller command line.
CSCvv99213	In Cisco Catalyst 9130AXE Access Point, the RF tag power settings does not work on Slot 2.
CSCvw01612	Cisco 9130AX Access Point does not send M1 over the air.
CSCvw02775	In Cisco DNA Center 2.1.2.0, the ICAP does not display correct data in auto packet analyzer.
CSCvw02981	Cisco Aironet 2802 Series Access Point suddenly drops in transmission power level.
CSCvw04654	Controller reloads unexpectedly on creating PMK cache.
CSCvw06053	The CA certificate gets deleted after reboot in Cisco Catalyst 9800-CL Cloud Wireless Controller.
CSCvw10308	Clients stop passing traffic when connected to the Cisco Catalyst 9130 Series Access Point.
CSCvw11488	When CTS enforcement is enabled on policy, the FIA is applied implicitly on all interfaces.
CSCvw16305	The WNCD core is displayed when a client gets the blacklisting flag from the WLAN policy.
CSCvw16864	AP uptime is not sent to third-party SNMP monitoring server when AP initially joins the controller.
CSCvw19820	The controller is unable to push SSIDs while doing a configuration change on the policy profile.
CSCvw28182	Controller reloads unexpectedly on Reaper Reset with Task "spamApTask3".
CSCvw30043	Cisco Aironet 3800 Series Access Points may stall traffic at session-timeout with WPA2 or enterprise.
CSCvw33054	Controller reloads unexpectedly due to NetFlow packets.
CSCvw34012	Standby controller sends ARP requests using the management interface IP address.
CSCvw35698	IOS APs fail to join the Cisco Catalyst 9800 Wireless Controller due to Connect, no AP name.
CSCvw36348	SAFEC error appears on the controller syslogs causing APs to disassociate from the controller.
CSCvw37503	Cisco Catalyst 9115 or 9120 APs do not process protected NDP from other AP models.

Caveat ID	Description
CSCvw38396	There is no option to disable the session timeout in RLAN policy profile.
CSCvw45695	Access request sent with different source port for the same ID.
CSCvw49225	Chrome OS using Intel AX201 unable to connect to 11AX APs in local mode.
CSCvw49555	The Cisco Catalyst 9800-CL Wireless Controller gets stuck at the boot process.
CSCvw50194	Cisco Catalyst 9120 Access Points stop using LSC and use only MIC.
CSCvw50596	The controller crashes due to critical process RRM fault on rp_0_0 (rc=139).
CSCvw51161	The controller triggers SIGSEV reload after neighbours added to the list exceeds 24.
CSCvw52979	Cisco Catalyst 9120 APs crash after an upgrade from Cisco IOS XE 17.3.1 to 17.3.2a.
CSCvw53114	Controller does not reflect IPv4 address for random clients.
CSCvw54497	Rogue detection causes high CPU in Cisco Catalyst 9130AX APs without any clients connected to it.
CSCvw55275	The controller reloads due to WNCD process crash when AP sends frequent CDP updates.
CSCvw55708	The NACM rules or DNAC connectivity is lost post switchover with RMI feature.
CSCvw55931	The Cisco Catalyst 9120AX AP crashes due to NULL pointer dereference.
CSCvw57243	Unable to change the Cisco Industrial Wireless 3702 AP Flex+Bridge mode using the controller GUI.
CSCvw63909	Cisco Catalyst 9120 APs registered to C9800 Wireless Controller experiences kernel panic.
CSCvw65582	CPP crash and CAPWAP reassembly error is observed in 17.3.2a release.
CSCvw67752	Cisco Wave 2 AP frames randomly get stuck in buffer when U-APSD is enabled on 17.3.2.
CSCvw76385	**aaa accounting** command breaks AAA part of the GUI.
CSCvw79225	The controller reloads due to qcp-ucode crash when the NBAR engine receives invalid packet length.

Caveat ID	Description
CSCvw81362	The IRCM tunnel between 9800 Wireless controller and AireOS fails to recover for 30+ minutes.
CSCvw84519	System crash occurs due to Critical process wncd fault on rp_0_1 (rc=139) in 16.12.4a.
CSCvw86133	DSCP marking is set to zero on mobility tunnel between 9800 and AireOS when web auth is enabled.
CSCvw89083	Cisco Catalyst 9120AX APs disconnect from controller after receiving CAPWAP payload.
CSCvw91795	Cisco Catalyst 9115 and 9120 Series APs use the wrong TID when responding to block ack requests.
CSCvw99507	The controller reloads unexpectedly with task name "Dot1x_NW_MsgTask_4".
CSCvw99524	The RFID entries are stuck on the Cisco Catalyst 9800-40 Wireless Controller.
CSCvx10905	Cisco C9130AX AP tri-radio enabled by manual dual-radio assignment mode disables HE on slot1.
CSCvx13355	DCA fails when the Outdoor AP is on channel 100.
CSCvx21714	The controller unexpectedly reboots due to qfp-ucode crash.
CSCvq22269	IOS APs are always stuck in downloading state until rebooted.
CSCvt65999	Controller sends CAPWAP fragmented packets in out-of-order sequence when heavy UDP traffic is sent.
CSCvu47855	Sourced packets are dropped when **ip verify unicast source reachable-via rx** command is configured.
CSCvu78124	Client join SNMP notifications display incorrect and missing values.
CSCvv03641	After AP SSO, few APs teardown DTLS and connect back to the controller.
CSCvv43986	IPv6 connectivity breaks when HA SSO is triggered with AAA override enabled for VLAN.
CSCvv50667	Cisco Wave 2 APs set global config for AP syslog level after reload instead of keeping per-AP config.
CSCvv56712	AAA or RADIUS Should have a way to adjust MTU based on interface settings.
CSCvv57343	Cisco Aironet 2802 AP reloads unexpectedly on CAPWAPd with WLAN AP service function.

Caveat ID	Description
CSCvv63863	Clients behind a WGB faces limited connectivity after a second failover (HA SSO).
CSCvv73570	The Cisco 9800 Anchor doesn't send called-station-id in the external web-auth access request.
CSCvv76781	QoS Priority is marked incorrectly with WMM UP 5 when DSCP value is 46.
CSCvv78366	Cisco Wave 2 APs flood syslog server with lat_client_add failure errors.
CSCvv79700	Fault Tolerance is broken in Flex APs due to vendor_set_ccx_elements.
CSCvv81234	MAP authentication failure after reboot is observed in Cisco Catalyst Industrial Wireless 6300 AP.
CSCvv82815	BA Session establishment errors and iPAD performance issues.
CSCvv89898	Clients fail to connect when WLAN Policy name includes certain special characters.
CSCvv94771	Trustpoint does not appear correctly in the Configuration > Interface > Wireless GUI page.
CSCvv97721	Controller reloads unexpectedly when "debug disable-all" command is issued.
CSCvv99765	The Cisco Catalyst 9120 series AP stops forwarding client traffic after random roam events.
CSCvw04389	Application visibility displays "No data available" in the controller GUI.
CSCvw08801	Unable to change the AP Country in the GUI.
CSCvw09472	Object "cLApWlanStatsEntry" SNMPWALK displays the value "0" when traffic is transmitted.
CSCvw11880	FMAN-FP crash is observed when deleting WLAN configured with "peer-blocking allow-private-group".
CSCvw13174	All Cisco Catalyst 9800 series platforms truncate the AP location string during join.
CSCvw14131	A crash is observed in TCL bytecode when running RA Trace in guest shell Python.
CSCvw20364	Webauth is broken when booted using secure-webauth-disable.
CSCvw21621	The controller ignores the DHPC offer for client.

Caveat ID	Description
CSCvw24920	ciscoLwappDot11ClientMovedToRunState throws wrong OIDs on the controller.
CSCvw30152	NETCONF sessions fail or timeout after 255 connections to the device.
CSCvw31938	Log files contain many WNCD_DB Stuck : tbl_bssid_dms messages.
CSCvw32098	Cisco switches connected to Wave 2 APs generate CDP-4-DUPLEX_MISMATCH.
CSCvw39267	Cisco Aironet 2800 Series AP running release 8.10.130 reloads unexpectedly due to FIQ or NMI reset.
CSCvw44218	There is no client-to-client communication after roaming when AVC is enabled.
CSCvw44807	URL Rules can be configured from more than 20 and “remove” issue exists from the 21st URL Rule.
CSCvw48811	Supervisor running IOS-XE crashes with error messages observed prior to the unforced system reload.
CSCvw51418	Probe suppression on macro cell does not work in Cisco Catalyst 9120 Series AP.
CSCvw53548	Controller displays Authentication failed (Timeout) logs every 90 seconds for clients not connected.
CSCvw54447	The ICAP chart displays increasing Rx average data rate when the most recent data rate is flat.
CSCvw54705	Users are required to configure both SNMP RO and RW from GUI.
CSCvw59261	Few clients do not connect to 2.4 GHz due to incorrect channel advertising on Cisco C9100 APs.
CSCvw61823	Crash observed on active chassis during longevity run.
CSCvw65861	MAC Filtering: Description not imported properly from CSV file.
CSCvw66096	Cisco Flex group configurations get appended with junk chars in "show tech-support" with multi-words.
CSCvw66140	Cisco Aironet 1852 Access Points switch to DHCP even if static-ip failover is disabled.
CSCvw66408	The controller displays transceiver is not supported by this card for a supported SFP.
CSCvw66446	Logs are flooded with IPContext when running **debug client <*mac address*>**.

Caveat ID	Description
CSCvw66560	Cisco Catalyst 9120AX APs stop forwarding some Moxa WGB client packet through CAPWAP.
CSCvw68994	The **debug wireless** command failed to execute decode when **exec prompt timestamp** is configured.
CSCvw74044	LAG APs reflect Wired0 traffic out of Wired1 when using LAG + flexconnect + local switching.
CSCvw76772	The control plane name fails with bad length or size error when provisioning VN anchor.
CSCvw76774	GUI unable to update and save WebAuth config after changing initial "Login Page" html file mapping.
CSCvw77005	Cisco Wave 1 devices cannot browse internet when connected to OEAP personal SSID.
CSCvw77453	RF Profile parameters are not pushed for optimized roaming.
CSCvw85996	The **show ap fra** command displays COF percentage as none when static mode is set.
CSCvw90631	The controller sends packets sourced from the client after the client is no longer available.
CSCvw90931	Tracebacks are observed in the controller after an upgrade.
CSCvw91859	Cisco 9120AX, 9115AX, 9105AX APs drop upstream traffic (various types) with data DTLS enabled.
CSCvw91983	Cisco Aironet 1562 mesh AP are not able to join the controller with FIPS enabled.
CSCvw92754	Mobilityd crash is observed in the controller due to Client whitelisting feature intersection.
CSCvw92906	ARP queries flood due to low value of BSS Max Idle Period.
CSCvx10256	Controller returns incorrect "Allowed Country Code" for APs via SNMP.

Resolved Caveats for Cisco IOS XE Amsterdam 17.3.2a

Caveat ID	Description
CSCvm17365	Cisco Wave 2 APs reloads unexpectedly due to FIQ/NMI reset.
CSCvr03516	Need **show mac address-table tree** command.
CSCvs48567	Unable to delete a client using SNMP OID bsnMobileStationDeleteAction.

Caveat ID	Description
CSCvs65189	AP Ethernet PHY interop issue when using IEEE Fast Retrain when connected at mGig speeds.
CSCvs48711	Controller shows LAN port status as UP, though the AP status is Down and the protocol is UP.
CSCvt06712	Max Transmit Power Level is set to 128 dBm in Country IE.
CSCvt61795	Cisco Aironet 3800 APs advertise Robust Security Network (RSN) Preshared Key (PSK) in the beacon on WLAN with open MAC filtering authentication.
CSCvt79194	Clients associated to Wave2 AP (having local switching WLAN with native VLAN) cannot resolve ARP.
CSCvu03389	Controller is remarking client DSCP packets to zero when voice Call Admission Control (CAC) is configured.
CSCvu03863	RF profile max clients configuration is not working.
CSCvu04160	Unexpected reload in device classifier code due to segmentation fault.
CSCvu17521	AP interface speed is shown as *None* in Cisco Prime.
CSCvu22410	If controller is disabled and reloaded, dot11n and dot11ac are forced to enable.
CSCvu34813	EG and BH code: 5-GHz Channel mismatch between controller and AP.
CSCvu43631	AP PnP does not try to synchronize time with public NTP server.
CSCvu50834	Cisco Aironet 3802 AP: No rx packets are seen for 5-GHz radio.
CSCvu58082	Cisco Aironet 3800 AP with data Data Datagram Transport Layer Security (DTLS) encryption disconnects from the controller due to CAPWAP keepalive after rx path MTU (PMTU) discover.
CSCvu64805	Stale entries are shown in the **show wireless device-tracking database ip** command output.
CSCvu71187	AID leak is observed with RLANs.
CSCvu71263	EoGRE Flexconnect Local Switching Deployment: Client gets IP from native VLAN after AP reboot.
CSCvu75470	IP address of configured nameserver seen flipped on controller after AP tears-down the connection.
CSCvu78608	Webauth redirect URL is getting looped for the client.
CSCvu78679	Cisco Aironet 2800 AP drops from controller due to malformed inactive_client_payload.

Caveat ID	Description
CSCvu81034	AP marks the Wi-Fi Multimedia (WMM) UP value as 0 despite receiving DSCP value as 46 (EF).
CSCvu83242	Cisco Aironet 1852 AP radio crash is obsereved; creates radio FW assert coredump file with reason beacon stuck.
CSCvu89290	Cisco Aironet 1815 and 1850 APs:- Local SSID client is not getting IP from local DHCP scope.
CSCvu89996	AP disjoins after client connects to SSID using LDAP with secure mode.
CSCvu90021	Wave 2 APs are sending static discoveries using stale entries in mobility list.
CSCvu90089	Controller crash is observed when using WebAuth SSID with Lightweight Directory Access Protocol (LDAP) authentication.
CSCvu92898	Cisco Catalyst 9800-L Wireless Controller: WNCD crash is observed due to process rrm_client_chd Assertion failed.
CSCvu94264	Controller sends junk LDAP bind password after a reload.
CSCvu95504	Controller reloads unexpectedly while doing MAC comparison.
CSCvv00513	AP transmits action frames from a different basic service set identifiers (BSSID).
CSCvv02099	AP should reject incorrect fast transition authentication requests.
CSCvv02121	AP is not sending re-association response.
CSCvv02670	Controller is showing incorrect AP Cisco Discovery Protocol (CDP) information.
CSCvv07059	Remove country code from the AP join profile.
CSCvv09526	Cisco Catalyst 9800-CL Wireless Controller: Memory corruption causes reload.
CSCvv12425	Web UI shows wrong timezone when daylight savings is enabled.
CSCvv13978	Cisco AP reloads unexpectedly on NMI watchdog.
CSCvv15396	Unable to schedule 3 guest user accounts with same start times but different end times.
CSCvv15476	Tracebacks are observed on the active controller when standby controller is down.
CSCvv16755	Cisco Aironet 2800 AP: Displays \"Rx Hang is detected DescLeak\" message followed by Kernel Panic crash.
CSCvv17400	Prevent web UI from locking out when generating RA traces.
CSCvv18778	Client association fails when changing the connected WLAN from 802.1X WLAN to PSK+MAC filtering WLAN.

Caveat ID	Description
CSCvv20346	Luajit process is active when Telnet/SSH session running monitor logging exits prematurely.
CSCvv22101	CMAND crash on Cisaco Catalyst 9300 Fabric in a Box (FiaB).
CSCvv22110	Cisco Catalyst 9130AX Series AP: Multicast traffic failures are observed after Group Transient Key (GTK) key index rotation for Vocera clients.
CSCvv22359	Cisco Aironet 2802 AP: XOR Radio (2.4GHz) shows 40 MHz channel width on monitoring tools.
CSCvv22536	Client moves to RUN state without Extensible Authentication Protocol (EAP).
CSCvv25877	Managed APs are reported as Rogue with state as LRAD and classification as Pending.
CSCvv26406	Some clients are assigned to an excluded VLAN, between 2 VLAN ranges in a VLAN group.
CSCvv28974	FlexConnect: Client goes in to continuous association loop and is unable to recover.
CSCvv29239	Controller crashed @ mdns_io_event_callback_v6.
CSCvv32743	AP policy authentication method list is reset after refreshing AAA tab and adjusting Auth Method list.
CSCvv33422	Controller is not sending DHCP payload to AP when user disables dhcp central + Flex nat/pat + dhcp required.
CSCvv35000	Cisco Embedded Wireless Controller: Wi-Fi Protected Access 3 (WPA3) Simultaneous Authentication of Equals (SAE) is not working.
CSCvv36288	Client is deleted due to CO_CLIENT_DELETE_REASON_CLIENT_EAP_ID_TIMEOUT after 11i roam.
CSCvv36645	Object cLApEntPhysicalIndex always equals to 1 for all AP registered to controller.
CSCvv36728	Cisco Aironet 1800, 2800, 3800, and 4800 APs are blocking TCP on port 64999 on FlexConnect Local Switching.
CSCvv37072	Flex Opportunistic Key Caching (OKC) roam M1 is not sent out.
CSCvv39596	Client is stuck in IP learn state and observing continuous cpp tracebacks.
CSCvv39666	Controller crashes with the reason "Critical process wncd fault on rp_0_0 (rc=134)".
CSCvv39762	Cisco Catalyst 9105, 9115, and 9120 APs starts beaconing during the Call Admission Control (CAC) time on Dynamic Frequency Selection (DFS) channel if 802.11h is disabled on the controller

Caveat ID	Description
CSCvv39859	apmgr_get_site_tag_name_from_wtp_mac fails when buffer is larger than TAG_NAME_LEN_MAX.
CSCvv40205	User gets session extension prompt immediately after login and eventually logs out.
CSCvv41414	Client is deleted with Invalid PMID (31) when it switches from 11i to 11r.
CSCvv44338	Mobilityd crash is observed @mm_dgram_init.
CSCvv45072	Controller reloads unexpectedly when configuration for BSSID QoS or auto-QoS is enabled.
CSCvv45722	Office Extend Access Points (OEAP): LAN port 3 (Local Port) client cannot reach the Internet.
CSCvv50036	The **show running-config** command output does not display the \"mandatory\" data rates set globally on the controller.
CSCvv50755	Cisco Aironet 2800 AP radio crashes due to exception.
CSCvv51321	Cisco Catalyst 9105, 9115, and 9120 APs unexpectedly experience "assert" kernel panics, when Target Wait Time is enabled.
CSCvv53676	Cisco Catalyst 9120 AP: MFP frame from decrypt failed messages are printed on the AP console when the 11w enabled client is connected to the FlexConnect group.
CSCvv54062	Cisco Catalyst 9800-80 Wireless Controller unexpectedly crashes in the CPP-MCPLO-UCODE process.
CSCvv54468	OID statistics for active controller power supply shows UNKNOWN even though its powered on.
CSCvv54538	Cisco Catalyst 9120 AP is crashing with the following message: + assert:\"dma_txactive(di) == 0\" failed: file \"wlc_tx.c:13678\".
CSCvv55733	Pixel client de-authenticates as NO ARP responses are received during NUD checks to Virtual Router Redundancy Protocol (VRRP) gateway.
CSCvv58057	Scale performance of Cisco Catalyst 9130 AP is worse than Cisco Catalyst 9120 AP, with less than sixty active clients.
CSCvv58252	Controller ignores disconnect request from RADIUS server.
CSCvv59497	Cisco Catalyst 9130 AP: No SIA antenna id from external antenna.
CSCvv62762	Cisco Catalyst 9120 AP crashes due to station data base entry becoming NULL.
CSCvv67696	Multicast streaming stops on client when wrong SGV value is pushed.

Caveat ID	Description
CSCvv68294	Cisco Catalyst IW6300 Heavy Duty Series AP: Mesh Access Point (MAP) is not retaining the Flexport Antenna Config \"Single or Dual Band\" across reboots.
CSCvv70908	After FT event, the following error is displayed: "vnid mapping record doesnt exist".
CSCvv71587	Office Extend Access Points (OEAP): AP is not able to join controller as the Keyman process is down.
CSCvv72665	Cisco Aironet 1562E-M-K9 Series Outdoor AP has 5ghz radio down with country AE (Emirates) when it joins the controller.
CSCvv73396	Cisco Catalyst 9115AX AP unexpectedly reloads.
CSCvv76241	Controller is rebooting instead of shutdown with Guest shutdown os feature in VM.
CSCvv76805	Controller crash: wncmgrd crashing @ apwap_ac_process_cleartxt_msg function.
CSCvv78442	When CAPWAP multicast is enabled, clients are not able to get IPv6 address if only Cisco Aironet 4800 AP is deployed.
CSCvv78921	Controller displays error messages and tracebacks similar to: \"%ID_MANAGER-3-INVALID_ID: Chassis 1 R0/0: wncd: bad id in id_to_ptr\" Tracebacks.
CSCvv82544	Cisco Catalyst 9120 AP is crashing unexpectedly: assert:\"0\" failed: file \"wlc_amsdu.c:4709\".
CSCvv83038	Controller web UI does not show Rogue Client detail in Japanese.
CSCvv89089	VPN configuration through web UI fails with an \"Internal Error\" when Pre-shared key contains \"%\".
CSCvv90831	Wired DHCP clients are unable to get IP address after OEAP reload.
CSCvv94747	DHCP packets are dropped by SISF when option82 is configured.
CSCvv96971	Mobility AP list is not updated on the controller when using IRCM code on AireOS controller.
CSCvv98567	Controller should not report LRAD rogue APs over NMSP to CMX.
CSCvv98793	Managed APs are reported as Rogue with state as LRAD and classification as Pending.
CSCvw00646	Controller crashed at tlv_flex_client_cache_extended_param_payload_ext_tlv_payload_set_client_mac.
CSCvw03003	Standby controller is sending ARP request with its eth.mac using wireless mgmt ip seen as IP-4-DUPADDR.
CSCvw09580	Controller will not take Cisco DNA-C certificate chains depth with 4 and above.

Caveat ID	Description
CSCvw09684	Chunk memory leak due to \"FMANRP msg chun\" @ fmanrp_tdl_alloc, module = \"l2m_config\".
CSCvw18047	Cisco Aironet 3800 AP: FlexConnect local-sw randomly stops forwarding frames after dot1x session-timeout.
CSCvw19761	Tracebacks are observed after upgrading to IOS XE 17.3.1.
CSCvw23306	AP performs DHCP reset after 5 failed attempts of CAPWAP discovery, but still responds to subsequent pings.

Resolved Caveats for Cisco IOS XE Amsterdam 17.3.1

Caveat ID	Description
CSCvq99108	Cisco Aironet 3700 AP series reloads unexpectedly.
CSCvr68729	High Availability fails to initialize NVRAM after multiple power cycles.
CSCvs63467	IPv6 dual stack is not working.
CSCvs31212	Cisco Aironet 3800 AP: Manufacturing Installed Certificate (MIC) errors observed for Cisco Centralized Key Management (CCKM) roams in FlexConnect local switch mode.
CSCvs52625	btman process at 100% while running **show tech** command.
CSCvs55102	WNCd unexpectedly reboots after association failure.
CSCvs55109	AP Ethernet link flaps at 5G speed due to Fast Retrain failure.
CSCvs56562	Cisco Catalyst 9800-40 Controller is crashing after receiving a bogus username.
CSCvs56849	Cisco Catalyst 9120AXI AP unexpectedly reloads with watchdog or grpc_server tainted.
CSCvs62464	Controller with more than 4000 APs in one site-tag (not default-site) is not allowing to do AP configuration changes.
CSCvs66107	Cisco Catalyst 9115AX AP: Rogue containment is not working when AP is in monitor mode.
CSCvs70091	-Q domain APs in Japan are advertising J4 as the country in beacon, instead of JP.
CSCvs71784	Controller crashes on receiving username with 246 characters on the third attempt.
CSCvs83955	Control packets are not honoring mobility Path MTU Discovery.

Caveat ID	Description
CSCvs93903	WNCd process goes down due to assert for basic SSID (BSSID) magic check.
CSCvs98528	WNCd crash is observed with roaming of long duration fabric clients.
CSCvt05007	Controller crashes when a 11r client tries to perform over-the-air or over-the-ds roam.
CSCvt08645	Multicast replicates over CAPWAP when global multicast is disabled.
CSCvt17820	Client gets excluded after VLAN changes following the machine and user authentication.
CSCvt29348	The **show tech wireless** command output is showing incomplete information for the sub-commands: **show ap auto-rf dot11 5ghz** and **show ap auto-rf dot11 2**.
CSCvt31484	Controller unexpectedly reloads when an AP joins and does not report the correct radios.
CSCvt34987	The Cisco Catalyst 9800-80 HA cluster crashes frequently.
CSCvt35766	Controller is not allowing Wi-Fi Protected Access (WPA)/Temporal Key Integrity Protocol (TKIP) only configuration.
CSCvt35811	Cisco Catalyst 9130 AP: Channel/Mode mismatch between WCP and WLAN driver.
CSCvt37835	Client is unable to associate due to DOT11_STATUS_DENIED_RATES when extended rates are used.
CSCvt38486	Cisco Wave 2 APs: EAP-PEAP (Protected Extensible Authentication Protocol) flex-auth fails occasionally because of low EAP timeout.
CSCvt41053	Clients are assigned to native VLAN instead of client VLAN.
CSCvt41519	Controller crashes due to AP with the same name and different existing radio mac.
CSCvt46733	Address Resolution Protocol (ARP) handling allows for the ARP entry to be removed for a wireless DHCP client.
CSCvt68112	Cisco Catalyst 9130 AP: Cisco OfficeExtend access point (OEAP) GUI is not accessible.
CSCvt75205	Controller crashes on Wi-Fi Multimedia (WMM) action, while roaming.
CSCvu19000	Cisco Catalyst 9800-L Controller goes administratively down after a reload following factory reset using CLI.

Caveat ID	Description
CSCvu44330	Memory leak is observed under process SACRcvWQWrk2 when Smart Licensing is enabled.
CSCvu57730	Controller crash is observed in CPP (data path).
CSCvu71871	Cisco Catalyst 9800-80 Controller crashes with SIGSEGV while removing timer RB tree color.
CSCvu78070	Controller crash is observed during WNCd process.
CSCvp76426	Controller is not honoring timezone when configuring dynamic channel allocation (DCA) anchortime.
CSCvs29013	Controller is not sending SNMP trap when AP is reset using GUI or CLI.
CSCvs40004	Cisco Catalyst 9800-L-C fails to install authorization code due to NO_AUTH_CODE_FOUND.
CSCvs50689	Improve the **show wireless stats loadbalance summary** command.
CSCvs52655	The **show wlan client stats** command output shows wrong WLAN with similar WLAN name on special conditions.
CSCvs73952	Client count shows zero for the **show ap dot11 5ghz/2.4ghz load-info** command output when Coverage Hole Detection (CHD) is disabled.
CSCvs75087	Global AP pre-image download is not working.
CSCvs77734	Frequent channel changes observed on the Cisco Aironet 4800 AP slot 0 radio while using 5 GHz.
CSCvs81826	Upgrading to Cisco IOS XE 16.12.2s deletes WLAN to policy profile mapping under default-policy-tag.
CSCvs93963	Support tspec processing when voice acm is disabled or with no tgr tspec.
CSCvt01659	Cisco Wave 1 APs: Client traffic is stuck after client is in RUN state for Central Web Authentication (CWA) or Local Web Authentication (LWA).
CSCvt13127	Cisco Catalyst 9800-CL Controller is unable to display medium power when AP sends a 25W message.
CSCvt19605	Guest anchor fails to load balance clients across anchors.
CSCvt23051	Cisco Catalyst 9120AX AP is not use the correct datarates.
CSCvt27421	Cannot remove AdvIPServices license.

Caveat ID	Description
CSCvt29373	UDP Port 5246 based Access Control List (ACL) filter fails to select Datagram Transport Layer Security (DTLS) encrypted CAPWAP control packets.
CSCvt29596	Current Tx rate for 802.11AX clients is displayed incorrectly.
CSCvt30657	Controller crashes with the following reason: \Critical process cpp_cp_svr fault on fp_0_0 (rc=134)\.
CSCvt37462	The factory-reset all command deletes the actual image when controller is in install mode.
CSCvt47787	Roaming is not successful when NAC is enabled in the policy profile.
CSCvt56911	Ethernet over GRE (EoGRE) tunnel is not copying Differentiated Services Code Point (DSCP) from inner payload IP header on injected packet.
CSCvt61509	Cisco Aironet 3700 AP is unable to join controller as the VLAN interface name exceeds character limit in flex profile.
CSCvt63940	Authentication fails for some clients, when local authentication is configured in the policy profile.
CSCvu18085	Cisco Catalyst 9117AX AP: 802.1x authentication is not working for clients.
CSCvu24770	Various models of Android 10 devices fail to associate.
CSCvu58564	AP uses non-allowed channel on dual radio when change setting to 5 GHz.
CSCvu61194	Cisco Aironet 2800 and 3800 APs are sending burst of Request to Send (RTS) and Block Ack Request (BAR) randomly leading to low client data rates.

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 Series 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 results you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco DevNet.
- 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.