Release Notes for Cisco Catalyst 9800 Series Wireless Controller, Cisco IOS XE 26.2.x

Cisco Catalyst 9800 Series Wireless Controller, Cisco IOS XE 26.2.x

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 26.2.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 26.2.1

Product impact	Feature	Description
Software Reliability	Cisco Live Protect Vulnerability Shields	Live Protect validates vulnerability shields that protect Cisco products without requiring device reloads or service interruptions. You can deploy security shields in two modes: • Monitoring mode: Provides visibility into potential exploit attempts without enforcement, allowing you to assess threats before taking action. • Enforce (Protecting) mode: Actively applies mitigation policies to reduce exposure to known vulnerabilities. Live Protect allows you to monitor, enforce, disable, and retire the vulnerability shields enabling a smooth transition to remediation. This capability helps businesses maintain continuous operations while managing risks until the software upgrades or patches are deployed.
	Sensor Connect Backup and Restore	This release introduces Backup and Restore for the Sensor Connect application database, preserving configuration and operational data not included in the controller configuration backup. The capability enables Sensor Connect to be restored to its saved Day-N state after controller replacement or application redeployment.
	AP and Sensor Connect Support for Full Filtering	This release enables Cisco Wireless APs to filter BLE advertisements before forwarding them to Sensor Connect and Cisco Spaces, reducing unnecessary traffic in dense Bluetooth environments. Advertisements can be filtered by Bluetooth MAC address type, RSSI threshold, and MAC address prefix using deny, static allow, dynamic allow, and limit lists.
	IPv6 Layer 3 Access	This release introduces controller-based IPv6 Layer 3 access, enabling the controller to terminate wireless client IPv6 subnets on switched virtual interfaces and advertise client routes through OSPFv3. It also provides VRF-aware services, including DHCPv6 relay, IPv6 multicast routing, NAT64, and flow-based ECMP forwarding.

	Enhanced BLE performance on Cisco Wireless APs	Cisco Spaces Connector IoT Service: Controllers running Cisco IOS XE Wireless release 26.2.1 and later support the Cisco Spaces Connector IoT Service solution only with Cisco Spaces Connector 3.3 or later and IOx App 2.1.x or later. Before upgrading the controller to release 26.2.1 or later, upgrade the Cisco Spaces Connector to release 3.3 or later and the IOx App to the latest 2.1.x release in Cisco Spaces.
	NDcPPv4.0 updates for Common Criteria Certification	To support NDcPP v4.0 Common Criteria certification, the HTTPS Web GUI now defaults ECDHE key establishment to the stronger **secp384r1** curve. The update aligns secure HTTP behavior with modern TLS requirements and applies consistently across CLI and YANG configuration interfaces.
	Post-Quantum Cryptography Support for the Web Server	Many applications and services still rely on TLS 1.2 or earlier, which lack the extensibility needed to negotiate post-quantum cryptography (PQC) cipher suites. Retrofitting these legacy versions is impractical, leaving applications that depend on them exposed to “harvest now, decrypt later” attacks. The migration to TLS 1.3 enables support for PQC algorithms such as ML-KEM.
	RMI Support for Syslog Source Interfaces	Syslog now supports the Redundancy Management Interface (RMI) as a logging source on wireless controllers. When RMI is selected, syslog uses the RMI IP address and automatically resets existing connections when the RMI configuration changes or is removed. Existing management-IP and source-interface behavior remains unchanged. The enhancement supports IPv4 and IPv6 on both active and standby controllers.
	High Availability support for CTS IP-SGT Bindings	Cisco TrustSec now synchronizes IP-SGT bindings from the active device to the standby device, including bindings learned through SXP, VLAN, LISP, OMP, and Layer 3 interfaces. Incremental and bulk synchronization preserve binding information during a Stateful Switchover, reducing relearning delays and maintaining consistent SGACL enforcement. The enhancement supports SXP version 5, IPv4 and IPv6 connections, VRFs, and stacked, SVL, and chassis deployments.
	AP Certificate Renewal Without an AP Reload	From Cisco IOS XE 26.2.1 onwards, supported Cisco Catalyst access points can apply renewed Locally Significant Certificates without a complete AP reload. This enhancement reduces service disruption during certificate renewal through Cisco Catalyst 9800 Series Wireless Controllers or Cisco Catalyst Center. This release also includes the ability to enable or disable LSC provisioning.
	Cryptographic Enhancements for Cisco aWIPS	From Cisco IOS XE 26.2.1 onwards, Cisco Advanced Wireless Intrusion Prevention System (aWIPS) includes updated cryptographic processing for secure profile exchange between Cisco Catalyst Center and Cisco Catalyst 9800 Series Wireless Controllers.
	6 GHz LPI Support for Korea	From this release, supported IW9165E APs can operate as URWB mobility clients in Korea’s 6-GHz Low Power Indoor domain, providing indoor connectivity across the U-NII-5 through U-NII-8 bands.
	Support for 802.1x Authentication on Ethernet Port for Controller Managed URWB Vehicle AP	This feature enables 802.1X authentication of wired clients connected to Vehicle APs operating as mobility clients. It validates RADIUS-based access control and EAP message forwarding through the URWB network. Supported methods include EAP-PEAP, EAP-TLS, and EAP-FAST. MAB is not supported, and the release supports one wired client per LAN port with up to two RADIUS servers per Vehicle AP.

	802.1X Authentication for Wired Clients	This feature enables 802.1X authentication for wired clients connected through a Workgroup Bridge (WGB), enforcing controlled network access through a configured RADIUS server. It ensures proper forwarding of EAP packets through the WGB wired0 and wired1 ports and supports multiple clients through a compatible switch or hub.
	WPA3-Enterprise and SCEP Certificate Renewal Support	This feature enables WPA3-Enterprise security on Industrial Wireless devices operating in Workgroup Bridge (WGB) mode, providing robust encryption and enterprise authentication for wireless connections. It supports EAP-TLS, PEAP, and EAP-FAST authentication and meets WPA3 requirements for the 6 GHz radio band, including mandatory Protected Management Frames (PMF). Simple Certificate Enrollment Protocol (SCEP) support automates digital certificate renewal for EAP-TLS deployments, simplifying certificate lifecycle management and reducing manual effort.
	802.11v Support for 6 GHz WGB	Enables 802.11v support on the WGB to optimize roaming performance by restricting channel scanning to those learned from the neighbor list.
	Software Model Version in the gRPC Header	The gRPC dialout message header dynamically determines the Cisco IOS XE software version running on the device, and based on this software version, the telemetry receiver selects the YANG model version.
	Resilient Infrastructure Changes	As part of Cisco's Resilient Infrastructure program and Cisco's commitment to secure infrastructure, this release includes additional changes aimed towards continuing to make Cisco IOS XE more secure by default. Note that some of these changes may require operational changes if you are not following secure best practices. This release includes these changes: • The RADIUS client appends the Message-Authenticator attribute (Attribute 80 HMAC-MD5) to all outgoing Access-Request packets to mitigate cryptographic forgery and Blast-RADIUS vulnerabilities (CVE-2024-3596). • The RADIUS client drops incoming Access-Accept, Access-Reject, and Access-Challenge packets if the Message-Authenticator packet is absent or invalid. Ensure AAA servers (example, Cisco ISE) are configured to return Attribute 80. • Outbound SSH connections enforce Trust-On-First-Use (TOFU). The device prompts to verify and store remote server host keys in the known-hosts database on first connection and validates against them on subsequent sessions. • The embedded web server daemon is disabled by default on factory configurations to restrict unauthenticated management access. Web UI and RESTCONF require explicit enablement of the ip http secure-server command. • The IOS XE device rejects unauthenticated NTP Mode 6 and Mode 7 control queries (monlist) to prevent NTP reflection and amplification DDoS attacks. Standard time synchronization (Modes 3 and 4) is unaffected. • System logging timestamps automatically include the four-digit calendar year (service timestamps log datetime msec year) to standardize multi-year audit logs and SIEM compliance. • Warning messages are emitted on the console and logged to syslog whenever legacy insecure protocols (Telnet, FTP, TFTP, HTTP) are enabled in the configuration. • Real-time tracking of active insecure services is published to the operational database (operDB) and YANG data models, allowing management controllers (such as Cisco Catalyst Center) to monitor security compliance.
Ease of Setup	Wireless Active Testing SCEP Support	This release adds SCEP-based certificate provisioning for Wireless Active Testing EAP-TLS SSIDs. Integration with customer SCEP servers enables automatic enrollment and renewal of client certificates, eliminating the need for manual certificate provisioning.

	Expanded SFP Module Support for Cisco Catalyst 9800 Series Wireless Controllers	This release expands SFP support across CW9800M, CW9800H1, and CW9800H2 controllers. The update adds support for the SFP-10G-T-X that delivers 10 Gigabit Ethernet connectivity over standard copper network cables, providing customers with greater deployment flexibility and broader hardware compatibility.
	Auto MACsec for Wireless Access Points	This release introduces Auto MACsec, which automatically discovers compatible access switches through LLDP, authenticates access points using a hardware-backed identity, and establishes MACsec encryption before the AP joins the wireless controller. The feature reduces per-port configuration while protecting wired uplink traffic from interception and man-in-the-middle attacks. Auto MACsec is enabled by default and can be managed through the AP join profile using the GUI or CLI. Auto MACsec peer detection is supported on Wi-Fi 7 APs equipped with MACsec-capable physical layer (PHY) interfaces.
	6 GHz Country Support	From Cisco IOS XE 26.2.1 onwards, 6 GHz radio support on supported Wi-Fi 6E and Wi-Fi 7 APs is added for Bosnia and Herzegovina (BA), North Macedonia (MK), Montenegro (ME), Ukraine (UA), Andorra (AD), Gibraltar (GI), Georgia (GE), El Salvador (SV), Isle of Man (IM), Moldova (MD), Namibia (NA), Paraguay (PY), and Togo (TG). This release also updates 5 GHz channel availability on supported Wi-Fi 7 access points. Support is added for Andorra, channels 149–165 are added for Bahrain, channels 36–165 are added for Togo, and channels 36–132 are added for Ukraine. For more information, refer to Cisco CW917x Wi-Fi 7 Access Point Country Codes and Phases.
	Regulatory Updates for Kuwait, Bahrain, and Ukraine	From Cisco IOS XE 26.2.1 onwards, regulatory settings for supported Wi-Fi 6E and Wi-Fi 7 access points are updated for Kuwait, Bahrain, and Ukraine. In Kuwait, the maximum transmit power for the UNII-2C band is reduced from 30 dBm to 27 dBm. In Bahrain, the maximum transmit power for the UNII-3 band is limited to 23 dBm. In Ukraine, support is added for the UNII-1 and UNII-2 bands. These updates align access-point operation with the applicable regulatory requirements in each country. For more information, refer to Cisco CW917x Wi-Fi 7 Access Point Country Codes and Phases.
	UNII-2C Channel Support for Outdoor Access Points in Mexico	From Cisco IOS XE 26.2.1 onwards, UNII-2C channels in the 5 GHz band are supported for outdoor deployments in Mexico on Cisco Catalyst 9124AXI, 9124AXD, and 9124AXE access points, Cisco Catalyst Wireless 9163E access points, and Cisco Wireless CW9179F access points operating with the outdoor configuration. This enhancement expands the 5 GHz channel availability for supported outdoor access points while maintaining compliance with Mexico's regulatory requirements. For detailed channel and maximum-power information, refer to the applicable Detailed Channels and Maximum Power Settings document. For CW9179F availability, refer to Cisco CW917x Wi-Fi 7 Access Point Country Codes and Phases.

	Support for Ethernet Encapsulation in CAPWAP Data Tunnels	From Cisco IOS XE 26.2.1 onwards, supported Cisco Wi-Fi 6, Wi-Fi 6E, and Wi-Fi 7 access points use Ethernet encapsulation for client traffic transported through CAPWAP data tunnels. Instead of carrying client data using an 802.11 frame header, the access point and controller transport the traffic using an 802.3 Ethernet frame with 802.1Q encapsulation. The access point advertises its capability when it joins the controller, allowing the controller to select the appropriate encapsulation automatically. No additional configuration is required. Existing wireless-specific information, including RSSI and SNR data, continues to be carried in the CAPWAP header. During an ISSU, the controller supports a combination of access points using the existing and new encapsulation formats, enabling continued client traffic while access points are upgraded in stages.
	Certificate Renewal Support for Secure AP Onboarding	From Cisco IOS XE 26.2.1 onwards, supported Cisco Wireless APs can receive and apply renewed certificates through the Cisco Catalyst Center secure AP onboarding workflow. This enhancement helps maintain certificate-based AP authentication by allowing certificates to be renewed before expiration.
	Controller-directed URWB Traffic Support	This feature centralizes forwarding and traffic egress at the controller, enabling vehicle APs and their wired clients to maintain seamless connectivity while roaming across infrastructure subnets.
	Network Address Translation on URWB	This feature enables multiple services on URWB mobile-unit networks to be accessed through a single external IP address using distinct TCP or UDP port mappings configured in the URWB network profile.
Ease of Use	Extended GUI Session Idle Timeout Configuration	This enhancement extends the configurable GUI idle-timeout beyond the current 20-minute maximum while keeping the default timeout unchanged. Customers can set longer timeouts—at least two hours—through CLI or YANG, preventing disruptive logouts during troubleshooting and other long-running activities while retaining control over their security posture.
	Secondary Ethernet Port Support (URWB)	This feature enables two wired interfaces in URWB deployments, allowing the primary and secondary Ethernet ports to be managed independently. It supports wired client connectivity, daisy-chaining, and mesh ring deployments without requiring external switches, improving deployment flexibility and cost efficiency. On supported Cisco Catalyst 9124AX Series access points, the secondary Ethernet port can also provide optional PoE-out to power downstream devices.
	Multi-Controller Topology Awareness	This feature provides all controllers in a mobility group with visibility into URWB telemetry across the entire group. It synchronizes topology information between peer controllers, ensuring a consistent network state and a unified view of URWB nodes and links. This capability simplifies network monitoring and troubleshooting when a URWB network spans multiple controllers.
API Experience	IOx Enablement	IOx adds secure, Docker-based application hosting to the IW9165E, enabling custom applications, analytics, and third-party software to run locally at the network edge.
Operational Efficiency	Power Saving Modes	Mapped digital I/O interfaces and IOx applications enable external control systems to place the IW9165E in light-sleep mode and restore it to active operation, reducing power consumption while retaining URWB backhaul connectivity.

Industrial Wireless Connectivity	URWB Support on CW9177I/D/E	URWB is now supported on all the CW9177 variants, such as CW9177I, CW9177D, and CW9177E.
	Enable GPIO on IW9165E APs	This feature exposes GPIO pins as /dev/dio-x character devices to IOx, allowing applications to monitor digital inputs, control external hardware signals, and manage LED indicators.

New hardware features

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

Table 2. New hardware features for Cisco Catalyst 9800 Series Wireless Controllers, Release 26.2.1

Feature	Description
Support for Cisco Wireless 9177I, 9177D, and 9177E Wi-Fi 7 Access Points	From Cisco IOS XE 26.2.1 onwards, the following Cisco Wireless 9177 Series Wi-Fi 7 access points are supported: • Cisco Wireless 9177I Series Wi-Fi 7 Access Point (CW9177I) • Cisco Wireless 9177D Series Wi-Fi 7 Access Point (CW9177D) • Cisco Wireless 9177E Series Wi-Fi 7 Access Point (CW9177E) The CW9177I, CW9177D, and CW9177E are tri-band access points that operate in the 2.4-GHz, 5-GHz, and 6-GHz bands. These access points interoperate with 802.11be, 802.11ax, and legacy clients and can be deployed alongside other access points and controllers in hybrid deployments. For a complete list of features and specifications, see the Cisco Wireless 9177 Series Wi-Fi 7 Access Point Data Sheet. *Note: For information about the countries in which these access points are supported, see the Cisco Wireless Compliance Tool.*
Support for CW-ANT-T-D4-N, CW-ANT-T-O3-N, and CW-ANT-T-D3-N Antennas	From Cisco IOS XE 26.2.1 onwards, the CW-ANT-T-D4-N, CW-ANT-T-O3-N, and CW-ANT-T-D3-N antennas are supported on the Cisco Wireless 9177E Wi-Fi 7 Access Point. For antenna features and specifications, see the Cisco Wireless 9177 Series Wi-Fi 7 Access Point Data Sheet.

MIBs

The following MIBs have been modified:

- AIRESPACE-WIRELESS-MIB.my
- CISCO-LWAPP-DOT11-CLIENT-MIB.my
- CISCO-LWAPP-DOT11-MIB.my
- CISCO-LWAPP-QOS-MIB.my
- CISCO-LWAPP-RF-MIB.my
- CISCO-LWAPP-RRM-MIB.my
- CISCO-WIRELESS-HOTSPOT-MIB.my

Changes in behavior

This section provides a brief description of the behavior changes introduced in this release.

Table 3. Behavior changes for Cisco Catalyst 9800 Series Wireless Controllers, Release 26.2.1

Description	Behavior changes
Updated Mesh PSK downgrade procedure	MAP is unable to connect if authentication method is PSK, during the downgrade process from Cisco IOS XE 26.2 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.
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.
YANG channel-width configuration fails with **band-default**	YANG-based configuration fails when the channel-width range of a 5 GHz or 6 GHz RF profile uses **band-default** for either the minimum or maximum value while the other limit is explicitly configured. Examples include: • 5 GHz: minimum **band-default**, maximum 80 MHz • 6 GHz: minimum **band-default**, maximum 160 MHz With the change in behavior, the YANG configuration now accepts band-default as either the minimum or maximum channel-width value when the other limit is explicitly configured with a valid value. This behavior is supported by both default and custom RF profiles in the 5-GHz and 6-GHz bands.

Add GCMP-256 support for WPA3-Enterprise non-192-bit mode	WPA3 specification version 3.4 requires GCMP-256 support with 802.1X-SHA256 (AKM 5) and FT-802.1X (AKM 3) to enable MLO and EHT for Wi-Fi 7 WLANs. Currently, these AKMs support only CCMP-128 because configuration validation blocks GCMP-256, preventing compatible Wi-Fi 7 clients from associating. With the change of behavior, GCMP-256 can now be configured with AKM 3 and AKM 5 in WPA3-Enterprise non-192-bit mode, either as the only cipher or together with CCMP-128. This enables MLO/EHT-capable Wi-Fi 7 clients to associate in accordance with WPA3 specification.
Update client details after an AP radio channel change	When an AP radio's channel is changed while a wireless client remains associated, the **show wireless client mac <MAC> detail** command on the controller continues to display the previous channel. The AP correctly operates on the new channel, but the client details are updated only after the AP state is toggled. The controller now updates the client's channel information when the associated AP radio changes channels. The show wireless client mac <MAC> detail command displays the current channel without requiring an AP state toggle.
NETCONF/YANG support for Regulatory Activation File (RAF)	In the earlier releases, you could activate regulatory domain on APs through CLI commands and through the GUI process ensuring compliance with regional regulations. With the change in behavior, NETCONF/YANG now supports Regulatory Activation File (RAF). The YANG paths are: • Cisco-IOS-XE-wireless-raf-cfg-rpc/apply-raf-config • Cisco-IOS-XE-wireless-raf-cfg-rpc/clear-country-ap-map • Cisco-IOS-XE-wireless-raf-cfg-rpc/clear-country-map-all-ap RPC-YANG support is added for the following RAF EXEC CLIs and **show** commands: • **ap regulatory activation file** *file-name* • **ap regulatory activation apply** • **ap regulatory activation clear all** • **ap regulatory activation clear** *mac-address* • **clear ap name** *ap-name* **country** • **show ap regulatory activation all** • **show ap regulatory activation mac** *mac-address*
Validate channel availability before enabling dual 5 GHz radios	The controller previously allowed XOR 5/6 GHz radio to be changed to the 5 GHz band without verifying that the configured country supports enough channels for dual 5 GHz operation. This could result in an invalid configuration on band-locked radios and APs requiring 100-MHz separation between radio channels. The controller now checks the country-specific 5 GHz channel availability before changing an XOR 5/6 GHz radio to 5 GHz. If the required lower and upper-band channels are unavailable, the command is rejected, preventing unsupported dual 5 GHz operation.
Display consistent URWB and power data in AP statistics	In the WebUI, the **General** tab under **Monitoring** > **Wireless > AP Statistics** does not consistently display data in the URWB and Power sections, resulting in incomplete or unreliable AP statistics. The **General** tab now consistently retrieves and displays URWB and Power information for the selected AP.

Resolved issues

This table lists the resolved issues in this specific software release.

Note: This software release may contain bug fixes first introduced in other releases. To see additional information, click the bug ID to access the Cisco Bug Search Tool.

Table 4. Resolved issues for Cisco Catalyst 9800 Series Wireless Controllers, Release 26.2.1

Bug ID	Description
CSCww11377	Refresh of Topology not happening post removal of any mesh-point from CURWB topology
CSCwt36615	Non-English Characters in CLI breaks the spacing
CSCwt09514	MAP is unable to connect if authentication method is PSK - AP
CSCwv47563	Flex mode APs loses auth token and fails to come up on controller when moving across 9800-CL running on different versions
CSCwr07706	C9120 txerr noticed followed by Dot11BaseDriver Recover for cause : 48 - Toggling radio
CSCwr81031	Memory leak on 9176 APs on kmalloc slabs
CSCws27309	CW9162I-ROW APs are disjoining from 9800-CL running 17.12.04 - SMU-PATCHED
CSCws32577	9130 RAP, systemd[1]: capwapd.service watchdog timeout (limit 1min 30s)! , continuously reloading and not joining to wlc
CSCws66689	When RLAN port 1 is connected 9172H sends DHCP discover out of wired1 instead of wired0
CSCws67290	Radio crash corrupted coredump is seen on AP CW9174I
CSCws68479	Missing support for certain bands and channels in wifi6/6e regdb
CSCws68505	AP crash due to kernel panic
CSCws68847	OOM crash observed after overnight run
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
CSCws83579	Radio Firmware crash seen while performing uplink
CSCws87617	9130 not able to upgrade to 17.18.2 CCO image due to another upgrade is still in progress
CSCws93044	AP does not transmit beacons for over one second right after the client connects
CSCwt01278	9115/9120 APs facing kernel panic crashes in 17.18.2

CSCwt02580	9172H/9179: Kernel panic seen at reg_get_sp_eirp
CSCwt05272	AP 9120 crashed due to Kernal Panic
CSCwt08175	AP Kernel Panic due to Use-After-Free Race Condition in SPSCPriorityQueue::push()
CSCwt18007	Pre-commit CDT failure | 9120 AP crash _ZN15IsCapwapEnabled4pushEiP6Packet+0x3c/0x130
CSCwt19011	9166 17.15.4b AP in SDA mode not forwarding IPv4 ARP upstream or other IPv4 packets after DHCP
CSCwt19117	Dot11u config is removed from AP so AP stops beaconing with dot11u impacting OpenRoaming
CSCwt19490	9800 WLC: 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
CSCwt24610	gaps in panic log - /dev/kmsg tail is not reflecting correctly in panic log
CSCwt26500	Need changes for CSCwq11842 to work in all AP models
CSCwt33908	PHY OFF error assert causing AP crash during longevity tests
CSCwt50389	Ascom Myco2 phones are not able to connect to 9176 APs due to EAP_ID_REQ or M2 not acked by AP
CSCwt64349	observing kfence calltrace on multiple AP models
CSCwt65349	CW9172I AP crashes with ar_wal_mlo_ipc.c assert and watchdog panic
CSCwt72800	CW9176I AP crash due to kernel panic with pc do_undefinstr+0x30/0x50
CSCwt74576	Cisco Catalyst 9136 AP wcpd process memory increasing gradually
CSCwt78829	Memory Leak in python Process on Wireless Active Testing (WAT) AP with TEAgent IOx Application
CSCwt80663	Tier E countries + RAF not working
CSCwt83641	CW9172 AP radio forwarding failure in upstream path
CSCwt88263	Pre-commit CDT failure-12 | AP crash kmem_cache_free+0x150/0x2c8
CSCwt92054	9176 not processing CTS packets when configured with datarate 36M and channel width 40M or higher
CSCwu04935	9178: AP continuously reloading with \" NSS CAPWAP tunnel creation failed\" log when vlan-tag is enabled
CSCwu08256	AP unable to join back to the controller after dropping from the controller
CSCwu13170	9176 AP has Kernel panic, pc: find_busiest_group
CSCwu14554	9105/9172H RLAN AP not passing multicast traffic for central switching

CSCwu18918	AP not completing DHCPv6 after dropping from the controller
CSCwu20280	9176 AP crashing due to kernel panic at wlan_sm_dispatch+0xb8/0x208 [umac]
CSCwu27163	9120 and 9130 APs see WhereCall V RFID it's configured for 5.5M rate but they don't transmit packet to WLC, while 2800 does
CSCwu42085	9120 kernel panic crash at wlc_twt_scb_get_schedid+0x34/0x170 [wl] & txq_hw_fill+0x8c8/0xff8 [wl]
CSCwu52744	C9120 COS AP crash PC is at phy_ac_noise_lte_avg LR is at phy_noise_lte_avg
CSCwu52745	C9120 COS AP crash PC is at sysfs_remove_bin_file LR is at lp55xx_unregister_sysfs
CSCwu66197	C9130AXI AP crashed due to Kernel panic after upgrading to 17.15.5.201(APSP 1)
CSCwu66664	AP 9136 crashes generating capwapd core
CSCwu84328	Client connectivity issues on 9176 AP due to scheduler stuck
CSCwu96123	9120 AP reload due to Radio firmware beacon TX stuck
CSCwv08841	Client connectivity issues on AP due to scheduler stuck
CSCwv11776	COS AP as WGB wired client unable to pass traffic randomly
CSCwv17189	Possible kernel slab leak in 17.15.4bESW1 EWC RAP
CSCwv30224	CW9172I running 17.18.3.18 crashes in RRMReceive::process_rx_frame_from_driver
CSCwv36063	Wifi6E and Wifi7 APs disconnecting all clients in 6ghz when bss-color change occur even if globally disable
CSCwv44721	Image upgrade failure: opkg_verify cost long time causing capwapd watchdog timeout.
CSCwv45612	9120 crashing due to kernel panic with PC at __delay in 17.18.2
CSCwv52872	AP may get stuck on boot when console is connected to unterminated cable (minimal fix)
CSCwv52931	When EWC AP in mesh mode (with PSK provisioning) is factory reset, the RAP must be reloaded in order for existing MAPs to join
CSCwr00948	Access points connected to 9xxx PoE ports cannot negotiate full power after switch power outage
CSCwr97166	Regdb update to fix all issues caught using new scripts
CSCws35315	Auxiliary-client interface taking over the CAPWAP connection from the AP
CSCws47852	AP intermittently joins WLC but WLC fails to get AP type resulting AP being rejected
CSCws70285	Clean up for /storage/cnssdaemon.log
CSCws72425	9136I IOX application activation failure

CSCws79118	Unexpectedly reduced transmit power for 9124-AXE on 2.4 GHz in -Z regulatory domain
CSCws93536	Panic log missed from AP crashfile when minidump is enabled
CSCwt13894	CW9172H WAT Agent fails to connect to SSIDs with leading or trailing spaces
CSCwt43633	C9166/C9176 AP Bad Intf: Dropped Corrupted Interferer Stream message continuously noticed on AP console
CSCwt47537	Kernel: BUG: KFENCE: memory corruption in | use-after-free write in | use-after-free read in. In ap version 17.12.6.28
CSCwt49364	ThousandEyes Endpoint Agent upgrade leads to duplicated agent in Active Testing AP
CSCwt51709	COS APs initiate DHCP process even when static IP is configured, causing intermittent DHCP Fallback issues
CSCwt68617	FT-SAE in Flex Standalone mode does not allow client association
CSCwt71378	Multiple APs hit bootloader failure after repeated reset testing
CSCwt77092	AP - KFENCE memory corruption events lead to RCU stalls and HW watchdog reset
CSCwt77136	continuous KFENCE IPv6 MLD memory corruption leads to RCU stalls and HW watchdog reset
CSCwt88383	9172I AP is crashing with pc : dp_rx_mon_process_2_0+0x26c0/0x28c0 [monitor]
CSCwt99080	CleanAir Spectrum AP Type Invalid
CSCwu17010	9120 AP forwards HE PHY Capability bitset with 40 / 80 MHz supported when configured 20 MHz only channel width
CSCwu17364	DHCP for Personal SSID on OEAP enabled after AP reboot.
CSCwu35228	9136 APs sending Accounting packet to AAA server when local-accounting is disabled
CSCwu52776	C9120 COS AP crash due to: RHL Probe failure, reboot to recover
CSCwu54425	C9120 COS AP crash PC is at _ZN7Element19read_cycles_handlerEPS_Pv
CSCwu65418	17.15.5 Catalyst 9176 5Ghz high retry rate
CSCwu70466	9136 APs sends interim accounting packet in Central auth/accounting configs
CSCwu88097	FIPS mode: AP is still offering SHA1 algorithms
CSCwu94430	C9800: bytes_rx/bytes_tx in client traffic statistics is incrementing by ~2^32 periodically
CSCwu98499	9105AW WGB mode, ports 1/2/3 do not go up in 17.15/17.18
CSCwv20470	Clients obtain an IP address from the VLAN mapped under the Policy Profile instead of the VLAN assigned by AAA Override.Flex local-auth roam
CSCwv40607	WAT reports wrong DNS IPs from previous connections in ThousandEyes

CSCwv58521	APs advertise invalid Maximum Transmit Power (-99 dBm) in 5 GHz Country Information IE when configured with Bolivia (BO) country code
CSCww06803	AP kernel crash in ieee80211_session_timeout_iter_cb() due to stale node reference
CSCww07021	AwipsRadioEncap can access released packet memory during header expansion
CSCwt39252	17155 - Client loses connectivity during ISSU upgrade form 17.12.4ESW15 to 17.15.5
CSCwq66623	SJC Alpha - 17.18.2 alpha APs not joining controller- stuck in DTLS
CSCwr20303	Controller unexpected reload after modifying ap location name config due to stale oid for AP
CSCwr65627	Large number of APs (2K+) take several minutes to join N+1 WLC when Primary goes down
CSCwr67652	wlc mem is noticed due to wsa_db
CSCwr90981	AP count varying in 5GHz radio
CSCws16148	WLC Crash after issuing the command \" ap geolocation ranging accurate method uwb\"
CSCws18528	[APCI] MLO Rogue Containment for all bands is not working
CSCws23072	RRM Crashes and tracebacks observed on CW9800 Platform
CSCws38733	ap ranging CLI triggers a WLC switchover and core file is created
CSCws39889	RF Based AP Load Balancing: WLC Crash due to observed during load balancing algo run
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 due to mac_theft
CSCws58494	WebAuth Clients moved to RUN State on the WLC 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)
CSCws68160	WLC Unexpected reload with Critical process wncd fault on rp_0_0 (rc=139) after client deletion due to continuous IP Theft
CSCws68876	Unexpected reload due to ISSU client ISSU Virtual-Template Client
CSCws76688	Client stuck in AUTHENTICATING state on Catalyst 9800 when OKC is enabled in Flex mode AP \u2013 EAP Identity Request sent after 4\u2011Way Handshake
CSCws91899	C9800 Crash while processing Flex Connect Client

CSCws93542	Post failover DHCP Offer is not forwarded by the WLC to the client
CSCwt07093	APs not being able to connect due capwap messages being queued due to fragments drop
CSCwt09034	DTLS Alert Message processing and Open SSL Decryption on C9800-CL leads to watchdog crash in WNCD
CSCwt13732	WNCD process terminated causing WLC to crash. Critical process wncd has failed (rc 0)) triggerd wired WGB client
CSCwt22893	WLC unexpected SISF reboot with WNCD core on 17.18.2
CSCwt26121	APMGR - Code Scan fixes for APMGR
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 wlc may reload
CSCwt38788	The mobility process ends unexpectedly due to an uninitialized variable; wlc may be reloaded.
CSCwt52617	Post SSO - Few wireless clients experiences loss of connectivity to devices outside the Fabric
CSCwt52815	WLC fails to update associated Channel width for client after it is changed on AP radio.
CSCwt87508	During Capture Enable Device Experienced an Unexpected Reload
CSCwt91818	C9800 WLC crash during APSP installation due to stale old APSP entry not correctly removed
CSCwt98619	CW9800L PID is missing in ISSU comp_matrix file
CSCwu00043	17.18.3: LSC certificate failure \" CRYPTO_PKI: Failed to add ca req pool entry 538\" in scale environment
CSCwu08974	C9800 wncd crashes on ARP probe debug log
CSCwu52200	C9800 Unexpected Reload After a wired guest client joins that previously joined as wireless
CSCwu77375	RRM DCA is not happening with AP9167EH slot1 configured as backhaul and slot2 as client serving
CSCwu92389	RMI link flaps logs on WLC but no switchover happens
CSCwv33315	wncd crash (SIGABRT) - heap buffer overflow in CAPWAP TX completion path
CSCwv33856	WLC experiences a WNCD process leak due to country code resolution failure
CSCwv40125	26.2.1eft11 AP recovery failure and WNCD Crash during HA switchover
CSCwv41569	SSID Broadcast Failure with Overnight Calendar Profile Schedule

CSCwv77065	WLC9800 ACR full-replace fails for AP filter priority mapping changes due to intermediate-state validation
CSCwq81507	Extend the timeout for IoT_Orchestrator delete operation
CSCwr30777	9800 standby chassis shows Cisco Unknown Power Supply and same SN on output from \" show inventory\" 17.12.4
CSCwr74373	C9800 WLC 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 correclty 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
CSCws17199	Add GCMP256 support in WPA3 enterprise(non-192-bit)
CSCws17518	Unexpected reload after running a command on a WLC
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	WLC 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
CSCws31123	Client deleted after CoA reauth with URL redirect
CSCws31873	Media-Stream and Multicast traffic fails after SSO when GTK key-rotation is enabled
CSCws46519	When running \" show ap lldp neighbor\" on the WLC, 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
CSCws80754	Local DHCP on Anchor WLC intermittently stops forwarding DHCP OFFER or ACK
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
CSCwt08276	RF Based AP Load Balancing: Algorithm issues could cluster scattered APs
CSCwt20158	bsnMobileStation showing only a few clients - root cause is Wifi7
CSCwt21195	Default 6 GHz RF profile cannot be selected when creating a new location.
CSCwt25978	Wireless bundle client does not work with site tag space in name
CSCwt40423	Cloudm Tracebacks running out of ID
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
CSCwt43333	XPath configuration failure for APs(9120/9166) in sniffer mode and for 9120 when radio role is sniffer
CSCwt58885	'debug wireless bundle client start ap-archive site-tag \" my site\" level critical monitor-time 60' does not work when the site tag name contains spaces
CSCwt61816	Monitoring > Wireless Clients shows an incorrectly large client count
CSCwt72694	Catalyst Center Sending Invalid/Legacy License Activation Command Syntax - C9500-40X
CSCwt84933	Channels 100-140 are available for Nigeria, but they are licensed spectrum
CSCwt87345	9800 clear wireless device-tracking counters vlan < vlanid > not working
CSCwt95088	No Duty Cycle present in Persistent device output
CSCwt98260	NameServer Configuration mandatory for AWIPS even if URL points to an IP address instead of FQDN
CSCwu20316	9800 showing dot1x pmf client deauth as CLIENT_DELETE_REASON_CLIENT_EAP_TIMEOUT_FAILURE
CSCwu32896	LWA Controller not sending redirection HTTP 200 for FlexConnect APs due to client ip address not learned for webauth
CSCwu42825	Wifi7 syslogs are generating in WLC in large numbers
CSCwu71312	17.18 : Support -A, -B domain support for Honduras indoor
CSCwu76364	CLUS26 - Client Telemetry status is Fair
CSCwu86004	9800 deauthenticates client when receiving DHCP RELEASE from client.
CSCwv31549	Incorrect Client Exclusion reasons on bsnStationBlacklistingReasonCode traps
CSCwv38974	9800 crash due to unexpected values in 6ghz channel power payload

Open issues

This table lists the open issues in this specific software release.

Note: This software release may contain open bugs first identified in other releases. To see additional information, click the bug ID to access the Cisco Bug Search Tool.

Table 5. Open issues for Cisco Catalyst 9800 Series Wireless Controllers, Release 26.2.1

Bug ID	Description
CSCwv09937	URWB: issue with Wi-Fi-client connectivity when mobile primary unit is restored after failover
CSCww25465	Topology Awareness: Coordinator dropdown fails to list coordinators with network names after Coordinator/Node AP moves between WLCs in the same mobility group
CSCwu65611	DHCP Offer Received by C9800 but Not Forwarded to AP/Client on VLAN 155 Resulting in Intermittent DHCP Failures
CSCwu92593	AP 9176I IPV6 RA packet drop using SLAAC
CSCwv27458	AP crashed due to kernel panic with different PC and LR
CSCwv40579	CW9176I AP crash due to kernel panic
CSCwv47361	AP CW9166 in fabric deployment does not send upstream mDNS queries/responses after upgrade to 17.15.5
CSCwv53150	9166 dropping upstream dot11ax QoS data packets after bss-color change causing client disassoc
CSCwv53177	9120 running 17.18.3 crashing due to _ZNK6String5derefEv
CSCwv71535	9176 in flex mode doesn't forward ipv6 RA for stateful DHCPv6 downstream client
CSCwv84099	OOB predownload fails with Unknown Error From Server
CSCwv85898	Controller mobility tunnel drops randomly on 17.12.6a.
CSCwv90808	9120 channel mismatch between wcpd and driver causing AP to detect own BSSIDs as rogue for 24ghz
CSCwv97545	9800 EHSA fsm: EHSA standby down, HA/SSO reloads both units
CSCww11976	9136 radio reset due to beacon stuck in slot 3 6ghz after switch upgrade
CSCws76413	CW9800M Raised Authentication failure as Sub-block is missing
CSCwu62311	AP crash - Kernel panic nss_core_handle_cause_queue
CSCwv22511	Client detail for some Associated Client doesn't show info element when using Cisco Spaces Connector
CSCwv54843	WLC \" show ap wlan summary\" command shows inflated client count
CSCwv61312	Client deletion on WLC due to IP Learn timeout after roam

CSCwv71860	9115 & 9120 AP crashed due to kernel panic with reason \" console_unlock+0x288/0x284 \"
CSCwv82245	CW9179 APs absent from bsnAP SNMP tables while older APs populate correctly
CSCwv84920	Unable to delete the RAF file from WLC running 17.18.3
CSCww10073	UTF tracelogs exceed maximum allowed size in 9800-CL
CSCww17212	C9115AP Radio reset happened due to radio firmware crash
CSCww21004	Swapping primary and secondary controller name on Bulk AP Provisioning gives an error

Known issues

The known issues for Cisco IOS XE 26.2.1 include:

Wireless clients cannot join or roam after an ISSU abort from Cisco IOS XE 26.2.1

If an ISSU from Cisco IOS XE 26.2.1 is aborted and the wireless controller reverts to an earlier release, such as Cisco IOS XE 17.18 or 26.1.1, the APs might remain on release 26.2.1 and continue using the updated local MAC behavior.

Since the reverted controller does not contain the code required to process the new anchor requests from these APs, new wireless clients cannot join the network, and existing clients cannot roam successfully. As a result, affected clients are denied network access.

Compatibility

Compatibility matrix

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

Table 6. Compatibility Matrix for Cisco Catalyst 9800 Series Wireless Controllers, Release 26.2.1

Cisco Catalyst 9800 Series Wireless Controller Software	Cisco Identity Services Engine	Cisco Catalyst Center	Cisco CMX
IOS XE 26.2.1	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.
- Unidirectional Link Detection (UDLD) protocol is not supported.
- 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 26.2.1

Table 7. Upgrade Path to Cisco IOS XE Dublin 26.2.1

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 26.2.1.
16.11.x	–	Upgrade first to 16.12.5 or 17.3.x and then to 26.2.1.
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 26.2.1.	Upgrade first to 17.3.5 or later or 17.6.x or later, and then to 26.2.1.
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 26.2.1.	Upgrade first to 17.3.5 or later and then to 26.2.1.
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 26.2.1.	Upgrade first to 17.3.5 or later and then to 26.2.1.

Current software	Upgrade path for deployments with 9130, 9124, or 916x	Upgrade path for deployments without 9130 and 9124
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 26.2.1.	Upgrade directly to 26.2.1.
17.3.4c or later	Upgrade to 17.9.6 or later or 17.12.x or later, and then to 26.2.1.	Upgrade directly to 26.2.1.
17.4.x	Upgrade first to 17.6.x and then to 26.2.1.	Upgrade directly to 26.2.1.
17.5.x	Upgrade first to 17.6.x and then to 26.2.1.	Upgrade directly to 26.2.1.
17.6.x	Upgrade to 17.9.6 or later or 17.12.x or later, and then to 26.2.1.	Upgrade directly to 26.2.1.
17.7.x	Upgrade to 17.9.6 or later or 17.12.x or later, and then to 26.2.1.	Upgrade directly to 26.2.1.
17.8.x	Upgrade to 17.9.6 or later or 17.12.x or later, and then to 26.2.1.	Upgrade directly to 26.2.1.
17.9.1 to 17.9.5	Upgrade to 17.9.6 or later or 17.12.x or later, and then to 26.2.1.	Upgrade directly to 26.2.1.
17.9.6 or later	Upgrade directly to 26.2.1.	Upgrade directly to 26.2.1.
17.10.x	Upgrade to 17.12.x or later, and then to 26.2.1.	Upgrade directly to 26.2.1.
17.11.x	Upgrade to 17.12.x or later, and then to 26.2.1.	Upgrade directly to 26.2.1.
17.12.x	Upgrade directly to 26.2.1.	Upgrade directly to 26.2.1.
17.13.x	Upgrade directly to 26.2.1.	Upgrade directly to 26.2.1.
17.14.x	Upgrade directly to 26.2.1.	Upgrade directly to 26.2.1.
17.15.x	Upgrade directly to 26.2.1.	Upgrade directly to 26.2.1.
17.16.x	Upgrade directly to 26.2.1.	Upgrade directly to 26.2.1.
17.17.x	Upgrade directly to 26.2.1.	Upgrade directly to 26.2.1.
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 26.2.1.	Upgrade directly to 26.2.1.

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 26.2.1

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

- C9800-80-universalk9_wlc.26.02.01.SPA.bin
- C9800-40-universalk9_wlc.26.02.01.SPA.bin
- C9800-L-universalk9_wlc.26.02.01.SPA.bin

Image names (CW9800M, CW9800H1/CW9800H2, CW9800L)

- CW9800H-wlc-universalk9.26.02.01.SPA.bin
- CW9800M-wlc-universalk9.26.02.01.SPA.bin
- CW9800L-wlc-universalk9.26.02.01.SPA.bin

Image names (9800-CL):

- **Cloud**: C9800-CL-universalk9.26.02.01.SPA.bin
- **Hyper-V/ESXi/KVM**: C9800-CL-universalk9.26.02.01.iso, C9800-CL-universalk9.26.02.01.ova
- **KVM**: C9800-CL-universalk9.26.02.01.qcow2
- **NFVIS**: C9800-CL-universalk9.26.02.01.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

Commands	Description
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 8. Test configuration for interoperability

Hardware or software parameter	Hardware or software type
Release	Cisco IOS XE 26.2.1
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 9. 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
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)

Client type and name	Driver or software version
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.	
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	

Client type and name	Driver or software version
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
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

Client type and name	Driver or software version
Huawei Mate 20 pro	Android 9.0
Huawei P20 Pro	Android 10
Huawei P40	Android 10
LG v40 ThinQ	Android 9.0
One Plus 8	Android 11
Oppo Find X2	Android 10
Redmi K20 Pro	Android 10
Samsung Galaxy S9+ - G965U1	Android 10.0
Samsung Galaxy S10 Plus	Android 11.0
Samsung S10 (SM-G973U1)	Android 11.0
Samsung S10e (SM-G970U1)	Android 11.0
Samsung 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

Client type and name	Driver or software version
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
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	

Client type and name	Driver or software version
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
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 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 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.

Platform	Description
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.
	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 11. 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 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.
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 13. 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	–	–	–	–	–

SFP name	C9800-80-K9	C9800-40-K9	C9800-L-F-K9	CW9800H1	CW9800H2	CW9800M	CW9800L
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	–
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	–	–	–	–	–	–

SFP name	C9800-80-K9	C9800-40-K9	C9800-L-F-K9	CW9800H1	CW9800H2	CW9800M	CW9800L
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	–	–
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 name	C9800-80-K9	C9800-40-K9	C9800-L-F-K9	CW9800H1	CW9800H2	CW9800M	CW9800L
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-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	Supported
SFP-10G-LRM	Supported	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	–	–	–	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 name	C9800-80-K9	C9800-40-K9	C9800-L-F-K9	CW9800H1	CW9800H2	CW9800M	CW9800L
SFP-H25G-CU1M	–	–	–	Supported	–	Supported	–
SFP-H25G-CU3M	–	–	–	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-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	Supported	Supported	Supported	Supported
SFP-H10GB-CU1M	Supported	Supported	Supported	Supported	Supported	Supported	Supported
SFP-H10GB-CU2.5M	Supported	Supported	Supported	–	–	–	Supported
SFP-H10GB-CU2M	Supported	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 14. Cisco Catalyst 9800 series wireless controller - network protocols and port matrix

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

Source	Destination	Protocol	Destination port	Source port	Description
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
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

Source	Destination	Protocol	Destination port	Source port	Description
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 15. Supported APs

AP type	AP names
Indoor Access Points	• Cisco Catalyst 9105AX (I/W) Access Points • 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
Outdoor Access Points	• Cisco Catalyst 9124AX (I/D/E) Access Points • Cisco Catalyst 9163 (E) Series Access Points • Cisco Wireless 9177 (I/E/D) Series Wi-Fi 7 Access Points • Cisco Wireless 9179 (F) Series Wi-Fi 7 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