Release Notes for Cisco Catalyst 9800 Series Wireless Controller, Cisco IOS XE 26.1.x

Contents

Cisco Catalyst 9800 Series Wireless Controller, Cisco IOS XE 26.1.x

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 are available in multiple forms to cater to your deployment options:

- Catalyst 9800 Series Wireless Controller Appliance
    - Cisco Catalyst 9800 Series Wireless Controllers (C9800-L, C9800-40, C9800-80)
    - Cisco CW9800 Series Wireless Controllers (CW9800L, CW9800M, CW9800H1, CW9800H2)
- Catalyst 9800 Series Wireless Controller for Cloud
- Embedded Wireless Controller (EWC) on Catalyst 9000 Series Switches

This document describes the new software features that were introduced or enhanced, change in behavior, issues, supported hardware, and so on, for Cisco IOS XE 26.1.x.

New software features

This section provides a brief description of the new software features introduced in this release.

Table 1. New software features for Cisco Catalyst 9800 Series Wireless Controllers, Release 26.1.1

Product impact	Feature	Description
Software Reliability	Standby monitoring with RMI	With this feature, in the controller High Availability setup, only the RMI interface remains up on the standby controller, while all other interfaces are administratively down. When Layer 3 (L3) is enabled on the controller in the policy profile, packets destined for the standby controller from non-RMI subnets reach the standby through the active controller through the RMI interface, as the active controller advertises the RMI subnet. When the standby receives a RMI source packet, it gives higher precedence to the RMI-sourced packet than the RIB (Routing Information Base)-sourced packet and updates its Forwarding Information Base (FIB) table based on the RMI sourced packets. This way, the standby controller routes all outgoing packets through the active controller over the RMI interface. Gateway monitoring is disabled when L3 is enabled. No CLI commands are newly introduced.
	MACsec support on Access Points	With this release, MACsec support is introduced on APs to provide Layer 2 hop-by-hop encryption and integrity protection for data transmitted between the AP and the connected switch. This feature leverages the IEEE 802.1AE standard and ensures robust security against eavesdropping and man-in-the-middle attacks without impacting AP performance. The following commands are introduced: • **key chain** *chain-name* **macsec** • **ap profile** *name* **macsec** • **show ap macsec summary** • **show macsec** • **debug macsec** For more information, refer to MACsec support on APs.

Product impact	Feature	Description
	Implement Wi-Fi coexistence with IOx apps	From this release, Wi-Fi coexistence based on IOx app is implemented to minimize signal interference between Wi-Fi and IoT radios on the 2.4 GHz ISM band. By utilizing Packet Traffic Arbitration (PTA) to coordinate airtime sharing, this collaborative mechanism ensures improved performance and reliability in environments with high IoT device density.
Ease of use	GNSS enhancements	From this release, two GNSS enhancements are available: • An option to enable or disable GNSS from the controller, and • improved output for the **show gnss info** command, offering more detailed runtime status and diagnostics. This command already has equivalent improved output for other Cisco Wireless APs that support GNSS. For more information, refer to: 9167I: GNSS 9167E: AP Mode Configuration 9165E: Control and Provisioning of Wireless Access Points 9165D: Control and Provisioning of Wireless Access Points
	Dynamically configure URWB parameters	This feature allows you to adjust certain Ultra-Reliable Wireless Backhaul (URWB) configuration parameters on supported access points (APs) without rebooting the device. For more information, refer to URWB.
	Remove ports limitation on PAT	From this release, you can use port numbers from 1 to 1024 for both TCP and UDP. However, use these ports with caution because they are reserved ports. The valid port range is 1 to 65535. For more information, refer to Workgroup Bridge-Advanced features and optimizations.
	Automatic certificate enrolment and renewal using SCEP	This feature enables automatic certificate enrollment and renewal for IW916x Workgroup Bridges (WGBs) using the Simple Certificate Enrolment Protocol (SCEP). WGBs can securely obtain and update digital certificates from a Certificate Authority (CA) server, streamline device authentication and management for large-scale EAP-TLS deployments. For more information, refer to Workgroup Bridge.
	Sensor Connect improvements	This release brings improved user experience for setting up and using the Sensor Connect App (IoT Orchestrator), helping customers and partners enable enhanced BLE outcomes. Customers will see a more streamlined installation and configuration of the Sensor Connect App, with more intuitive networking parameterization through automated IP address and NAT configuration rules during the setup workflow.
Upgrade process	Support for kernel minidump and TrustZone upgrade	From Cisco IOS XE 26.1.1 onwards, kernel minidump and TrustZone upgrade is supported on Cisco Catalyst 9162 Series Access Points, Cisco Catalyst 9164 Series Access Points, and Cisco Catalyst 9166 Series Access Points.
Ease of setup	Legacy data rate selection at the SSID Level	From this release, the Legacy Data Rate Selection at the SSID Level feature enables the configuration of 802.11a/b/g data rates per WLAN. This feature allows you to specify minimum bit rates for specific SSIDs, ensuring APs do not advertise rates lower than the configured minimum. It provides the granular control needed to meet specific performance thresholds for various user groups and applications. For more information, refer to Data Rate Selection at SSID Level.
	Accelerometer sensor support for Access	In this release, you can enable the accelerometer sensor by default when the AP joins the controller after upgrade. The accelerometer provides information to determine the antenna

Product impact	Feature	Description
	Points	down tilt. The following are the APs with accelerometer sensor support: • Cisco Catalyst Wireless 9166D1 APs • Cisco Wireless 9176I / 9176D1 APs • Cisco Wireless 9178I APs • Cisco Wireless 9179F APs • Cisco Wireless 9174E* APs (*when used with CW-ANT-T-D2-D8 antenna) The following show command was introduced: • **show ap name** <*ap-name*> accelerometer For more information, refer to AP Configuration.
	Recovery CLI commands for URWB APs	The URWB Recovery CLI has been upgraded to enable initial provisioning and automated recovery for Access Points (APs). With this update, APs can restore connectivity with the controller through the recovery commands. For more information, refer to URWB.
	Static AP name configuration	Static AP naming allows administrators to pre-configure a specific name for an AP before it joins the controller. This ensures the AP adopts the designated name upon its initial connection, maintains strict naming consistency across the network, and prevents accidental duplicate naming or unauthorized modifications, even when the AP is offline. The following command was introduced: • **name** static-ap-name For more information, refer to New Configuration Model.
	Native IPv6 support for Cisco TrustSec-ISE communication	In this release, native IPv6 support for Cisco TrustSec-ISE communication is introduced, empowering organizations to modernize their network security infrastructure. This update facilitates seamless identity-based access control and policy enforcement across IPv6-enabled networks, effectively addressing the limitations of IPv4 such as address exhaustion and routing inefficiencies. With simplified configuration options available through CLI and GUI, you can now ensure robust, scalable, and future-ready security management for your enterprise environment. For more information, refer to Cisco TrustSec.
Hardware reliability	SFP support with Forward Error Correction (FEC) mode cl74 between CW9800M, CW9800H1, and Nexus switches	In this release, interfaces using SFP-25G-CSR-S, SFP-25G-LR-S, and SFP-25G-SR-S transceivers will successfully establish links with Nexus switches configured for Forward Error Correction (FEC) mode cl74. Previously, these interfaces failed to come up under this configuration. This update resolves the connectivity issue, enabling stable links between the controllers and Nexus switches using these SFPs with FEC mode cl74. **Note**: Ensure that the FEC mode cl74 is enabled on both devices for proper link operation. This update resolves prior connectivity issues and improves link stability.
Compliance	6 GHz country support for new countries	From Cisco IOS XE 26.1.1 onwards, Azerbaijan (AZ), Egypt (EG), Kazakhstan (KZ), Mauritius (MU), Tunisia (TN) and Monaco (MC) are added to the list of countries that support the 6 GHz radio band. For more information, refer to Countries and Regulations.
API experience	IPv6 support in Network Services	This feature exposes DHCPv6 statistics — including message counts, message latency, address assignment counts, request success rates, and error metrics — to the network service analytics framework such as Catalyst Center, enabling monitoring and

Product impact	Feature	Description
	Analytics (NSA) for DHCP	troubleshooting of DHCPv6 operations. The primary benefit of operation is improved visibility into IPv6 address assignment behavior and faster identification of assignment failures or performance regressions, enhancing operational reliability and incident response.
	Cisco TrustSec REST-based policy and environment data provisioning enhancement	This feature enables Cisco TrustSec-enabled devices to download SGACL policies and environment data from a Cisco Identity Services Engine (ISE) server using a secure, REST-based transport protocol. By replacing or supplementing the older RADIUS-based methods, this approach provides faster, more reliable data delivery and enhanced security through TLS 1.2 encryption on port 9063. The feature supports multiple server configurations with both ordered and random selection logic, allowing for effective load distribution. Additionally, it includes robust failover mechanisms, such as server liveliness checks and the ability to handle HTTP 429 "overloaded" responses, ensuring that network devices maintain synchronized and up-to-date security policies. For more information, refer to Cisco TrustSec.

MIBs

The following MIB has been modified:

- AIRESPACE-WIRELESS-MIB.my

Product analytics

Cisco IOS XE Product Analytics collects device Systems Information for the purposes of understanding product usage, enabling product improvements and product development, and assisting in product adoption and sales support. Only summarized data of feature usage and statistical counters of configuration are collected. No personal identifiable information, such as MAC/IP addresses, usernames, custom configuration names, or user provided strings, are collected as part of Cisco IOS XE Product Analytics. Cisco processes this data following the General Terms, the Cisco Privacy Statement, and any other applicable agreement with Cisco.

Refer to Cisco Enterprise Networking Product Analytics Frequently Asked Questions.

Change in behavior

Table 2. Change in behavior for Cisco Catalyst 9800 Series Wireless Controllers, Release 26.1.1

Feature	Description
The show AP command does not work for 5 GHz with slot 0	AP models such as CW9176D1 and CW9176I with dual-band radios support 5 GHz operation on slot 0, but the controller only recognizes slots 1 and 2 for 5 GHz commands. As a result, the commands targeting 5 GHz on slot 0 return an invalid input error. This limitation affects both command execution and slot selection prompts, impacting management of these APs. With the change in behavior, the **show ap** *ap-name* **dot11 dual-band urwb detail** command has been added to display dual-band radio details to address this gap.

Feature	Description
Support for standard power bias in Automated Frequency Coordination (AFC)	With the introduction of AFC and standard power, managing standard power bias has become increasingly important, especially for deployments using CW9179F or external-antenna 6 GHz APs in high-ceiling environments, where reliability is critical. This enhancement provides an option to enable standard power bias within RRM, ensuring optimal performance and compliance, particularly in AFC environments. To operate the APs in standard power mode: • At least five AFC channels must be available based on the configuration (including channel width, DCA channel list, and PSC settings). • The AFC license must support a minimum power level of 1.
Deprecation of commands of obsolete features	This update introduces a warning message for certain wireless configuration commands as part of a feature deprecation process. Previously, these configuration commands could be used without any warnings: • OSEN: **security wpa osen** • Aggressive Load Balancing: **load-balance** • WEP: **security static-wep-key** • Airtime Fairness (ATF): **wireless profile airtime-fairness** *profile-name id* From 17.18.2 onwards, using any of these commands displays a warning message indicating that the features are deprecated.
CW9179F Environmental Pack Serial Number is displayed in the AP command output	The output of **show** commands (for example, **show ap name** *ap-name* **config general**) have been updated to include the CW9179F Environmental Pack Serial Number. In the earlier release, this information was not displayed in the command output. With this enhancement, you can now easily view the CW9179F Environmental Pack Serial Number directly from the command output improving visibility and simplifying device management.
Unable to push a large RPC configuration through Netconf over SSH	Previously, the configuration was blocked at the input level if it exceeded the platform's AP limit for a specific site tag. Now, the system allows the configuration to be applied, but the actual enforcement of the limit (preventing APs from joining) is handled by the configuration validator, to avoid configuration failure due to the high time taken in validating the input.
Updated Mesh PSK downgrade procedure (Release 26.1.1)	MAP is unable to connect if authentication method is PSK, during the downgrade process from Cisco IOS XE 26.1.1 to an older release such as 17.18.x or 17.15.x. If you are using PSK for Mesh authentication and need to downgrade to a version that does not include this fix, follow these steps: 1. Before downgrade: Enable the default PSK. 2. After downgrade: MAPs should typically join the controller successfully if the provisioned PSK remains unchanged. If MAPs fail to join using PSK, perform these recovery steps: • Change the Mesh authentication method to EAP. • Once the MAPs have joined the controller through EAP, run this command on the controller for each of the affected APs: **ap name** *ap_name* **mesh security psk provisioning delete** • Change the Mesh authentication method back to PSK. The MAPs will join using the default PSK and then automatically update to the provisioned PSK. 3. Once all APs have successfully joined the controller, disable the default PSK.

Feature	Description
Cisco Catalyst 9800 Controller mobility tunnel encryption downgrade	In the earlier releases, if two mobility peers had different settings for Mobility DTLS Encryption, the tunnel was allowed to be set up. With the change in behavior, both peers must have the DTLS encryption enabled, for the tunnel to be established (up).
SELinux denials for power cycling after FPGA upgrade	A manual power cycle was required after an FPGA upgrade to ensure the changes took effect. With the change in behavior, the system performs an automatic power cycle upon completion of the FPGA upgrade.
Non-standard CLI naming convention for dual-band channel width	The CLI command **ap name** *ap_name* **dot11 dual-band channel width** displays non-standard sub-options, incorrectly appending a " w" to each channel width value (for example, " 160w" instead of the standard " 160"). This issue is seen across all APs with XOR radios in both Local and FlexConnect modes. With the behavior change, the “w” has been removed from the command sub-options.
Support added for Policy Type, Encryption Cipher, and AKM on the Clients Grid, in the controller GUI	In the earlier releases, users could not view the WLAN policy, encryption, and AKM that a client is currently connected to, all at one place. Due to this limitation, administrators had to perform manual CLI checks for each client individually or develop custom scripts to aggregate the necessary information, resulting in significant operational inefficiency. With the change in behavior, Policy Type, Encryption Cipher, and AKM details are added to the Clients Grid in the controller GUI.
Accelerometer support – Integration of tilt information (accelerometer) into the **show ap config general** command output	To improve the efficiency of physical installation monitoring, accelerometer data—specifically tilt angle and last update timestamp—were directly integrated into the **show ap config general** command and the **show tech wireless** output. This information was isolated within a specific, granular command, which hindered the ability to perform automated, large-scale detection of mounting or installation issues. Including this data in the general configuration summary will allow for streamlined, automated verification of AP physical orientation across the network.
Command failure for 5 GHz radio-reset statistics on CW9171I APs	The **show** *ap-name* **dot11 5ghz radio-reset stats** command was non-functional for CW9171I APs operating on the 5 GHz radio band. A new command has been introduced to address this issue: **show ap name** *ap-name* **dot11 dual-band slot** *0-2* **radio-reset stats**.
Deprecation of **jumbo-mtu** and removal of CAPWAP jumbo frame from AP profile.	CAPWAP jumbo frames are not supported on the AP side. Therefore, the **jumbo-mtu** command is deprecated and CAPWAP jumbo frame is removed from the AP profile.
Enhanced output for **show ap location stats** command	In the earlier CLI output format of the **show ap location stats** command, the details for “Clients on 11a" was not displayed properly. With the change in behavior, the output has been modified to display details about clients on slot 0, 1, 2, and 3.

Notice of upcoming changes in the Cisco IOS XE 26.1.1 release and beyond

Resilient infrastructure

As part of the ongoing commitment to network security, this release introduces secure alternatives to legacy commands. These updates are designed to mitigate potential risks and assist in establishing a more robust and secure operational baseline.

The identified insecure commands are categorized as:

- Line transport: Updates to secure remote access methods.
- Device server configuration: Hardening of server-side settings.
- File transfer protocols: Transitioning to encrypted transfer methods.
- SNMP: Enhancements to secure management traffic.
- Passwords: Strengthening authentication and credential management.
- Miscellaneous: General security improvements for various system functions.

The **show system insecure** configuration command introduced in Cisco IOS XE 17.18.2 release list all configured insecure commands configured on the device. For all detected insecure configurations during device boot or upgrade, error messages are displayed.

In Cisco IOS XE 26.1.1 release, all insecure CLI commands are blocked by default to strengthen your network infrastructure. If your environment requires the use of a legacy command, you must enable the **system mode insecure** command in global configuration mode.

- Recommendation: Do not use insecure mode. This mode is temporary and will be removed in a future release. Identify and replace all insecure commands with their secure alternatives.
- Upgrade behavior: If you upgrade to Cisco IOS XE 26.1.1 release with insecure commands already present in the running configuration, the system mode insecure command is automatically added to your configuration to prevent service disruption.

For more information, refer this document Cisco 9800 Wireless Controller Resilient Infrastructure.

Resolved issues

To refer to additional information about the issues, click the bug ID to access the Bug Search Tool (BST).

Table 3. Resolved issues in Cisco Catalyst 9800 Series Wireless Controllers, Release 26.1.1

Bug ID	Description
CSCwq60926	IOT APs sending Geolocation Reports very frequently
CSCws39961	URWB: Wi-Fi2 channel not applied in dual-radio mode
CSCws98340	IW9165E WGB 6 GHz radio firmware crash during long-duration roaming
CSCwq72187	Kernel Panic Crash When Disabling Built-in Packet Dump with Ongoing Traffic on WGB
CSCwr00889	URWB Standalone: CDP dropped when native vlan disabled; unable to negotiate POE
CSCwr25112	IW916x WGB: Group Key (GTK) rekey failure when Radio2 becomes uplink

CSCwr70521	Standalone URWB: Live **mcs maxmcs** command disables HE rates
CSCwr83518	IW9165 : SNMPd Crash on Cisco IW9165 in URWB Mode on Software Version 17.18.1
CSCws60129	WGB Out of Service due to NAPT Port Range Configuration Sequence
CSCws61721	Standalone URWB: LNO is not fully enabled with default setting but CLI showing it is enabled
CSCws68524	Fluidity 5845 MHz not working between IW9165 and IW9167
CSCwp14628	Cisco Aironet 3800 APs display client authentication issue after AP Migration to a controller running 17.15.3
CSCwp20385	Cisco Catalyst 9136 AP wired 0 interface gets stranded, and RX packets are not processed
CSCwp27601	Radio 1 FW crash observed while running longevity with ~20+ clients on 3802 AP
CSCwp65769	Cisco Wave 2 APs performing with fast transition with 802.1X authentication send incorrect M2 message during re-key on session timeout
CSCwq12607	9120 AP unexpected reload due to Radio firmware beacon TX stuck
CSCwq18287	17.15.4 - Capwapd Crash on 9162 AP's while notifying to spaces_grpcd
CSCwq50978	9176 access points slot 1 reset with reason (radio failure (Firmware crash))
CSCwq71415	AP1852 sends excessive BAR flood due to Client not responding to data
CSCwq93561	[SIT]17.18.2: CW9172 Observed crash while running longevity
CSCwq96192	17.18.2: 9171/9174: qdf_bug Kernel Panic lr: vap_wait_for_vdev_init_state+0x27c/0x2c0
CSCwq97854	Flex WLAN VLAN mappings not retained on COS APs with 9800 controller
CSCwr21290	Catalyst 9105 APs stops ACKing frames due to RX Stuck and fails for clients connected in 5 GHz Slot
CSCwr21879	SKB memory related crashes on Wi-Fi7 APs
CSCwr56409	Wireless client is not receiving IPv6 RA from wired on FlexConnect AP
CSCwr67024	Edge receives a Discover from AP in L2LI0 interface, instead of in the Access Tunnel, due to the wrong IP source of the AP.
CSCwr77247	AP crash on 9174I running 17.18.2: Kernel Panic
CSCwr81031	Memory leak on 9176 APs on kmalloc slabs
CSCwr94814	9115 AP unexpected reload due to Radio firmware beacon TX stuck
CSCwr98669	C9176 FW Crash - cnss_pci 0004:01:00.0: CRASHED
CSCws01793	NSS driver initialization failure during bootup on the 9178 AP
CSCws06706	C9178: Clients unable to join 2.4 radio due to MAC HW Hang/PHY Error
CSCws08240	Wi-Fi 7 APs: Crash files generated in controller with reason reload due to power on reset - 33

CSCws08681	CW9178I AP - No Clients are able to connect due to NSS count not incrementing
CSCws22667	Throughput Issue on Uploads via RLAN Ports 2 and 3 on Cisco 9105AWX/9172H AP; Port 1 Unaffected
CSCws26825	9105 stops accepting clients due to RX too late errors
CSCws32577	9130 RAP, systemd[1]: CAPWAPd.service watchdog timeout (limit 1min 30s)! , continuously reloading and not joining to controller
CSCws67290	BGL18 Alpha: Radio crash corrupted coredump is seen on AP CW9174I
CSCws77227	AP CW9176I kernel panic crash
CSCws77337	9166 SDA APs having image download issues due to /tmp not having enough space caused by sdavc App pack
CSCws80385	AP CW9176I kernel panic random crash
CSCws87617	9130 not able to upgrade to 17.18.2 CCO image due to another upgrade is still in progress
CSCwt19117	Dot11u config is removed from AP so AP stops beaconing with dot11u impacting OpenRoaming
CSCwt26500	Need changes for CSCwq11842 to work in all AP models
CSCwt33908	9136-26.2.1: \" ERR_IN_PHY_OFF:0 Ucode Asserted\" radio 1 crash followed by AP crash \" lr : ol_ath_wifi_ssr+0xde4/0x10e0 [qca_ol]\" during longevity
CSCwt53021	2.4G Radio not coming up for CW9163-E AP when country code is configured as SR
CSCwp63176	Cisco IOx app channel is down due to a state mismatch between the IOx and CAF apps on the Cisco Catalyst 9136 AP
CSCwp65077	AP crash due to radio failure(too many radio failures)
CSCwq66265	Client sending HE capabilities to wifi5 AP triggers association failure
CSCwq73441	CW9172I AP: Kernel panic running 17.15.4
CSCwq73700	COS APs is not keeping manual Geolocation coordinates across reboots
CSCwr01343	9166 AP Radio Interface down after booting up process
CSCwr26505	C9130 AP fails to send Discovery Request with IPv6 Address post an Outage.
CSCwr28328	kernel log messages \" wlan_crypto_encap: Key is NULL\" filling up the AP syslog
CSCwr32085	1815 AP Trace Event Crash
CSCwr69841	CW9176 showing two mac addresses behind the switchport
CSCwr77108	When using FT11r or OKC in FlexConnect local auth, AP discard VLAN pushed by RADIUS server
CSCwr77143	CW9166/IW9167: Kernel panic crash running 17.15
CSCwr96590	C9120 AP NMI watchdog crash : soft lockup - CPU#3 stuck for s! [kclick:]
CSCwr97281	9105 AP is over reporting interference under \" auto-rf\" result

CSCws25172	9166 APs keep crashing when 6GHz radio is on, using RO country code on controller version 17.15.3
CSCws35315	Auxiliary-client interface taking over the CAPWAP connection from the AP
CSCws47852	AP intermittently joins the controller, but controller fails to get AP type resulting AP being rejected
CSCws60984	9166 crash systemd[1]: CAPWAPd.service failed.
CSCws70285	Clean up for /storage/cnssdaemon.log
CSCws72425	9136I IOX application activation failure
CSCws76582	17.15.3 -Stale client entries prohibiting fresh assoc on AP
CSCws79118	Unexpectedly reduced transmit power for 9124-AXE on 2.4 GHz in -Z regulatory domain
CSCwt09003	Clients not connecting to \" FT+SAE\" when AP is in FlexConnect mode with central authentication
CSCwq66623	SJC Alpha - 17.18.2 alpha APs not joining controller- stuck in DTLS
CSCwr20303	Controller unexpected reload after modifying ap location name config
CSCwr65627	Large number of APs (2K+) take several minutes to join N+1 controller when Primary goes down
CSCwr67652	Controller mem is noticed due to wsa_db
CSCwr90981	AP count varying in 5 GHz radio
CSCws16148	Controller crash after issuing the command \" ap geolocation ranging accurate method uwb\"
CSCws18528	[APCI] MLO Rogue Containment for all bands is not working
CSCws38733	AP ranging CLI triggers a controller switchover and core file is created
CSCws39889	RF Based AP Load Balancing: controller crash due to observed during load balancing algo run
CSCws58494	WebAuth Clients moved to RUN State on the controller but it is stuck in WebAuth on the AP
CSCws58703	SST: ndbmand cores are seen after ISSU upgrade from 17.15.x to 17.18.2 with CatC, NETCONF not working
CSCws65956	Controller crash with wncmgrd has been helddown (rc 139)
CSCws91899	C9800 Crash while processing FlexConnect Client
CSCws93542	Post failover DHCP Offer is not forwarded by the controller to the client
CSCwr30777	9800 standby chassis shows Cisco Unknown Power Supply and same SN on output from \" show inventory\" 17.12.4
CSCwr74373	C9800 controller Accounting-Request packets are not sent when an ungraceful disassociation takes place
CSCwr79853	In file manager, when selecting one file in the location box, download fails
CSCwr80088	Site tag and policy tag are not mapped correctly to 9130AP on controller

CSCwr96860	Antenna Gain configuration via RESTCONF RPC fails for AP models 3800E and 9120AXE \u2014 \u201cslot: 0 does not have a dedicated radio\u201d error
CSCws10863	9800 - APs with an unresolved regulatory domain stop RRM from running for other APs
CSCws17702	PAED process crashes every 24 after record pruning and DB query errors.
CSCws19686	Configuring duplicate AP names results in \" Internal Error, Check Logs\" instead of duplicate name warning
CSCws22542	17.15.3 6GHz band support missing for Turkey in RW domain
CSCws26758	Controller client entries causing AP to reach max number of clients per radio
CSCws30144	Cloud services OTP token for Virtual Wireless Controller disappears in some edge cases
CSCws31873	Media-Stream and Multicast traffic fails after SSO when GTK key-rotation is enabled
CSCws46519	When running \" show ap lldp neighbor\" on the controller, outdated information continues to persist.
CSCws49525	SIT: CleanAir Pro - Spectral Capture; fails to provide: spectral_recording directory/file on eWLC despite: Upload-Response (Success)
CSCws62182	The GUI displays the channel Bandwidth (Negotiated/capable) wrong
CSCws66137	Client association time shown as \" 01/01/1970 00:00:00\" while local authentication (no central authentication) is in place
CSCws82703	SeLinux: qwlc: subject polaris_iosd_t denials 2026-01-16 11:14:35 - while trying to access installation file from webui
CSCws83128	AP rename fails with false \u201cAP name already exists\u201d conflict for a specific hostname string (not present in AP database), controller reverts AP to default name
CSCws93326	SJC Alpha 26.1.1 ERR Logs: (ERR): MAC: 0000.0000.0000 \u00a0Set RA trace entry for multi link client. Unable to fetch dot11 operational data
CSCwt21195	Default 6 GHz RF profile cannot be selected when creating a new location
CSCwt21642	802.11r PMK cache uses wrong client auth type because it is never looked up
CSCwt25978	Wireless bundle client does not work with site tag space in name
CSCwt41808	wncmgrd Process Crash Due to Invalid String Pointer during AP Join AVL Tree
CSCwt41939	TMPFS Memory leak in IOS_PRIV_OPER_DB tbl_ewlc_critical_events table after selinux denials

Open issues

To refer to additional information about the issues, click the bug ID to access the Bug Search Tool (BST). This section lists the open issues that apply to the current release and might apply to releases earlier than Cisco Catalyst 9800 Series Wireless Controllers, Release 26.1.1. An issue that is open for an earlier release and is still unresolved applies to all future releases until it is resolved.

Table 4. Open issues in Cisco Catalyst 9800 Series Wireless Controllers, Release 26.1.1

Bug ID	Description
CSCwp26522	IW9167E slot2 as client serving on 5G band hit beacon stuck
CSCwt37025	URWB controller: connecting issue (to controller) after factory reset
CSCwr37961	QZSS Constellation Incorrectly Reported by GNSS Filtering Logic
CSCwr74409	Signaling packets 0x998 do NOT forwarded after Mobility Client scanning
CSCws62538	IW9165E WGB 6G band downlink broadcast pkts not converted to reliable Unicast when interop with 17.15 WIFI7 infra APs
CSCwt40834	IW9165E Remote Mobility Client Fails to Rejoin Controller via Wireless Backhaul After Dynamic Channel Width Change
CSCwt42516	AP URWB radio channel display inconsistency between the AP and controller after applying the channel hot config
CSCwt38787	MPO enabled on wired-only mobility coordinator requires mobility profile on slot
CSCwt31537	When AP is configured with MACsec and switch is not, AP fails to obtain IP address
CSCwk79990	9800-L encounters kernel unresponsiveness due to IntelResetRequest
CSCws42581	Memory corruption in L2 multicast while handling dynamic multicast router ports and group
CSCws47700	WGB roaming may trigger a wncd process unexpected reload and wireless controller reload.
CSCws68160	Controller Unexpected reload with Critical process wncd fault on rp_0_0 (rc=139) after client deletion
CSCws68479	Missing support for certain bands and channels in wifi6/6e regdb
CSCwt03837	Standby Platform with HA facing unexpected reloads due LocalSoft
CSCwt07093	APs not being able to connect due CAPWAP messages being queued
CSCwt08175	AP Kernel Panic due to PC is at _ZN17SPSCPriorityQueue4pushEiP6Packet+0x7c/0x4c8 LR is at _ZN17SPSCPriorityQueue4pushEiP6Packet+0x40/0x4c8
CSCwt09034	DTLS Alert Message processing and Open SSL Decryption on C9800-CL leads to watchdog crash in WNCD
CSCwt13732	WNCD process is getting terminated unexpectedly, causing controller to crash (Critical process wncd has failed (rc 0))
CSCwt19011	9166 17.15.4b AP in SDA mode not forwarding IPv4 ARP upstream or other IPv4 packets after DHCP
CSCwt19092	9179 running 17.18.2 reporting more than 4 DFS in less than 1 hour
CSCwt19490	9800 controller: Stale client IP used in RADIUS accounting causes ISE IP\u2013SGT/SXP overwrite
CSCwt20299	Application traffic is using wired0 as egress interface instead of auxiliary client interface
CSCwt22893	Controller unexpected SISF reboot with WNCD core on 17.18.2

Bug ID	Description
CSCwt26353	After ISSU upgrade to 17.15.4d from 17.12.5, SSIDs aren't pushed to APs
CSCwt26718	eCA upgrade operation failed due to non response from wncmgrd
CSCwt31565	Wireless Clients Stuck in RUN State on Cisco 9800-40-K9 Running 17.12.6a
CSCwt31826	Constant switchover and/or reload due to SIGSEGV on rogued process
CSCwt37351	The wncd process unexpected finish due to an invalid handler-id for a a radio WLAN id and controller may reload
CSCwt38788	The mobility process ends unexpectedly due to an uninitialized variable; controller may be reloaded.
CSCwt42369	C9136I Radio Crash
CSCwt50389	Ascom Myco2 phones are not able to connect to 9176 APs due to EAP_ID_REQ or M2 not acked by AP
CSCwt52617	Post SSO - Few wireless clients experiences loss of connectivity to devices outside the Fabric
CSCwt52815	Controller fails to update associated Channel width for client after it is changed on AP radio
CSCwt53635	Memory Leak on C9800-40-K9 in the wncmgrd process
CSCwt58260	AP drops dot11 open auth request at driver
CSCwt58849	CAPWAPd process keeps crashing
CSCwk07132	AP AAA client rate limit with flex connect local switching changed in 17.12.3 to per stream
CSCwr96781	No AQ info output for 6Ghz band \" show ap dot11 6ghz cleanair air-quality summary\" command in controller
CSCws03721	9120/9115/9105 AP does not ACK frames sent from iOS devices follow up of CSCwj91255
CSCws17518	Unexpected reload after running a command on a controller
CSCws78457	Wired client behind WGB stops passing traffic after several days
CSCws80754	Local DHCP on Anchor controller intermittently stops forwarding DHCP OFFER or ACK
CSCws93044	AP does not transmit beacons for over one second right after the client connects
CSCws94151	SFP \" SFP-H25G-CU1M\" is not working in C9800M - 17.15.03 and Nexus C93180YC-EX
CSCws95359	10G Ports not coming UP on CW9800M, CW9800H1 with various SPFs models.
CSCwt20158	bsnMobileStation showing only a few clients - root cause is Wifi7
CSCwt39820	APs Does Not Receive Accelerometer Settings from AP Join Profile
CSCwt40423	Cloudm Tracebacks running out of ID
CSCwt43333	C9120E dual-band-role XPath does not apply 5 GHz sniffer configuration despite HTTP 204 success

Bug ID	Description
CSCwt44743	CW9166I randomly drops ARP query from Zebra MC9300 RF gun
CSCwt47490	CW9166 COS AP crashed after first initial boot up due to kernel panic
CSCwt51709	COS APs initiate DHCP process even when static IP is configured, causing intermittent DHCP Fallback issues
CSCwt53740	AP not broadcast SSID due to some policy config pushing failed from controller
CSCwt58405	C9800-CL-K9/CAC triggered after failover despite no channel change

Compatibility

Compatibility matrix

The following table provides software compatibility information. For more information, refer to Cisco Wireless Solutions Software Compatibility Matrix.

Table 5. Compatibility Matrix for Cisco Catalyst 9800 Series Wireless Controllers, Release 26.1.1

Cisco Catalyst 9800 Series Wireless Controller Software	Cisco Identity Services Engine	Cisco Catalyst Center	Cisco CMX
IOS XE 26.1.1	3.4 3.3 3.2 3.1 3.0 * all with latest patches	Refer to Cisco Catalyst Center Compatibility Information.	11.1.1

Software requirements

Operating Systems:

- Windows 10 or later
- macOS 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 that 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:

```
Device# configure terminal
Device(config)# line vty 50
```

The best practice is to configure the service tcp-keepalives to monitor the TCP connection to the device.

```
Device(config)# service tcp-keepalives-in
Device(config)# service tcp-keepalives-out
```

Before you upgrade

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

- If you have APs in remote sites, behind a WAN link, read the following document to accelerate the image download and make it more reliable: https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/223125-understand-access-point-image-upgrades.html.
- When you upgrade from Cisco IOS XE 17.9.5 or lower, or 17.12.2 or lower, to Cisco IOS XE 17.18.2, the controller WebUI does not support images greater than 1.5 GB.

  Workaround:

  - Upgrade using the CLI commands, or,
  - Upgrade to 17.9.6, 17.12.3, or higher, then upgrade to 17.18.2 or later.
- For images: If upgrading from 17.9.6 or lower, 17.12.4 or lower, or 17.15.1 or lower, to 17.18.2, Cisco Catalyst Wi-Fi 6 APs may fail to upgrade their image due to lack of space on the temporary partition.

  Workaround:

  - Reboot the impacted APs using a power cycle, then procced to upgrade normally.

  For more information, refer to CSCwm08044 and CSCwm07499.
- APs running older release code (before 8.10.190.0, 17.3.8, 17.6.5, 17.9.3 or older), may get into a boot loop when upgrading software over a WAN link. For more information, refer to : 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 in 17.18.2 and higher, and they will not join the controller. We recommend that you validate the current models before upgrading:
  - Cisco Aironet 1570 Series Access Point
  - Cisco Aironet 1700 Series Access Point
  - Cisco Aironet 2700 Series Access Point
  - Cisco Aironet 3700 Series Access Point
- 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, refer to 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:
    - 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>
```

    - 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
```

    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 use of MTU lower than 1500 on G0 (OOB) interface that may cause fragmentation for RADIUS packets for client authentication, is not supported.
- 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:

```
ip http session-module-list pkilist OPENRESTY_PKI
ip http active-session-modules pkilist
```

- Cisco Aironet 1815T OfficeExtend Access Point will be in local mode when connected to the controller. However, when it functions as a standalone AP, it gets converted to FlexConnect mode.
- The Cisco Catalyst 9800-L Wireless Controller may fail to respond to the BREAK signals received on its console port during boot time, preventing users from getting to the ROMMON. This problem is observed on the controllers manufactured until November 2019, with the default config-register setting of 0x2102. This problem can be avoided if you set config-register to 0x2002.

  This problem is fixed in the 16.12(3r) ROMMON for Cisco Catalyst 9800-L Wireless Controller. For information about how to upgrade the ROMMON, refer to 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.
- 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:

```
device# configure terminal
```

```
device(config)# no crypto pki trustpoint trustpoint_name
device(config)# no ip http server
device(config)# no ip http secure-server
device(config)# ip http server
device(config)# ip http secure-server
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.
- 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 Centralized Key Management (CCKM) feature was deprecated in Cisco IOS XE 17.10.x but currently remains supported. However, support for CCKM will be removed in a future release. Therefore, we recommend that you migrate to Fast Transition (FT) with 802.1X authentication and validate the configuration with supported key caching mechanisms.
- 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 to reflect an earlier time.
- 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: 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.

- Before you begin a downgrade process, you must manually remove the configurations which are applicable in the current version but not in the older version. Otherwise, you might encounter unexpected behavior.
- To upgrade the field programmable hardware devices for Cisco Catalyst 9800 Series Wireless Controllers, refer to Upgrading Field Programmable Hardware Devices for Cisco Catalyst 9800 Series Wireless Controllers.

Upgrade path to Cisco IOS XE 26.1.1

Table 6. Upgrade Path to Cisco IOS XE Dublin 26.1.1

Current software	Upgrade path for deployments with 9130, 9124, or 916x	Upgrade path for deployments without 9130 and 9124
16.10.x	– **Note:** The Cisco Catalyst 9130 and 9124 APs are not supported in 16.10.x and 16.11.x releases.	Upgrade first to 16.12.5 or 17.3.x and then to 26.1.1.
16.11.x	–	Upgrade first to 16.12.5 or 17.3.x and then to 26.1.1.
16.12.x	Upgrade first to 17.3.5 or later or 17.6.x or later, then to 17.9.6 or later or 17.12.x or later, and then to 26.1.1.	Upgrade first to 17.3.5 or later or 17.6.x or later, and then to 26.1.1.
17.1.x	Upgrade first to 17.3.5 or later or 17.6.x or later, then to 17.9.6 or later or 17.12.x or later, and then to 26.1.1.	Upgrade first to 17.3.5 or later and then to 26.1.1.
17.2.x	Upgrade first to 17.3.5 or later or 17.6.x or later, then to 17.9.6 or later or 17.12.x or later, and then to 26.1.1.	Upgrade first to 17.3.5 or later and then to 26.1.1.
17.3.1 to 17.3.4	Upgrade first to 17.3.5 or later or 17.6.x or later, then to 17.9.6 or later or 17.12.x or later, and then to 26.1.1.	Upgrade directly to 26.1.1.
17.3.4c or later	Upgrade to 17.9.6 or later or 17.12.x or later, and then to 26.1.1.	Upgrade directly to 26.1.1.
17.4.x	Upgrade first to 17.6.x and then to 26.1.1.	Upgrade directly to 26.1.1.
17.5.x	Upgrade first to 17.6.x and then to 26.1.1.	Upgrade directly to 26.1.1.
17.6.x	Upgrade to 17.9.6 or later or 17.12.x or later, and then to 26.1.1.	Upgrade directly to 26.1.1.
17.7.x	Upgrade to 17.9.6 or later or 17.12.x or later, and then to 26.1.1.	Upgrade directly to 26.1.1.
17.8.x	Upgrade to 17.9.6 or later or 17.12.x or later, and then to 26.1.1.	Upgrade directly to 26.1.1.
17.9.1 to 17.9.5	Upgrade to 17.9.6 or later or 17.12.x or	Upgrade directly to 26.1.1.

Current software	Upgrade path for deployments with 9130, 9124, or 916x	Upgrade path for deployments without 9130 and 9124
	later, and then to 26.1.1.	
17.9.6 or later	Upgrade directly to 26.1.1.	Upgrade directly to 26.1.1.
17.10.x	Upgrade to 17.12.x or later, and then to 26.1.1.	Upgrade directly to 26.1.1.
17.11.x	Upgrade to 17.12.x or later, and then to 26.1.1.	Upgrade directly to 26.1.1.
17.12.x	Upgrade directly to 26.1.1.	Upgrade directly to 26.1.1.
17.13.x	Upgrade directly to 26.1.1.	Upgrade directly to 26.1.1.
17.14.x	Upgrade directly to 26.1.1.	Upgrade directly to 26.1.1.
17.15.x	Upgrade directly to 26.1.1.	Upgrade directly to 26.1.1.
17.16.x	Upgrade directly to 26.1.1.	Upgrade directly to 26.1.1.
17.17.x	Upgrade directly to 26.1.1.	Upgrade directly to 26.1.1.
8.9.x or any 8.10.x version prior to 8.10.171.0	Upgrade first to 8.10.171.0 or later, 17.3.5 or later, or 17.6.x or later, then to 17.9.6 or later or 17.12.x or later, and then to 26.1.1.	Upgrade directly to 26.1.1.

Upgrading the controller software

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

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 26.1.1

Image names (9800-80, 9800-40, and 9800-L):

- C9800-80-universalk9_wlc.26.01.01.SPA.bin
- C9800-40-universalk9_wlc.26.01.01.SPA.bin

- C9800-L-universalk9_wlc.26.01.01.SPA.bin

Image names (CW9800M, CW9800H1/CW9800H2, CW9800L)

- CW9800H-wlc-universalk9.26.01.01.SPA.bin
- CW9800M-wlc-universalk9.26.01.01.SPA.bin
- CW9800L-wlc-universalk9.26.01.01.SPA.bin

Image names (9800-CL):

- **Cloud**: C9800-CL-universalk9.26.01.01.SPA.bin
- **Hyper-V/ESXi/KVM**: C9800-CL-universalk9.26.01.01.iso, C9800-CL-universalk9.26.01.01.ova
- **KVM**: C9800-CL-universalk9.26.01.01.qcow2
- **NFVIS**: C9800-CL-universalk9.26.01.01.tar.gz

Software installation commands

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.

Commands	Description
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

Cisco Wireless Licenses

Cisco Wireless Licenses, a part of the Cisco Networking Subscription licensing model, is a software license that helps you to deploy your Wi-Fi 7 Access Points in an on-premise, hybrid, or a cloud managed network. From Cisco IOS XE 17.15.2, Cisco Wireless licenses are supported on Wi-Fi 7 Access Points (APs) and later models.

The Cisco Wireless Licenses consist of the following tiers:

- Cisco Wireless Essentials: The tier that provides fundamental features and functionalities that are essential to manage a network.

- Cisco Wireless Advantage: The tier that supports additional features and capabilities and includes all the essential capabilities in addition to the advanced capabilities to manage a network.

For more information, refer to Cisco Wireless Licensing.

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 7. Test configuration for interoperability

Hardware or software parameter	Hardware or software type
Release	Cisco IOS XE 26.1.1
Cisco Wireless Controller	Refer to Supported hardware
Access Points	Refer to Supported APs
Radio	• 802.11ac • 802.11ax • 802.11a • 802.11g • 802.11n • 802.11be (Wi-Fi 7)
Security	Open, PSK (WPA2-AES), 802.1X (WPA2-AES) (EAP-FAST, EAP-TLS), WPA3 AKM
RADIUS	Refer to Compatibility Matrix
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 8. Client types

Client type and name	Driver or software version
Laptops	
Acer Aspire E 15 E5-573-3870 (Qualcomm Atheros QCA9377)	Windows 10 Pro (12.0.0.832)
Apple MacBook Air 11 inch	macOS Sierra 10.12.6
Apple MacBook Air 13 inch	macOS High Sierra 10.13.4
MacBook Pro Retina	macOS Catalina
MacBook Pro Retina 13 inch early 2015	macOS Mojave 10.14.3
MacBook Pro OS X	macOS X 10.8.5

Client type and name	Driver or software version
MacBook Air	macOS Sierra v10.12.2
MacBook Air 11 inch	macOS Yosemite 10.10.5
MacBook M1 Chip	macOS Catalina
MacBook M1 Chip	macOS Ventura 13.2.1
MacBook Pro M2 Chip	macOS Ventura 13.3 beta
MacBook Pro M2 Chip	macOS Ventura 13.1
Dell Inspiron 2020 Chromebook	Chrome OS 75.0.3770.129
Google Pixelbook Go	Chrome OS 97.0.4692.27
HP Chromebook 11a	Chrome OS 76.0.3809.136
Samsung Chromebook 4+	Chrome OS 77.0.3865.105
Dell Latitude (Intel AX210)	Windows 11 (22.110.x.x)
Dell Latitude 3480 (Qualcomm DELL wireless 1820)	Win 10 Pro (12.0.0.242)
Dell Inspiron 15-7569 (Intel Dual Band Wireless-AC 3165)	Windows 10 Home (21.40.0)
Dell Latitude E5540 (Intel Dual Band Wireless AC7260)	Windows 7 Professional (21.10.1)
Dell Latitude E5430 (Intel Centrino Advanced-N 6205)	Windows 7 Professional (15.18.0.1)
Dell Latitude E6840 (Broadcom Dell Wireless 1540 802.11 a/g/n)	Windows 7 Professional (6.30.223.215)
Dell XPS 12 v9250 (Intel Dual Band Wireless AC 8260)	Windows 10 Home (21.40.0)
Dell Latitude 5491 (Intel AX200)	Windows 10 Pro (21.20.1.1)
Dell XPS Latitude12 9250 (Intel Dual Band Wireless AC 8260)	Windows 10 Home
Dell Inspiron 13-5368 Signature Edition	Windows 10 Home (18.40.0.12)
FUJITSU Lifebook E556 Intel 8260 (Intel Dual Band Wireless-AC 8260 (802.11n))	Windows 8 (19.50.1.6)
Lenovo Yoga C630 Snapdragon 850 (Qualcomm AC 2x2 Svc)	Windows 10 Home
Lenovo ThinkPad Yoga 460 (Intel Dual Band Wireless-AC 9260)	Windows 10 Pro (21.40.0)
Note: For clients using Intel wireless cards, we recommend that you update to the latest Intel wireless drivers if the advertised SSIDs are not visible.	

Client type and name	Driver or software version
Tablets	
Apple iPad Pro (12.9 inch) 6th Gen	iOS 16.4
Apple iPad Pro (11 inch) 4th Gen	iOS 16.4
Apple iPad 2021	iOS 15.0
Apple iPad 7the Gen 2019	iOS 14.0
Apple iPad MD328LL/A	iOS 9.3.5
Apple iPad 2 MC979LL/A	iOS 11.4.1
Apple iPad Air MD785LL/A	iOS 11.4.1
Apple iPad Air2 MGLW2LL/A	iOS 10.2.1
Apple iPad Mini 4 9.0.1 MK872LL/A	iOS 11.4.1
Apple iPad Mini 2 ME279LL/A	iOS 11.4.1
Apple iPad Mini 4 9.0.1 MK872LL/A	iOS 11.4.1
Microsoft Surface Pro 3 13 inch (Intel AX201)	Windows 10 (21.40.1.3)
Microsoft Surface Pro 3 15 inch (Qualcomm Atheros QCA61x4A)	Windows 10
Microsoft Surface Pro 7 (Intel AX201)	Windows 10
Microsoft Surface Pro 6 (Marvell Wi-Fi chipset 11ac)	Windows 10
Microsoft Surface Pro X (WCN3998 Wi-Fi Chip)	Windows
Mobile phones	
Apple iPhone 5	iOS 12.4.1
Apple iPhone 6s	iOS 13.5
Apple iPhone 7 MN8J2LL/A	iOS 11.2.5
Apple iPhone 8	iOS 13.5
Apple iPhone 8 Plus	iOS 14.1
Apple iPhone 8 Plus MQ8D2LL/A	iOS 12.4.1
Apple iPhone X MQA52LL/A	iOS 13.1
Apple iPhone 11	iOS 15.1
Apple iPhone 12	iOS 16.0

Client type and name	Driver or software version
Apple iPhone 12 Pro	iOS 15.1
Apple iPhone 13	iOS 15.1
Apple iPhone 13 Mini	iOS 15.1
Apple iPhone 13 Mini Pro	iOS 15.1
Apple iPhone SE MLY12LL/A	iOS 11.3
Apple iPhone SE	iOS 15.1
ASCOM i63	Build v 3.0.0
ASCOM Myco 3	Android 9
Cisco IP Phone 8821	11.0.6 SR4
Drager Delta	VG9.0.2
Drager M300.3	VG3.0
Drager M300.4	VG3.0
Drager M540	VG4.2
Google Pixel 3a	Android 11
Google Pixel 4	Android 11
Google Pixel 5	Android 11
Google Pixel 6	Android 12
Google Pixel 7	Android 13
Huawei Mate 20 pro	Android 9.0
Huawei P20 Pro	Android 10
Huawei P40	Android 10
LG v40 ThinQ	Android 9.0
One Plus 8	Android 11
Oppo Find X2	Android 10
Redmi K20 Pro	Android 10
Samsung Galaxy S9+ – G965U1	Android 10.0
Samsung Galaxy S10 Plus	Android 11.0

Client type and name	Driver or software version
Samsung S10 (SM-G973U1)	Android 11.0
Samsung S10e (SM-G970U1)	Android 11.0
Samsung Galaxy S20 Ultra	Android 10.0
Samsung Galaxy S21 Ultra 5G	Android 13.0
Samsung Galaxy S22 Ultra	Android 13.0
Samsung Fold 2	Android 10.0
Samsung Galaxy Z Fold 3	Android 13.0
Samsung Note20	Android 12.0
Samsung G Note 10 Plus	Android 11.0
Samsung Galaxy A01	Android 11.0
Samsung Galaxy A21	Android 10.0
Sony Experia 1 ii	Android 11
Sony Experia	Android 11
Xiaomi Mi 9T	Android 9
Xiaomi Mi 10	Android 11
Spectralink 84 Series	7.5.0.x257
Spectralink 87 Series	Android 5.1.1
Spectralink Versity Phones 92/95/96 Series	Android 10.0
Spectralink Versity Phones 9540 Series	Android 8.1.0
Vocera Badges B3000n	4.3.3.18
Vocera Smart Badges V5000	5.0.6.35
Zebra MC40	Android 4.4.4
Zebra MC40N0	Android 4.1.1
Zebra MC92N0	Android 4.4.4
Zebra MC9090	Windows Mobile 6.1
Zebra MC55A	Windows 6.5
Zebra MC75A	OEM ver 02.37.0001

Client type and name	Driver or software version
Zebra TC51	Android 6.0.1
Zebra TC52	Android 10.0
Zebra TC55	Android 8.1.0
Zebra TC57	Android 10.0
Zebra TC58	Android 11.0
Zebra TC70	Android 6.1
Zebra TC75	Android 10.0
Zebra TC520K	Android 10.0
Zebra TC8000	Android 4.4.3
Printers	
Zebra QLn320 Mobile Printer	LINK OS 5.2
Zebra ZT230 IndustrialPrinter	LINK OS 6.4
Zebra ZQ310 Mobile Printer	LINK OS 6.4
Zebra ZD410 Industrial Printer	LINK OS 6.4
Zebra ZT410 Desktop Printer	LINK OS 6.2
Zebra ZQ610 Industrial Printer	LINK OS 6.4
Zebra ZQ620 Mobile Printer	LINK OS 6.4
Wireless module	
Intel AX 411	Driver v22.230.0.8
Intel AX 211	Driver v22.230.0.8, v22.190.0.4
Intel AX 210	Driver v22.230.0.8, v22.190.0.4, v22.170.2.1
Intel AX 200	Driver v22.130.0.5
Intel 11AC	Driver v22.30.0.11
Intel AC 9260	Driver v21.40.0
Intel Dual Band Wireless AC 8260	Driver v19.50.1.6
Samsung S21 Ultra	Driver v20.80.80
QCA WCN6855	Driver v1.0.0.901

Client type and name	Driver or software version
PhoenixContact FL WLAN 2010	Firmware version: 2.71

Supported hardware

Supported virtual and hardware platforms

The following table lists the supported virtual and hardware platforms. (Refer to Supported PIDs and ports for the list of supported modules.)

Table 9. Supported virtual and hardware platforms

Platform	Description
Cisco Catalyst 9800-80 Wireless Controller	A modular wireless controller with up to 100-GE modular uplinks and seamless software updates. The controller occupies a 2-rack unit space and supports multiple module uplinks.
Cisco Catalyst 9800-40 Wireless Controller	A fixed wireless controller with seamless software updates for mid-size to large enterprises. The controller occupies a 1-rack unit space and provides four 1-GE or 10-GE uplink ports.
Cisco Catalyst 9800-L Wireless Controller	The Cisco Catalyst 9800-L Wireless Controller is the first low-end controller that provides a significant boost in performance and features.
Cisco 9800 Series Wireless Controller for Cloud	A virtual form factor of the Catalyst 9800 Wireless Controller that can be deployed in a private cloud (supports VMware ESXi, Kernel-based Virtual Machine [KVM], Microsoft Hyper-V, and Cisco Enterprise NFV Infrastructure Software [NFVIS] on Enterprise Network Compute System [ENCS] hypervisors), or in the public cloud as Infrastructure as a Service (IaaS) in Amazon Web Services (AWS), Google Cloud Platform (GCP) marketplace, and Microsoft Azure.
Embedded Wireless Controller on Catalyst 9000 Series Switches	The Catalyst 9800 Wireless Controller software for the Cisco Catalyst 9000 switches brings the wired and wireless infrastructure together with consistent policy and management. This deployment model supports only Software Defined-Access (SDA), which is a highly secure solution for small campuses and distributed branches.
Cisco CW9800 Series Wireless Controller (CW9800M, CW9800H1, CW9800H2, and CW9800L)	The CW9800M controller is the next generation Cisco CW9800 series wireless LAN controller built to deliver a 53% performance improvement while consuming 18% less power when compared to the previous generation models. Additionally, the CW9800M controller supports 3000 APs and 32000 clients to ensure better performance and scale for business-critical networks and provides up to 40 Gbps of forwarding throughput for both normal packet and encrypted packets while remaining a single RU designed to save you space and provide greater flexibility in your datacenters.

Platform	Description
	The CW9800H1 and CW9800H2 controllers are the next-generation Cisco CW9800 wireless LAN controllers that boast up to a 36% increase in performance and consume up to 40% less power compared to their predecessors. Additionally, the CW9800H1 and CW9800H2 models are built with a space-saving single RU design and support up to 6000 APs and 64,000 clients with 100 Gbps of maximum throughput. They also offer a choice of uplinks with either 4 x 25 Gbps (CW9800H1) or 2 x 40 Gbps (CW9800H2) configurations to meet high throughput demands of next-generation wireless requirements.
	The CW9800L controller is the next-generation, low-end controller that provides a significant boost in performance and features. Supporting up to 10 Gbps throughput, 500 APs, and 10,000 clients, the CW9800L delivers double the capacity and increased performance compared to the base C9800-L.

Supported host environments - public and private cloud

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

Table 10. Supported host environments for public and private cloud

Host environment	Software version
VMware ESXi	• VMware ESXi vSphere 6.5, 6.7, 7.0, and 8.0 • VMware ESXi vCenter 6.5, 6.7, 7.0, and 8.0
KVM	• Linux KVM-based on Red Hat Enterprise Linux 9.2, or latest version • Ubuntu 16.04.5 LTS, Ubuntu 18.04.5 LTS, Ubuntu 20.04.5 LTS
AWS	AWS EC2 platform
NFVIS	ENCS 3.8.1 and 3.9.1
GCP	GCP marketplace
Microsoft Hyper-V	Windows Server 2019, Windows Server 2025, with Hyper-V Manager (Version 10.0.x)
Microsoft Azure	Microsoft Azure

Supported PIDs and ports

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

Table 11. Supported PIDS and ports

Controller model	Description
C9800-CL-K9	Cisco Catalyst Wireless Controller as an infrastructure for cloud.
C9800-80-K9	Eight 1/10-Gigabit Ethernet SFP or SFP+ ports and two power supply slots.
C9800-40-K9	Four 1/10-Gigabit Ethernet SFP or SFP+ ports and two power supply slots.
C9800-L-C-K9	• 4x2.5/1-Gigabit ports • 2x10/5/2.5/1-Gigabit ports
C9800-L-F-K9	• 4x2.5/1-Gigabit ports • 2x10/1-Gigabit ports
CW9800H1	• 8x1 GE/10 GE SFP ports • 4x25 GE SFP interfaces
CW9800H2	• 8x1 GE/10 GE SFP Ports • 2X 40 GE QSFP interfaces
CW9800M	• Four built-in 1 GE /10 GE SFP ports • Two built-in 25 GE SFP ports
CW9800L	• 2x 10G/1G SFP Ports (Data Ports) • 2x1G Copper (RP and SP ports)

Supported SFPs

The following table lists the supported SFP models.

Table 12. Supported SFP models

SFP name	C9800-80-K9	C9800-40-K9	C9800-L-F-K9	CW9800H1	CW9800H2	CW9800M	CW9800L
COLORCHIP-C040-Q020-CWDM4-03B	Supported	–	–	–	–	–	–
DWDM-SFP10G-30.33	Supported	Supported	–	–	–	–	–
DWDM-SFP10G-61.41	Supported	Supported	–	–	–	–	–
FINISAR-LR – FTLX1471D3BCL (The FINISAR SFPs are not Cisco specific and some of the features, such as DOM, may not work properly.)	Supported	Supported	Supported	–	–	–	–
FINISAR-SR – FTLX8574D3BCL	Supported	Supported	Supported	–	–	–	–
GLC-BX-D	Supported	Supported	Supported	Supported	Supported	Supported	–

SFP name	C9800-80-K9	C9800-40-K9	C9800-L-F-K9	CW9800H1	CW9800H2	CW9800M	CW9800L
GLC-BX-U	Supported	Supported	Supported	Supported	Supported	Supported	–
GLC-EX-SMD	Supported	Supported	–	Supported	Supported	Supported	–
GLC-LH-SMD	Supported	Supported	–	Supported	Supported	Supported	Supported
GLC-SX-MMD	Supported	Supported	Supported	Supported	Supported	Supported	Supported
GLC-T	Supported	–	–	–	–	–	–
GLC-TE	Supported	Supported	Supported	Supported	Supported	Supported	Supported
GLC-ZX-SMD	Supported	Supported	Supported	Supported	Supported	Supported	–
QSFP-100G-LR4-S	Supported	–	–	–	–	–	–
QSFP-100G-SR4-S	Supported	–	–	–	–	–	–
QSFP-40G-BD-RX	Supported	–	–	Supported	Supported	Supported	–
QSFP-40G-ER4	Supported	–	–	–	Supported	–	–
QSFP-40G-LR4	Supported	–	–	–	Supported	–	–
QSFP-40G-LR4-S	Supported	–	–	–	Supported	–	–
QSFP-40G-LR4-S-RF			–	Supported	Supported	Supported	–
QSFP-40G-CSR4	–	–	–	–	Supported	–	–
QSFP-40G-SR4	Supported	–	–	–	Supported	–	–
QSFP-40G-SR4-S	Supported	–	–	–	Supported	–	–
QSFP-40G-SR-BD	–	–	–	Supported	Supported	Supported	–
QSFP-40GE-LR4	Supported	–	–	–	–	–	–
QSFP-H40G-ACU7M	–	–	–	Supported	Supported	Supported	–
QSFP-H40G-ACU10M	–	–	–	–	Supported	–	–
QSFP-H40G-CU1M	–	–	–	–	Supported	–	–
QSFP-H40G-CU2M	–	–	–	–	Supported	–	–
QSFP-H40G-CU3M	–	–	–	–	Supported	–	–
QSFP-H40G-CU4M	–	–	–	–	Supported	–	–
QSFP-H40G-CU5M	–	–	–	–	Supported	–	–

SFP name	C9800-80-K9	C9800-40-K9	C9800-L-F-K9	CW9800H1	CW9800H2	CW9800M	CW9800L
QSFP-H40G-CU0-5M	–	–	–	–	Supported	–	–
QSFP-H40G-AOC1M	–	–	–	–	Supported	–	–
QSFP-H40G-AOC2M	–	–	–	–	Supported	–	–
QSFP-H40G-AOC3M	–	–	–	–	Supported	–	–
QSFP-H40G-AOC5M	–	–	–	–	Supported	–	–
QSFP-H40G-AOC7M	–	–	–	–	Supported	–	–
QSFP-H40G-AOC10M	–	–	–	–	Supported	–	–
QSFP-H40G-AOC15M	–	–	–	–	Supported	–	–
QSFP-H40G-AOC20M	–	–	–	–	Supported	–	–
QSFP-H40G-AOC25M	–	–	–	–	Supported	–	–
QSFP-H40G-AOC30M	–	–	–	–	Supported	–	–
SFP-10G-AOC10M	Supported	Supported	–	–	–	–	Supported
SFP-10G-AOC1M	Supported	Supported	–	Supported	Supported	Supported	Supported
SFP-10G-AOC2M	Supported	Supported	–	Supported	Supported	Supported	Supported
SFP-10G-AOC3M	Supported	Supported	–	Supported	Supported	Supported	Supported
SFP-10G-AOC5M	Supported	Supported	–	Supported	Supported	Supported	Supported
SFP-10G-AOC7M	Supported	Supported	–	Supported	Supported	Supported	Supported
SFP-10G-BXD-I				Supported	Supported	Supported	Supported
SFP-10G-BXU-I				Supported	Supported	Supported	Supported
SFP-10G-CSR-S				Supported	Supported	Supported	–
SFP-10G-ER	Supported	Supported	–	Supported	Supported	Supported	–
SFP-10G-LR	Supported	Supported	Supported	Supported	Supported	Supported	Supported

SFP name	C9800-80-K9	C9800-40-K9	C9800-L-F-K9	CW9800H1	CW9800H2	CW9800M	CW9800L
SFP-10G-LR-I			–	Supported	Supported	Supported	–
SFP-10G-LR-S	Supported	Supported	Supported	Supported	Supported	Supported	Supported
SFP-10G-LR-X	Supported	Supported	Supported	Supported	Supported	Supported	–
SFP-10G-LRM	Supported	Supported	Supported	–	–	–	–
SFP-10G-SR	Supported	Supported	Supported	Supported	Supported	Supported	Supported
SFP-10G-SR-S	Supported	Supported	Supported	Supported	Supported	Supported	Supported
SFP-10G-SR-I	–	–	–	Supported	Supported	Supported	Supported
SFP-10G-SR-X	Supported	Supported	Supported	–	–	–	–
SFP-10G-ZR			–	Supported	Supported	Supported	–
SFP-10G-ZR-I	–	–	–	Supported	Supported	Supported	Supported
SFP-10G-T-X	–	–	–	Supported	Supported	Supported	–
SFP-25G-CSR-S	–	–	–	Supported	Supported	Supported	–
SFP-25G-SR-S	–	–	–	Supported	–	Supported	–
SFP-25G-ER-I	–	–	–	Supported	–	Supported	–
SFP-10/25G-LR-I	–	–	–	Supported	–	Supported	–
SFP-10/25G-LR-S	–	–	–	Supported	–	Supported	–
SFP-10/25G-CSR-S	–	–	–	Supported	–	Supported	–
SFP-10/25G-BXD-I	–	–	–	Supported	–	Supported	Supported
SFP-10/25G-BXU-I	–	–	–	Supported	–	Supported	Supported
SFP-H25G-CU1M	–	–	–	Supported	–	Supported	–
SFP-H25G-CU5M	–	–	–	Supported	–	Supported	–
SFP-25G-AOC1M	–	–	–	Supported	–	Supported	–
SFP-25G-AOC2M	–	–	–	Supported	–	Supported	–
SFP-25G-AOC3M	–	–	–	Supported	–	Supported	–
SFP-25G-AOC5M	–	–	–	Supported	–	Supported	–
SFP-25G-AOC7M	–	–	–	Supported	–	Supported	–
SFP-25G-AOC10M	–	–	–	Supported	–	Supported	–

SFP name	C9800-80-K9	C9800-40-K9	C9800-L-F-K9	CW9800H1	CW9800H2	CW9800M	CW9800L
SFP-H10GB-ACU10M	Supported	Supported	Supported	Supported	Supported	Supported	Supported
SFP-H10GB-ACU7M	Supported	Supported	Supported	Supported	Supported	Supported	Supported
SFP-H10GB-CU1.5M	Supported	Supported	Supported	–	–	–	–
SFP-H10GB-CU1M	Supported	Supported	Supported	Supported	Supported	Supported	–
SFP-H10GB-CU2.5M	Supported	Supported	Supported	–	–	–	Supported
SFP-H10GB-CU2M	Supported	Supported	Supported	Supported	Supported	Supported	–
SFP-H10GB-CU3M	Supported	Supported	Supported	Supported	Supported	Supported	Supported
SFP-H10GB-CU5M	Supported	Supported	Supported	Supported	Supported	Supported	Supported
SFP-H10GB-CU1-5M	Supported	Supported	–	Supported	Supported	Supported	–
SFP-H10GB-CU2-5M				Supported	Supported	Supported	
Finisar-LR (FTLX1471D3BCL)	–	–	Supported	Supported	Supported	Supported	Supported
Finisar-SR (FTLX8574D3BC)	–	–	–	Supported	Supported	Supported	Supported

Optic modules

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

https://www.cisco.com/c/en/us/support/interfaces-modules/transceiver-modules/products-device-support-tables-list.html.

Network protocols and port matrix

Table 13. Cisco Catalyst 9800 series wireless controller - network protocols and port matrix

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

Source	Destination	Protocol	Destination port	Source port	Description
Any	Cisco Catalyst 9800 Series Wireless Controller	TCP	80	Any	HTTP
Any	Cisco Catalyst 9800 Series Wireless Controller	TCP	443	Any	HTTPS
Any	Cisco Catalyst 9800 Series Wireless Controller	UDP	161	Any	SNMP agent
Any	Any	UDP	5353	5353	mDNS
Any	Cisco Catalyst 9800 Series Wireless Controller	UDP	69	69	TFTP
Any	DNS Server	UDP	53	Any	DNS
Any	Cisco Catalyst 9800 Series Wireless Controller	TCP	830	Any	NetConf
Any	Cisco Catalyst 9800 Series Wireless Controller	TCP	443	Any	REST API
Any	WLC Protocol	UDP	1700	Any	Receive CoA packets
AP	Cisco Catalyst 9800 Series Wireless Controller	UDP	5246	Any	CAPWAP Control
AP	Cisco Catalyst 9800 Series Wireless Controller	UDP	5247	Any	CAPWAP Data
AP	Cisco Catalyst 9800 Series Wireless Controller	UDP	5248	Any	CAPWAP MCAST
AP	Cisco Catalyst Center	TCP	32626	Any	Intelligent capture and RF telemetry
AP	AP	UDP	16670	Any	Client Policies (AP-AP)
Cisco Catalyst 9800 Series Wireless Controller	Cisco Catalyst 9800 Series Wireless Controller	UDP	16666	16666	Mobility Control
Cisco Catalyst 9800 Series Wireless Controller	SNMP	UDP	162	Any	SNAMP Trap
Cisco Catalyst 9800 Series Wireless Controller	RADIUS	UDP	1812/1645	Any	RADIUS Auth

Source	Destination	Protocol	Destination port	Source port	Description
Cisco Catalyst 9800 Series Wireless Controller	RADIUS	UDP	1813/1646	Any	RADIUS ACCT
Cisco Catalyst 9800 Series Wireless Controller	TACACS+	TCP	49	Any	TACACS+
Cisco Catalyst 9800 Series Wireless Controller	Cisco Catalyst 9800 Series Wireless Controller	UDP	16667	16667	Mobility
Cisco Catalyst 9800 Series Wireless Controller	NTP Server	UDP	123	Any	NTP
Cisco Catalyst 9800 Series Wireless Controller	Syslog Server	UDP	514	Any	SYSLOG
AP	Cisco Catalyst 9800 Series Wireless Controller	HTTPS	8443	Any	Out of Band AP Image Download Cisco CleanAir Spectral Capture
Cisco Catalyst 9800 Series Wireless Controller	NetFlow Server	UDP	9996	Any	NetFlow
Cisco Catalyst 9800 Series Wireless Controller	Cisco Connected Mobile Experiences (CMX)	UDP	16113	Any	NMSP
Cisco Catalyst Center	Cisco Catalyst 9800 Series Wireless Controller	TCP	32222	Any	Device Discovery
Cisco Catalyst Center	Cisco Catalyst 9800 Series Wireless Controller	TCP	25103	Any	Telemetry Subscriptions

Supported APs

The following Cisco APs are supported in this release:

Table 14. Supported APs

AP type	AP names
Indoor Access Points	• Cisco Catalyst 9105AX (I/W) Access Points

AP type	AP names
	• Cisco Catalyst 9115AX (I/E) Access Points • Cisco Catalyst 9120AX (I/E/P) Access Points • Cisco Catalyst 9130AX (I/E) Access Points • Cisco Catalyst 9136AX Access Points • Cisco Catalyst 9162 (I) Series Access Points • Cisco Catalyst 9164 (I) Series Access Points • Cisco Catalyst 9166 (I/D1) Series Access Points • Cisco Wireless 9171 (I) Series Wi-Fi 7 Access Points • Cisco Wireless 9172 (I/H) Series Wi-Fi 7 Access Points • Cisco Wireless 9174 (I/E) Series Wi-Fi 7 Access Points • Cisco Wireless 9176 (I/D1) Series Wi-Fi 7 Access Points • Cisco Wireless 9178 (I) Series Wi-Fi 7 Access Points • Cisco Wireless 9179 (F) Series Wi-Fi 7 Access Points • Cisco Aironet 1815 (I/W/M/T), 1830 (I), 1840 (I), and 1852 (I/E) Access Points • Cisco Aironet 2800 (I/E) Series Access Points • Cisco Aironet 3800 (I/E/P) Series Access Points • Cisco Aironet 4800 (I) Series Access Points
Outdoor Access Points	• Cisco Aironet 1540 (I/D) Series Access Points • Cisco Aironet 1560 (I/D/E) Series Access Points • Cisco Catalyst Industrial Wireless 6300 Heavy Duty Series Access Point • Cisco 6300 Series Embedded Services Access Point • Cisco Catalyst 9124AX (I/D/E) Access Points • Cisco Catalyst 9163 (E) Series Access Points • Cisco Catalyst Industrial Wireless 9167 (I/E) Heavy Duty Access Points • Cisco Catalyst Industrial Wireless 9165E Rugged Access Point • Cisco Catalyst Industrial Wireless 9165D Heavy Duty Access Point
Integrated Access Points	Integrated Access Point on Cisco 1100 ISR (ISR-AP1100AC-x, ISR-AP1101AC-x, and ISR-AP1101AX-x)
Network Sensor	Cisco Aironet 1800s Active Sensor
Pluggable Modules	Cisco Wi-Fi Interface Module (WIM) - WP-WIFI6-x

Supported AP channels and maximum power settings

Supported access point channels and maximum power settings on Cisco APs are compliant with the regulatory specifications of channels, maximum power levels, and antenna gains of every country in which the access points are sold. For more information about the supported access point transmission values in Cisco IOS XE software releases, refer to the Detailed Channels and Maximum Power Settings document at https://www.cisco.com/c/en/us/support/wireless/catalyst-9100ax-access-points/products-technical-reference-list.html.

For information about Cisco Wireless software releases that support specific Cisco AP modules, refer to Cisco Access Points Supported in Cisco Wireless Controller Platform Software Releases.

Related content

Cisco Wireless Controller:

For more information about the Cisco wireless controller, lightweight APs, and mesh APs, refer to 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:

Data Sheet Listing

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 Spaces:

Cisco Spaces Documentation

Cisco Catalyst Center:

Cisco Catalyst Center Documentation

Product Analytics

Cisco Enterprise Networking Product Analytics Frequently Asked Questions

Communications, services, and additional information:

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions, and services, visit Cisco 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.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a gateway to the Cisco bug-tracking system, which maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. The BST provides you with detailed defect information about your products and software.

Documentation feedback

To provide feedback about Cisco technical documentation, use the feedback form available on the right pane of every online document.

Legal information