Release Notes for Cisco Catalyst 9800 Series Wireless Controller, Cisco IOS XE 17.18.2

Contents

Cisco Catalyst 9800 Series Wireless Controller, Cisco IOS XE 17.18.2 3
New software features 3
New hardware features 5
Change in behavior 6
Notice of upcoming changes in the Cisco IOS XE 17.18.2 release and beyond 7
Resolved issues 9
Open issues 13
Known issues 15
Compatibility 16
Supported hardware 30
Related content 40
Communications, services, and additional information: 41
Legal information 41

© 2025 Cisco and/or its affiliates. All rights reserved.

Cisco Catalyst 9800 Series Wireless Controller, Cisco IOS XE 17.18.2

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

The controllers are 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 17.18.2.

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 17.18.2

Product impact	Feature	Description
Software Reliability	TrustSec policy High Availability support for FlexConnect mode APs	This feature ensures that Cisco TrustSec SGACL enforcement remains available and consistent during High Availability events such as Stateful Switchover (SSO) between wireless controllers. This provides uninterrupted security policy enforcement on FlexConnect mode APs even during controller failover or redundancy events. For more information, see Cisco TrustSec.
	TLS signature algorithm enhancements for NDcPP v3.0e	Cisco IOS XE 17.18.2 introduces crucial TLS signature algorithm enhancements, specifically for products operating in FIPS Common Criteria (CC) mode, to achieve full compliance with the NDcPP v3.0e security standard. This feature significantly strengthens network security by removing outdated and less secure signature algorithms and ciphersuites, thereby protecting against known vulnerabilities. It outlines the approved, robust signature algorithms for TLS and DTLS applications, including EST TLS clients, RadSec, Syslog, and HTTP Secure servers. The following commands are introduced: • **logging tls-profile** *tls-profile-name* • **ciphersuite** • **ip http secure-ciphersuite** *ciphersuites* • **ip http client secure-ciphersuite** *ciphersuites* For more information, see FIPS.

© 2025 Cisco and/or its affiliates. All rights reserved.

Product impact	Feature	Description
	AP name in beacon with vendor-specific information elements (IEs)	This feature introduces a new vendor-specific information element (IE) to advertise the AP name in beacon and probe response frames, supporting AP names up to 32 characters. Legacy CCX Aironet IE behavior remains unchanged and continues to advertise AP names with a 16-character limit when CCX is enabled. The new IE is disabled by default and can be enabled independently through GUI, CLI, or NETCONF-YANG using the **advertise ap-name** configuration. When enabled alongside CCX, both the legacy CCX IE and the new AP name IE are advertised. This feature provides an alternative mechanism for clients to receive the full AP hostname without impacting the existing CCX-based deployments. For more information, see WLANs.
	Wireless Active Testing (WAT) with ThousandEyes	With this release, Wireless Active Testing with ThousandEyes allows you to enable Cisco Wireless 9172H APs to act as synthetic clients, proactively identifying Wi-Fi issues in real time. By integrating the ThousandEyes Endpoint Agent, these wall plate APs perform end-to-end wireless onboarding and application performance tests directly at the network edge, delivering wireless assurance insights and driving towards an optimal user experience. For more information, see Wireless Active Testing with ThousandEyes and *Cisco Active Testing for Wireless with ThousandEyes On-Prem Deployment Guide*.
	Fast Switching on RLAN Ports in Cisco Wireless 9172 Series Access Points	From this release, fast switching for RLAN client traffic is supported on Cisco Wireless 9172 Series Access Points. For more information, see Remote LANs.
Ease of setup	Smart Spaces location and AnyLocate capabilities	AnyLocate capabilities enhance indoor location services by leveraging ultra-wideband (UWB) and Wi-Fi fine timing measurement (FTM). This suite enables precise indoor wayfinding and asset tracking, transforming APs into powerful location sensors. The following commands are introduced: • **[no] geolocation uwb wayfinding** • **geolocation uwb wayfinding b-duration** • **[no] geolocation height-above-the-floor** • **show ap geolocation uwb wayfinding** • **show ap geolocation uwb asset-trackings** For more information, see Smart Spaces - AnyLocate capabilities.
	SAE client exclusion visibility	The SAE client exclusion visibility feature in Cisco IOS XE 17.18.2 centralizes client authentication failure and exclusion data on the controller. This significantly reduces manual log collection and operational costs in Flex central authentication deployments with SAE-enabled WLANs, providing administrators with improved visibility, syslog messages for events, and configurable control over client exclusion durations. For more information, see IP Theft.
	Cisco Support Assistant integration in the controller GUI	This feature integrates the Cisco Support Assistant (CSA) directly within the controller GUI. You can now open TAC cases, upload logs, record screens, and access contextual help directly from within the controller GUI, and without installing the Chrome browser extension. You can find a feature demonstration here. For more information, see Overview of the Controller.

© 2025 Cisco and/or its affiliates. All rights reserved.

Product impact	Feature	Description
	Enhanced client data enrichment with new complex event processing (CEP) gather point	In this release, a new CEP gather point has been added to the Cisco-IOS-XE-wireless-client-global-oper module, using the xpath: /client-global-oper-data/client-cnsld-data. This enhancement consolidates data from multiple sources—including common-oper-data, dot11-oper-data, traffic-stats, and sisf leafs—using the client MAC address as the key.
	Catalyst 9800 Series Wireless Controller for Cloud (C9800-CL) support for Cloud Monitoring for wireless	The C9800-CL virtual wireless controllers can now be onboarded directly to the Meraki dashboard through the new virtual Catalyst registration service. This enables C9800-CL to benefit from the same simple, secure Meraki cloud connectivity and monitoring experience as physical C9800 appliances.
	Packet Capture support for Cloud Monitoring for wireless	Support for manual and scheduled packet capture on cloud-monitored APs enables administrators to remotely initiate on-demand captures or automate recurring capture schedules directly from the Meraki dashboard. This facilitates faster root-cause analysis and streamlined troubleshooting, all without requiring on-site access to the AP.
Compliance	6 GHz country support for Vietnam	From Cisco IOS XE 17.18.2 onwards, Vietnam (VN) is added to the list of countries that support the 6 GHz radio band. For more information, see Countries and Regulations.
	Additional country support for Cisco Wireless 9179F Access Points	From Cisco IOS XE 17.18.2 onwards, numerous countries support the Cisco Wireless 9179F APs, enhancing functionality and broadening deployment options worldwide. For more information, see Countries and Regulations.

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.

See Cisco Enterprise Networking Product Analytics Frequently Asked Questions.

New hardware features

- With Cisco IOS XE 17.18.2, the Cisco Wireless 9174I Series Wi-Fi 7 Access Points (CW9174I), Cisco Wireless 9174E Series Wi-Fi 7 Access Points (CW9174E), and Cisco Wireless 9171I Series Wi-Fi 7 Access Points (CW9171I) are supported.

  The CW9174I APs, CW9174E APs, and CW9171I APs, are tri-band (2.4 GHz, 5 GHz, 6 GHz) APs. The APs support full interoperability with leading 802.11be, 802.11ax, and legacy clients, and a hybrid deployment with other APs and controllers. For a full listing of the APs' features and specifications, see:

  Cisco Wireless 9174 (I/E) Series Wi-Fi 7 Access Point Data Sheet

  Cisco Wireless 9171I Series Wi-Fi 7 Access Point Data Sheet

© 2025 Cisco and/or its affiliates. All rights reserved.

For more information regarding the AP hardware, see:

Cisco Wireless 9174I Series Wi-Fi 7 Access Point Hardware Installation Guide

Cisco Wireless 9174E Series Wi-Fi 7 Access Point Hardware Installation Guide

Cisco Wireless 9171I Series Wi-Fi 7 Access Point Hardware Installation Guide

Note: Software support for CW9174I, CW9174E, and CW9171I is available for all countries in this release. We recommend that you consult the Product Approval Status page to check individual country compliance approval: https://cae-cnc-prd.cisco.com/pdtcnc/#/.

- Cisco CW9800L Wireless Controller (CW9800L): CW9800L is the next-generation entry-level controller for small campuses and distributed branches, offering 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.

  The latest release adds an external redundant power supply option for greater reliability, up to 10dB quieter operation for noise-sensitive environments, and hardware acceleration for advanced encryption—ensuring secure, high-performance connectivity for modern enterprises.

  For more information, see *Cisco CW9800L Wireless Controller Hardware Installation Guide* and *Cisco CW9800L Wireless Controller Data Sheet*.

Change in behavior

Table 2. Change in behavior for Cisco Catalyst 9800 Series Wireless Controllers, Release 17.18.2

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.
WLAN Compatibility Improvements for Wi-Fi 6E and Wi-Fi 7 in the WLAN GUI page	WLAN compatibility improvements for Wi-Fi 6E and Wi-Fi 7 include: • Individual compatibility checks: Each WLAN now has its own dedicated compatibility check for Wi-Fi 7, with Wi-Fi 6E status displayed alongside. • Comprehensive compatibility assessment: Compatibility is evaluated based on settings, including WPA3, cipher, PMF configurations, and band enablement. • Enhanced navigation: New hyperlinks make it easier to move between configuration pages. • Improved monitoring view: The updated view provides detailed information on SSID compatibility and the current operational status.
Support for Spectrum Preference (SP) bias in Automated Frequency Coordination (AFC)	With the introduction of AFC and SP, managing SP 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 SP Bias within RRM, ensuring optimal performance and compliance, particularly in AFC environments. To operate the radio in SP mode, at least five AFC channels must be available based on the configuration (including channel width, DCA channel list, and PSC settings), and the AFC license must support a minimum power level of 1.

© 2025 Cisco and/or its affiliates. All rights reserved.

Feature	Description
Deprecation of commands of obsolete features in local MAC	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	Starting with 17.18.2, 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.
SFP Support with FEC mode cl74 between CW9800M/CW9800H1 and Nexus switches	Starting with Cisco IOS XE 26.1.1, 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.

Notice of upcoming changes in the Cisco IOS XE 17.18.2 release and beyond

Cisco is committed to safeguarding our products and customer networks against increasingly sophisticated threat actors. As computing power and the threat landscape have evolved, some features and protocols currently in use have become vulnerable to attack. While more secure alternatives are now available, legacy protocols may still be in use in some environments.

To improve network security, reduce the attack surface, and protect sensitive data, Cisco is phasing out legacy and insecure features and protocols, encouraging customers to transition to more secure alternatives. This process is gradual and designed to minimize operational impact. This is part of a broader initiative to make Cisco products more secure by default and secure by design.

Starting with the Cisco IOS XE 17.18.2 release and in future releases, Cisco software will display warning messages when configuring features or protocols that do not provide sufficient security such as those transmitting sensitive data without encryption or using outdated encryption mechanisms. Warnings will also appear when security best practices are not followed, along with suggestions for secure alternatives.

This list is subject to change, but the following is a list of features and protocols that are planned to generate warnings from version Cisco IOS XE 17.18.2.

Release notes for each release will describe exact changes for that release.

- **Plain-text and weak credential storage**: Type 0 (plain text), 5 (MD5), or 7 (Vigenère cipher) in configuration files.

© 2025 Cisco and/or its affiliates. All rights reserved.

Recommendation: Use Type 6 (AES) for reversible credentials, and Type 8 (PBKDF2-SHA-256) or Type 9 (Scrypt) for non-reversible credentials.

- **SSHv1**:

  Recommendation: Use SSHv2.

- **SNMPv1 and SNMPv2, or SNMPv3 without authentication and encryption**:

  Recommendation: Use SNMPv3 with authentication and encryption (authPriv).

- **MD5 (authentication) and 3DES (encryption) in SNMPv3**:

  Recommendation: Use SHA1 or, preferably, SHA2 for authentication, and AES for encryption.

- **IP source routing based on IP header options**:

  Recommendation: Do not use this legacy feature.

- **TLS 1.0 and TLS 1.1**:

  Recommendation: Use TLS 1.2 or later.

- **TLS ciphers using SHA1 for digital signatures**:

  Recommendation: Use ciphers with SHA256 or stronger digital signatures.

- **HTTP**:

  Recommendation: Use HTTPS.

- **Telnet**:

  Recommendation: Use SSH for remote access.

- **FTP and TFTP**:

  Recommendation: Use SFTP or HTTPS for file transfers.

- **On-Demand Routing (ODR)**:

  Recommendation: Use a standard routing protocol in place of CDP-based routing information exchange.

- **BootP server**:

  Recommendation: Use DHCP or secure boot features such as Secure ZTP.

- **TCP and UDP small servers (echo, chargen, discard, daytime)**:

  Recommendation: Do not use these services on network devices.

- **IP finger**:

  Recommendation: Do not use this protocol on network devices.

- **NTP control messages**:

  Recommendation: Do not use this feature.

- **TACACS+ using pre-shared keys and MD5**:

  Recommendation: Use TACACS+ over TLS 1.3, introduced in release Cisco IOS XE 17.18.1.

- **Wireless LAN Controller, CAPWAP DTLS**:

© 2025 Cisco and/or its affiliates. All rights reserved.

Recommendation: Do not use DTLSv1.0 and weaker ciphersuites.

- **Wireless LAN Controller, WLAN**:

  Recommendation: Do not use 802.1x key management security.

- **Wireless LAN Controller, Mobility**:

  Recommendation: Do not use weaker ciphers and use stronger ciphers.

- **Wireless LAN Controller, NMSP**:

  Recommendation: Do not use weaker ciphers and use strong ciphers.

Cisco is committed to supporting customers through this transition. Subsequent releases on the Cisco IOS XE 17.18 train will continue to support these features but will display warnings if they are used. Future release trains may impose additional restrictions on these features which will be communicated through release notes.

For more information, see Resilient Infrastructure IOS XE Security Warnings Reference.

Resolved issues

To see 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 17.18.2

Bug ID	Description
CSCwr22504	Controller crashed due to critical process wncmgrd fault on rp_0_0 (rc=134)
CSCwq81750	WMI IP is null (0.0.0.0) in the CAPWAP packet while forwarding the multicast traffic
CSCwo61286	Audit session ID changes after inter-WNCd roam on Central Web Authentication (CWA) with PSK
CSCwo79334	17.15.3 multicast traffic fails post to controller switchover
CSCwp20530	Controller does not forward downstream packets to the wireless client after switchover
CSCwp65184	Controller crash after predownload initiated
CSCwp95190	C9800 controller unable to handle new client connections due to memory failure
CSCwp96099	17.18.1: C9800-L stand-by crash @ Process = EWLC IOSD CAPWAP PROCESS
CSCwp96707	C9800-CL: show ap summary command output column misalignment
CSCwq02929	[URWB_CW] Show AP command not working for 5ghz with slot 0
CSCwq30202	Frequent channel changes seen on 6 GHz
CSCwq35878	High Availability not forming due to Active and Standby configuration being out of sync
CSCwq44647	Bulk sync failing after multiple SSO
CSCwq60945	Access point data tunnel going to NULL state an unable to recover it as it incorrectly detects an existing session already in place

© 2025 Cisco and/or its affiliates. All rights reserved.

Bug ID	Description
CSCwq66623	SJC Alpha - 17.18.2 alpha APs not joining controller- stuck in DTLS
CSCwq68606	C9800 controller unexpected crash at fair_q_hash modules due to invalid QOS parameters
CSCwq70914	linux_iosd crash seen on C9800 in process IGMPSN
CSCwq73135	9800 controller memory leak in /tmp/rp/tdldb_rcow database handle WNCD_DB
CSCwq94551	Multicast stream occasionally stuck after WGB roaming between COS APs
CSCwr01746	Unexpected reloads when processing the command \" show ap sum sort name\"
CSCwr29181	CDP Proximity: AP not resolving via CDP/LLDP when they are on different site tag
CSCwr33067	/client-oper-data/dot11-oper-data invalid value
CSCwr37495	High Channel Utilization due to high interference on 6GHz channels
CSCwr44462	EMUL DB records are not destroyed and increasing the memory utilization
CSCwr80374	9800 controller reboots due memory leak in wncloudm
CSCws16148	Controller crash after issuing the command “ap geolocation ranging accurate method uwb”
CSCws18528	[APCI] MLO Rogue Containment for all bands is not working
CSCwn47435	Unable to fill roaming OI field when adding an ANQP server
CSCwn55495	Cisco Catalyst 9800-40 controller displays random CPU spikes on EZMAN
CSCwo70155	Optimize rogue/neighbor bssid processing by WNCD when the bssid-neighbor-stats config is enabled
CSCwo73753	C9800 not enforcing SGT policies for static/sxp tags on the same L2 network
CSCwp25836	Request for RPC support for dual band radio use-cases
CSCwp39409	Controller reboots unexpectedly due to an assertion failure in WNCd process
CSCwp51241	Policy details are not updating properly in User Administration
CSCwp59492	Controller console flooded with " wncd: Failed to handle IGMP join" errors
CSCwp60602	17.9.3 - Slot values shows ok for status-desc in the response body of the REST API call
CSCwp63587	RF profiles is not displayed in the controller CLI through 'show wireless tag rf all'
CSCwp64707	C9400 switch fails to provide \" show running-config | format netconf-xml\"
CSCwp80750	Showing blank in Assisted Roaming prediction-minimum Value in CLI
CSCwp99623	C9800-CL public cloud VLAN page In GUI fails to load
CSCwq16047	Flex CA LS MLO OKC roam fails as controller is not sending Add Mobile

© 2025 Cisco and/or its affiliates. All rights reserved.

Bug ID	Description
CSCwq23533	Enable SP bias in AFC operation
CSCwq31446	Configuration syntax for flex site tags is out of order. no local site not specified before flex site configs
CSCwq33181	\" open-roaming-oi allow-all beacon\" does not advertise 5A03BA0000 in dot11 beacon frames
CSCwq34114	\" no shutdown\" not accepting if trying to change the configs under WLAN
CSCwq46350	After the AP refresh, the old AP name is not being retained or carried over to the new AP
CSCwq64936	IP theft feature is disconnecting the legit client when there is an event
CSCwq65879	Invalid character in AP name causing AP bulk provisioning failures
CSCwq68954	Controller reloaded due to a crash on RRM process
CSCwq73627	AAA CUI Attribute missing in the controller
CSCwq96211	The controller DNS Servers added to the DHCP pool are not visible in the Web UI
CSCwr00047	Mobility tunnel between 9800-40 controller and AireOS controller flapping, after upgrade of 9800-40 controller to 17.15.4
CSCwr29697	Controller failover issue due to rogue containment
CSCwr32755	Controller GUI does not show Trustpoints in PKI Management Trustpoints tab 17.12
CSCwr33787	Wireless controller reloads due to Segmentation Fault on WNCD process
CSCwr46982	FEW: Client IP-MAC address binding features cause high number of CAPWAP control traffic during client join or slow roaming events
CSCwr59243	The controller crashed several times during the RRM process
CSCwr60281	Cannot import PFX from GUI, but works from CLI
CSCwr60386	CW9800M GUI displays incorrect Wi-Fi 7 client connection speed
CSCwr70752	The controller is not displaying Fabric Media Stream clients in Web GUI
CSCwo68312	Cisco Catalyst 9124AXE-E APs identifies antennas wrongly
CSCwo88544	AP9120 crashed due to kernel panic
CSCwp06870	Functional SJC Alpha CW9176I AP Kernel Crash on ap-17.18.0.45
CSCwp14628	Cisco Aironet 3800 APs display client authentication issue after AP Migration to a controller running 17.15.3
CSCwp27215	Cisco Catalyst 9124 AP in mesh mode encounters poor iperf traffic performance
CSCwp38822	9166 will not allow 802.1x QoS WLAN markers/VAP but will Open and PSK
CSCwp61910	C9130AX - RHL driver bootup failure causes sh crash, which triggers kernel panic.

© 2025 Cisco and/or its affiliates. All rights reserved.

Bug ID	Description
CSCwp62799	C9130AX - RHL bootup failure due to Wbpll handshake failure.
CSCwp65769	Cisco Wave 2 APs performing with fast transition with 802.1X authentication send incorrect M2 message during re-key on session timeout
CSCwp68123	11be APs degrading DSCP 34/AF41 QoS to Best Effort and/or Background to downstream traffic
CSCwq12607	9120 AP unexpected reload due to Radio firmware beacon TX stuck
CSCwq15811	CSBUCS-793 : 17.18.1 : UWB Firmware crashes seen on CW9178/CW9176 APs
CSCwq18337	BLE firmware not updated when Access Point image is downgraded
CSCwq29604	SJC Alpha CW9166I Kernel crash on ap-17.18.0.75 image
CSCwq31343	BGL18 Alpha: 9120 AP crashed due to kernel panic
CSCwq36499	EWC 9124 Crash - Controller log indicates Internal error: Oops: 96000004 [#1] SMP[#08006182, #08069984]
CSCwq46170	CW9166I AP Radio 1 crash due to beacon stuck on ap-17.18.1.6
CSCwq71415	AP1852 sends excessive BAR flood due to Client not responding to data
CSCwq86660	SJC Alpha CW9178I AP core_grpcd on ap-17.18.2.12
CSCwq93561	17.18.2: CW9172 Observed crash while running longevity
CSCwq97854	Flex WLAN VLAN mappings not retained on COS APs with 9800 controller
CSCwr00210	CW9178 AP not taking clients in 2.4 GHz due to MAC HW Hang/PHY Error
CSCwr13657	SJC Alpha C9136, C9164, C9166, C9178, C9176 AP core-ble_transport on ap-17.18.2.27
CSCwr21290	Catalyst 9105 APs stops ACKing frames due to RX Stuck and fails for clients connected in 5 GHz Slot
CSCwr24495	SJC Alpha CleanAir cores seen on APs due to Scan Radio Down on ap-17.18.2.30
CSCwr60764	Kernel Panic at pc : dp_rx_peer_map_handler+0x6a8/0x12c0 in 17.18.2
CSCwr71932	WAT IOx Upgrade of TE EPA Sometimes Fails and Creates New Agent on TE Platform
CSCws06002	[17.18.2 - EWLC SIT] - AP9176/9178 ranging crashes continuously
CSCwo75325	SST:17.12.6: Crash due to radio failures (Beacon Stuck) seen on 1832 or 1852 APs
CSCwp20425	Roaming failure in FlexConnect mode with WPA3-SAE and OKC enabled
CSCwp33811	9136 AP - Air quality and temperature sensor status not reflecting as disabled
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)

© 2025 Cisco and/or its affiliates. All rights reserved.

Bug ID	Description
CSCwp93242	AP serial number in IOX application
CSCwp95843	AP failed to join controller with multiple iCAP subscription client statistics filter in join profile
CSCwp99091	IW9167EH- AP Seen CleanAird core file during, during this testing AP was just connected, no active activity
CSCwq03579	Malformed scan packets on Silabs NCP
CSCwq14248	17.15.4: Kernel panic during assert recovery
CSCwq17491	Observing randomly ICMP packet drops with 3802 AP and propietary high roaming device
CSCwq18287	17.15.4 [SST] - CAPWAPd Crash on 9162 AP's while notifying to spaces_grpcd
CSCwq19861	IOX app not able to communicate with IOt chip
CSCwq28572	Association response frames were missing in the anomaly PCAP after mapping the \" Invalid RSNIE/Rate mismatch\" bad profile on WiFi-7 APs.
CSCwq34135	CW9178 AP not taking in clients on 2.4 GHz
CSCwq51237	ThousandEyes Endpoint Agent Fails to Download with OpenSSL Error
CSCwq66265	Client sending HE capabilities to Wi-Fi 5 AP triggers association failure
CSCwq73700	COS APs does not keep manual Geolocation coordinates across reboots
CSCwr01343	9166 AP Radio Interface down after booting up process
CSCwr11967	AP9162: Radio1 FW Core dump
CSCwr14196	9172H: RLAN clients still seen on controller when fast switching enabled
CSCwr19606	Wireless Active Testing (WAT) ThousandEyes Endpoint Agent is testing wrong gateway
CSCwr26505	C9130 AP fails to send Discovery Request with IPv6 Address post an Outage.
CSCwr32085	1815 AP Trace Event Crash
CSCwr42229	C9120/C9130 COS AP showing false positive TDD Transmit and Wi-Fi Inv. Ch interferer alerts
CSCwr69625	CleanAir not reporting on specific APs - 9120
CSCwr69841	CW9176 showing two MAC addresses behind the switchport
CSCwr77143	IW9167EH: Kernel panic running 17.15.2

Open issues

To see 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

© 2025 Cisco and/or its affiliates. All rights reserved.

Catalyst 9800 Series Wireless Controllers, Release 17.18.2. 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 17.18.2

Bug ID	Description
CSCws53690	17.12.6a ->17.18.2 ISSU, AP disjoin after active -> standby
CSCws58703	SST: ndbmand cores are seen after ISSU upgrade from 17.15.x to 17.18.2 with CATC, NETCONF not working
CSCws46393	AP gets disconnected post SSO as AP packets do not reach the controller post SSO
CSCws44009	17.18.2: Power table update for CW9174I, CW9174E, and CW9171I - US - Mexico 2.4 GHz separation
CSCwk79990	C9800-L encounters kernel unresponsiveness due to IntelResetRequest
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
CSCwr75465	High CPU in wncd 99%-100% after change AP name to AP name that already exist in the controller
CSCwr75650	Cisco 8821 IP Phones experiencing reliability issue with 9136 APs
CSCwr77247	AP crash on 9174I running 17.18.2EFT10: Kernel Panic
CSCws06706	C9178: Clients unable to join 2.4 radio due to MAC HW Hang/PHY Error
CSCws15207	9120 WGB taking long time to send authentication requests after scan is done during roaming same channel
CSCws15213	9120 WGB taking long time to send authentication request after scan is done while roaming different channels
CSCws26236	WGB 9105 crashes when wired0 flaps \" NMI watchdog: BUG: soft lockup - CPU#x stuck for xxs\"
CSCws26825	C9105 AP stops accepting clients due to RX too late errors CSP
CSCws29453	C9120 AP capwapd process crash without reboot
CSCwq96233	C9120 COS AP crash NMI watchdog: BUG: soft lockup - CPU stuck for #s! wl0-kthrd CSP
CSCwr30777	9800 standby chassis shows Cisco Unknown Power Supply and same SN on output from \" show inventory\" 17.12.4
CSCwr79853	In file manager, when selecting one file in the location box, download fails
CSCwr87352	Remove Mesh country restriction warning from UI
CSCwr96781	No AQ info output for 6 GHz band \" show ap dot11 6ghz cleanair air-quality summary\" command in the controller

© 2025 Cisco and/or its affiliates. All rights reserved.

Bug ID	Description
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
CSCws02701	Cisco Catalyst 9166i APs are unable to detect RRM neighbors on 5GHz radio while on channel 56
CSCws03213	Unexpected reboot on controller produced due to wncd process due to assertion failure
CSCws08239	Ucode crash with segfault in cce_sce_classify
CSCws10863	9800 – Global config is not overridden by the RF profile
CSCws17702	PAED process crashes every 24 after record pruning and DB query errors
CSCws19600	AP BLE Radio Status \" Powered Off\" despite \" no ap dot15 shutdown\" configuration enabled on the controller
CSCws25172	9166 APs keep crashing when 6GHz radio is on, using RO country code on controller version 17.15.3
CSCws26758	Controller client entries causing AP to reach max number of clients per radio

Known issues

The known issues for Cisco IOS XE 17.18.2 include:

Cisco Catalyst 9130 Series and 9124 Series APs cannot boot software that are earlier than 17.9, after an upgrade

After upgrading a Cisco Catalyst 9130 or 9124 AP to Cisco IOS XE 17.18.2, 26.1.1, or a later release, the AP cannot boot an image earlier than Cisco IOS XE 17.9. Attempts to boot images such as Cisco AireOS 8.10 or Cisco IOS XE 17.3 will fail. For more information, refer to CSCwv10846.

2.4 GHz output power in CW9174(I/E) and CW9171I APs

For the CW9174x and CW9171x APs, the 2.4 GHz output power has been lowered in the U.S. and Canada regulatory domains for channels 1 to 4, channel 10, and channel 11. This issue occurs only in version 17.18.2 and will be resolved with CSCws44009.

Channels	2.4 GHz output power for U.S and Canada regulatory domains
1	9 dBm
2	12 dBM
3	15 dBm
4	18 dBm
5	20 dBm
6	20 dBm
7	20 dBm

© 2025 Cisco and/or its affiliates. All rights reserved.

Channels	2.4 GHz output power for U.S and Canada regulatory domains
8	20 dBm
9	20 dBm
10	18 dBm
11	15 dBm

Cisco Wireless 9174E Series AP operates in On-Channel Neighbor Discovery Protocol (NDP) mode by default

The Cisco Wireless 9174E Series Access Point operates in On-Channel Neighbor Discovery Protocol (NDP) mode by default. In this mode, NDP is transmitted on the client-serving radio and received by the auxiliary (Aux) or scan radio. You can also configure the AP to Off-Channel mode. In Off-Channel mode, NDP is transmitted on the Aux/scan radio and received by the client-serving radio. Typically, NDP is transmitted at higher power level in 6 GHz. However, when the 9174E operates in Off-Channel mode, the NDP Tx power is the same for both 6 GHz SP and LPI due to Board Data File (BDF) limitations.

Avoiding AP sniffer mode in Cisco ACI environment

Avoid enabling AP sniffer mode when the controller is connected to Cisco Application Centric Infrastructure (ACI) that uses default endpoint learning. For more information, refer to CSCwa45713.

Compatibility

Compatibility matrix

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

Table 5. Compatibility Matrix for Cisco Catalyst 9800 Series Wireless Controllers, Release 17.18.2

Cisco Catalyst 9800 Series Wireless Controller Software	Cisco Identity Services Engine	Cisco Prime Infrastructure	Cisco AireOS-IRCM Interoperability	Cisco Catalyst Center	Cisco CMX
IOS XE 17.18.2	3.4 3.3 3.2 3.1 3.0 * all with latest patches	Not available	8.10 latest MR 8.5 latest MR	See Cisco Catalyst Center Compatibility Information.	11.1.1

GUI system requirements

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

Table 6. Hardware requirements

© 2025 Cisco and/or its affiliates. All rights reserved.

Processor speed	DRAM	Number of colors	Resolution	Font size
233 MHz minimum **Note**: We recommend 1 GHz.	512 MB **Note**: We recommend 1-GB DRAM.	256	1280 x 800 or higher	Small

Software requirements

Operating Systems:

- Windows 7 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:

- ISSU process recommendations for Cisco IOS XE 17.18.2:
    - This is applicable only for ISSU upgrades.
    - Direct ISSU upgrade from 17.12 to 17.18.2 will result in AP reload after 17.18.2 ISSU upgrade with approximate downtime of five minutes (may depend on the network traffic and congestion) - Due to CSCws53690.

      To avoid AP reload (CSCws53690) from 17.12 to 17.18, perform intermediate N+1 ISSU upgrade (17.12.x -> 17.15.4d -> 17.18.2). Intermediate upgrade should be done only from 17.15.4d.

© 2025 Cisco and/or its affiliates. All rights reserved.

    - Any ISSU upgrade from 17.15.x to 17.18.2 will not impact AP reload issue. We recommend that you reconfigure NETCONF/YANG on 17.18.2 after rolling AP upgrades due to CSCws58703, if NETCONF connection is down.

- 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.
- 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, see 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, see: https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/220443-how-to-avoid-boot-loop-due-to-corrupted.html.
- The following Wave 1 APs are not supported 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, see the SSH Algorithms for Common Criteria Certification document available at: https://www.cisco.com/c/en/us/td/docs/routers/ios/config/17-x/sec-vpn/b-security-vpn/m_sec-secure-shell-algorithm-ccc.html.
- If APs fail to detect the backup image after running the archive download-sw command, perform the following steps:
    - 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>
```

© 2025 Cisco and/or its affiliates. All rights reserved.

- 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.

- Fragmentation lower than 1500 is not supported by the RADIUS packets generated by wireless clients in the Gi0 (OOB) interface.
- 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, see the Upgrading ROMMON for Cisco Catalyst 9800-L Wireless Controllers section of the Upgrading Field Programmable Hardware Devices for Cisco Catalyst 9800 Series Wireless Controllers document.

- By default, the controller uses a TFTP block size value of 512, which is the lowest possible value. This default setting is used to ensure interoperability with legacy TFTP servers. If required, you can change the block size value to 8192 to speed up the transfer process, using the **ip tftp blocksize** command in global configuration mode.
- 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.

© 2025 Cisco and/or its affiliates. All rights reserved.

- 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.
- Communication between Cisco Catalyst 9800 Series Wireless Controller and Cisco Prime Infrastructure uses different ports:
    - All the configurations and templates available in Cisco Prime Infrastructure are pushed through SNMP and CLI, using UDP port 161.
    - Operational data for controller is obtained over SNMP, using UDP port 162.
    - AP and client operational data leverage streaming telemetry:

  Cisco Prime Infrastructure to controller: TCP port 830 is used by Cisco Prime Infrastructure to push the telemetry configuration to the controller (using NETCONF).

  Controller to Cisco Prime Infrastructure: TCP port 20828 is used for Cisco IOS XE 16.10.x and 16.11.x, and TCP port 20830 is used for Cisco IOS XE 16.12.x, 17.1.x and later releases.
- 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
  ```

© 2025 Cisco and/or its affiliates. All rights reserved.

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, see Upgrading Field Programmable Hardware Devices for Cisco Catalyst 9800 Series Wireless Controllers.

Upgrade path to Cisco IOS XE 17.18.2

Note: For Cisco Catalyst 9136, 9164, and 9166 APs, a direct upgrade from 17.9.1 to 17.15.x or 17.18.x will fail due to insufficient space. To perform the upgrade, you must first update to 17.9.6 or 17.9.7 before proceeding to 17.15.x or 17.18.x.

Table 7. Upgrade Path to Cisco IOS XE Dublin 17.18.2

Current software	Upgrade path for deployments with 9130 or 9124	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 17.18.2.
16.11.x	–	Upgrade first to 16.12.5 or 17.3.x and then to 17.18.2.
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 17.18.2.	Upgrade first to 17.3.5 or later or 17.6.x or later, and then to 17.18.2.
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 17.18.2.	Upgrade first to 17.3.5 or later and then to 17.18.2.
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 17.18.2.	Upgrade first to 17.3.5 or later and then to 17.18.2.
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 17.18.2.	Upgrade directly to 17.18.2.
17.3.4c or later	Upgrade to 17.9.6 or later or 17.12.x or later, and then to 17.18.2.	Upgrade directly to 17.18.2.
17.4.x	Upgrade first to 17.6.x and then to 17.18.2.	Upgrade directly to 17.18.2.
17.5.x	Upgrade first to 17.6.x and then to 17.18.2.	Upgrade directly to 17.18.2.
17.6.x	Upgrade to 17.9.6 or later or 17.12.x or later, and then to 17.18.2.	Upgrade directly to 17.18.2.

© 2025 Cisco and/or its affiliates. All rights reserved.

Current software	Upgrade path for deployments with 9130 or 9124	Upgrade path for deployments without 9130 and 9124
17.7.x	Upgrade to 17.9.6 or later or 17.12.x or later, and then to 17.18.2.	Upgrade directly to 17.18.2.
17.8.x	Upgrade to 17.9.6 or later or 17.12.x or later, and then to 17.18.2.	Upgrade directly to 17.18.2.
17.9.1 to 17.9.5	Upgrade to 17.9.6 or later or 17.12.x or later, and then to 17.18.2. **Note**: For Cisco Catalyst 9136, 9164, and 9166 APs, a direct upgrade from 17.9.1 to 17.15.x or 17.18.x will fail due to insufficient space. To perform the upgrade, you must first update to 17.9.6 or 17.9.7 before proceeding to 17.15.x or 17.18.x.	Upgrade directly to 17.18.2.
17.9.6 or later	Upgrade directly to 17.18.2.	Upgrade directly to 17.18.2.
17.10.x	Upgrade to 17.12.x or later, and then to 17.18.2.	Upgrade directly to 17.18.2.
17.11.x	Upgrade to 17.12.x or later, and then to 17.18.2.	Upgrade directly to 17.18.2.
17.12.x	Upgrade directly to 17.18.2.	Upgrade directly to 17.18.2.
17.13.x	Upgrade directly to 17.18.2.	Upgrade directly to 17.18.2.
17.14.x	Upgrade directly to 17.18.2.	Upgrade directly to 17.18.2.
17.15.x	Upgrade directly to 17.18.2.	Upgrade directly to 17.18.2.
17.16.x	Upgrade directly to 17.18.2.	Upgrade directly to 17.18.2.
17.17.x	Upgrade directly to 17.18.2.	Upgrade directly to 17.18.2.
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 17.18.2.	Upgrade directly to 17.18.2.

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.

© 2025 Cisco and/or its affiliates. All rights reserved.

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 17.18.2

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

- C9800-80-universalk9_wlc.17.18.02.SPA.bin
- C9800-40-universalk9_wlc.17.18.02.SPA.bin
- C9800-L-universalk9_wlc.17.18.02.SPA.bin

Image names (CW9800M, CW9800H1/CW9800H2, CW9800L)

- CW9800H-wlc-universalk9.17.18.02.SPA.bin
- CW9800M-wlc-universalk9.17.18.02.SPA.bin
- CW9800L-wlc-universalk9.17.18.02.SPA.bin

Image names (9800-CL):

- **Cloud**: C9800-CL-universalk9.17.18.02.SPA.bin
- **Hyper-V/ESXi/KVM**: C9800-CL-universalk9.17.18.02.iso, C9800-CL-universalk9.17.18.02.ova
- **KVM**: C9800-CL-universalk9.17.18.02.qcow2
- **NFVIS**: C9800-CL-universalk9.17.18.02.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

© 2025 Cisco and/or its affiliates. All rights reserved.

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, see 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 17.18.2
Cisco Wireless Controller	See Supported hardware
Access Points	See 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	See 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

© 2025 Cisco and/or its affiliates. All rights reserved.

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)
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

© 2025 Cisco and/or its affiliates. All rights reserved.

Client type and name	Driver or software version
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	
Apple iPhone 5	iOS 12.4.1
Apple iPhone 6s	iOS 13.5

© 2025 Cisco and/or its affiliates. All rights reserved.

Client type and name	Driver or software version
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
Huawei Mate 20 pro	Android 9.0
Huawei P20 Pro	Android 10

© 2025 Cisco and/or its affiliates. All rights reserved.

Client type and name	Driver or software version
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
Spectralink Versity Phones 9540 Series	Android 8.1.0
Vocera Badges B3000n	4.3.3.18

© 2025 Cisco and/or its affiliates. All rights reserved.

Client type and name	Driver or software version
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	
Intel AX 411	Driver v22.230.0.8
Intel AX 211	Driver v22.230.0.8, v22.190.0.4

© 2025 Cisco and/or its affiliates. All rights reserved.

Client type and name	Driver or software version
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. (See 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.
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.

© 2025 Cisco and/or its affiliates. All rights reserved.

Platform	Description
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, 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.

© 2025 Cisco and/or its affiliates. All rights reserved.

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	–	–	–	–	–
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	–	–	–	–

© 2025 Cisco and/or its affiliates. All rights reserved.

SFP name	C9800-80-K9	C9800-40-K9	C9800-L-F-K9	CW9800H1	CW9800H2	CW9800M	CW9800L
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	–	–	–	–	–	–
QSFP-H40G-ACU7M				Supported	Supported	Supported	
QSFP-H40G-ACU10M	–	–	–	–	Supported	–	–
QSFP-H40G-CU1M	–	–	–	–	Supported	–	–
QSFP-H40G-CU2M	–	–	–	–	Supported	–	–

© 2025 Cisco and/or its affiliates. All rights reserved.

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

© 2025 Cisco and/or its affiliates. All rights reserved.

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

© 2025 Cisco and/or its affiliates. All rights reserved.

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

© 2025 Cisco and/or its affiliates. All rights reserved.

Source	Destination	Protocol	Destination port	Source port	Description
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)
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

© 2025 Cisco and/or its affiliates. All rights reserved.

Source	Destination	Protocol	Destination port	Source port	Description
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
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

© 2025 Cisco and/or its affiliates. All rights reserved.

AP type	AP names
Indoor Access Points	• Cisco Catalyst 9105AX (I/W) Access Points • Cisco Catalyst 9115AX (I/E) Access Points • Cisco Catalyst 9117AX (I) 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) Series Wi-Fi 7 Access Points • Cisco Wireless 9172 (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 1800i Access Point • 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, see the Detailed Channels and Maximum Power Settings document at

© 2025 Cisco and/or its affiliates. All rights reserved.

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, see 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, see these documents:

Cisco Wireless Solutions Software Compatibility Matrix

Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide

Cisco Catalyst 9800 Series Wireless Controller Command Reference

Cisco Catalyst 9800 Series Configuration Best Practices

In-Service Software Upgrade Matrix

Upgrading Field Programmable Hardware Devices for Cisco Catalyst 9800 Series Wireless Controllers

The installation guide for your controller is available at:

Hardware Installation Guides

All Cisco Wireless Controller software-related documentation

Cisco Catalyst 9800 Series Wireless Controller Data Sheets:

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

© 2025 Cisco and/or its affiliates. All rights reserved.

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

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2025 Cisco Systems, Inc. All rights reserved.