Release Notes for Cisco Catalyst 9800 Series Wireless Controller, Cisco IOS XE 17.18.x

Contents

Cisco Catalyst 9800 Series Wireless Controller, Cisco IOS XE 17.18.x

Cisco Catalyst 9800 Series Wireless Controllers comprise next-generation wireless controllers (referred to as controller in this document) built for intent-based networking. The controllers 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 9800-80, Catalyst 9800-40, and Catalyst 9800-L Wireless Controllers
  - Cisco Catalyst CW9800H1 and CW9800H2 Wireless Controllers
  - Cisco Catalyst CW9800M Wireless Controller
- Catalyst 9800 Series Wireless Controller for Cloud
- Catalyst 9800 Embedded Wireless Controller for a Cisco Switch

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.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 17.18.1

Product impact	Feature	Description
Software Reliability	RMI Serviceability Enhancement - Enhanced Gateway Reachability Monitoring	This feature improves visibility into gateway reachability and provides detailed statistics for ICMP, ARP, and ND probes. This feature also enables simplified troubleshooting, greater transparency, and more reliable diagnostics for High Availability, and RMI functionality. The following commands are introduced: • **show platform software rif-mgr chassis active r0 gateway-statistics** • **show platform software rif-mgr chassis active r0 resource-status** For more information, see High Availability.
	Software-Defined Application Visibility and Control (SD-AVC) Wireless Support with IPv6	From Cisco IOS XE 17.18.1 onwards, this feature extends the support for adding IPv6 SD-AVC controller or end-point address. The following platforms are supported: • Cisco Catalyst 9800 controllers-9800-40, 9800-80, 9800-L, 9800-CL, 9800-SW, CW9800M, CW9800H1, and CW9800H2. • Cisco Catalyst 9300/9400 switches in Fabric mode. • Cisco Wave 2, Wi-Fi 6/6E, and Wi-Fi 7 APs. SD-AVC IPv6 is not supported on Cisco Wireless AireOS Controllers, Cisco Embedded Wireless Controller on Catalyst APs, and Cisco Wave 1 APs. For more information, see Software-Defined Application Visibility and Control.
	Wireless AAA Authentication Survivability Cache	The Wireless AAA authentication survivability cache feature enhances the reliability of wireless client authentication by storing successful authentication results locally on the controller.

Product impact	Feature	Description
	Enhancement	This cache includes details such as the client's MAC address, username, hashed password, and Attribute-Value Pairs (AVPs) received from the RADIUS server. This feature is supported in both Local and FlexConnect central authentication modes. For more information, see Wireless AAA Authentication Survivability Cache.
	Ultra Reliable Wireless Backhaul (URWB) – Software Integration on the Controller	From Cisco IOS XE 17.18.1 onwards, the URWB technology is supported by Cisco Catalyst Controllers to provision and configure URWB devices from the controller. The URWB on Cisco Wireless is introduced as a beta feature and is intended for use by customers in testing and lab environments only. You should use caution when deploying the beta software. For more information about URWB AP support and country specific compliance, see the URWB on Cisco Wireless Use Case and Country Support document. For more information regarding URWB, see Ultra Reliable Wireless Backhaul.
	ThousandEyes Integration	In this release, ThousandEyes Integration is only a limited customer beta feature and is not supported by Cisco TAC. For beta testing help, contact the following mailer list: wireless-te-beta-feedback@external.cisco.com.
Ease of Use	Wi-Fi 7 Multi-Link Operation Support in Low-Power Mode for Cisco Wireless 9176 Series Access Points and Cisco Wireless 9178 Series Access Points	This feature ensures seamless multi-link operations (MLO) under constrained power conditions (low-power mode), providing improved flexibility and efficiency for network operations. In the 17.18.1 release, this feature is supported on the Cisco Wireless 9178 Series Access Points. For more information, see AP Management.
	Access Point Live Data and Packet Capture Support – NextTunnel to APs from Meraki Dashboard	In this release, the following command is added to help you view the Meraki connect information of a Cisco AP: **show ap name** *ap-name* **meraki connect**
	Per WLAN Wi-Fi 7 Toggle	From Cisco IOS XE 17.18.1 onwards, you can enable or disable Wi-Fi 7 (802.11be) on individual WLANs, allowing both Wi-Fi 7 and non-Wi-Fi 7 WLANs to run simultaneously in the same band. A default 802.11be profile is created for all bands, providing greater configuration flexibility. The following commands are introduced: • **wireless profile dot11be** • **mlo-group {24ghz | 5ghz | 5ghz-sec | 6ghz}** • **show wireless profile dot11be summary** • **show wireless profile dot11be detailed** • **show wireless tag policy detailed** • **show ap wlan summary** • **show ap name wlan dot11 6ghz** For more information, see Wi-Fi 7 Operations.
	AP MAC Authorization –	From Cisco IOS XE 17.18.1 onwards, you can enhance security by configuring AP MAC authorization with different delimiters, ensuring only authorized APs connect to

Product impact	Feature	Description
	Delimiter Support	the controller. This feature supports AP MAC registration through an external RADIUS server and lets you adjust AAA server group settings for efficient management. The functionality of the following commands is enhanced to support the AP MAC authorization use-case: • **mac-delimiter** • **subscriber mac-filtering security-mode** For more information, see Security.
	Traffic Filtering on AP by Source IP ACL	This feature enables APs to filter incoming data packets based on their source IP address. This is achieved when the controller pushes Access Control List (ACL) rules to the AP. For more information, see Traffic Filtering on AP by Source IP ACL.
	E-Label Display	From Cisco IOS XE 17.18.1 onwards, an E-Label display feature is introduced that allows you to view regulatory approvals for wireless APs digitally via the controller's GUI, eliminating the need for physical modifications. This feature supports Cisco Catalyst Wi-Fi 6, Wi-Fi 6E, and Cisco Wireless Wi-Fi 7 APs. For more information, see E-Label Display.
	Support for 6-GHz AFC for Canada	The Cisco Catalyst IW9167EH and IW9167I APs now support Standard Power mode using AFC in the -A (Canada) domain. These devices operate within the UNII-5, UNII-6, and UNII-7 frequency bands, covering a range of 5.925 GHz to 6.875 GHz. For more information, see AFC Support for 6 GHz Standard Power Mode.
Upgrade	Staggered AP Upgrade	This feature enables you to gain enhanced control over AP upgrades, minimizing network disruption. We provide new configurations that allow you to set up smaller batch sizes for upgrades. You can either have a staggered update of 1% batch size or upgrade APs one at a time (serial). The CLI and YANG models support these options, allowing you to manage upgrades effectively across various scenarios while maintaining optimal network performance. For more information, see Staggered AP Upgrade.
	Kernel Minidump and Trustzone Upgrade Support	This feature enhances control over minidump collection on Wi-Fi 7 (802.11be) APs. A new option has been added to limit the number of kernel core dump directories stored on the AP. The following command has been modified: **core-dump kernel dir-limit** Support has been added for the following access points: • Cisco Wireless 9178 Series Access Points • Cisco Wireless 9176 Series Access Points
Compliance	6 GHz Country Support for Bahrain, Macau, Oman, Pakistan, and Philippines	From Cisco IOS XE 17.18.1 onwards, Bahrain (BH), Macau (MO), Oman (OM), Pakistan (PK), and Philippines (PH) are added to the list of countries that support the 6-GHz radio band. For more information, see Countries and Regulations.
	Tier B/C/D/E Support for Cisco Wireless 9172I and 9172H Access	From Cisco IOS XE 17.18.1 onwards, numerous countries support the Cisco Wireless 9172I and 9172H APs, enhancing functionality and broadening deployment options worldwide.

Product impact	Feature	Description
	Points	For more information, see Countries and Regulations.
	Channel 144 Support for all Regulatory Domains	From Cisco IOS XE 17.18.1 onwards, Australia (AU), Brunei (BN), Fiji (FJ), Macao (MO), New Zealand (NZ), Papua New Guinea (PG), Singapore (SG), South Africa (ZA), and Thailand (TH) are added to the list of countries that support channel 144 for all regulatory domains. 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 17.18.1, the Cisco Wireless 9179F Series Wi-Fi 7 Access Points (CW9179F) are supported.

The Cisco Wireless 9179F Wi-Fi 7 APs are enterprise-class tri-band (2.4 GHz, 5 GHz, 6 GHz) access points. CW9179F APs are the industry's first enterprise-grade, Wi-Fi 7 certified high-density APs, made specifically for connecting large public venues and stadiums.

The APs support the CW-ANT-T-D3-N antennas. The CW-ANT-T-D3-N antennas are a single port, triple-band, directional antennas that support various deployment scenarios for both indoor and outdoor environments.

Note: For more information about all the countries supported for the APs, see Wireless LAN Compliance Lookup.

Change in behavior

Table 2. Change in behavior for Cisco Catalyst 9800 Series Wireless Controllers, Release 17.18.1

Feature	Description
Removal of the **ip proxy-arp** configuration command after reloading	The **ip proxy-arp** configuration is disabled by default under VLAN interfaces for the controller.
Removal of redundant counters from **show wireless stats ap name ap-name dot11 5GHz** command output	The output of the **show wireless stats ap name ap-name dot11 5GHz** command, displays two counters: **FailedCount** and **AckFailureCount**. Confirm if both counters are identical and remove one of them (preferably **AckFailureCount**, since it is not incremental.

Feature	Description
MAC addresses with hyphen, dot, and colon are converted while adding AAA device authentication	The APs support MAC address authorization using different delimiter formats to enhance the controller's support, which previously did not accept any delimiter.
Slot1 6-GHz radio profile support	Slot1 was only supported in 5-GHz radio profile. With the change in behavior, Slot1 is supported in 6-GHz radio profile.
AES ciphers removed from FIPS to establish mobility tunnel	By default, AES ciphers were allowed to establish mobility tunnels - TLS_ECDHE_RSA_AES128_GCM_SHA256, TLS_RSA_AES256_GCM_SHA384, and TLS_RSA_AES128_CBC_SHA. From Cisco IOS XE 17.18.1 onwards, when FIPS is enabled, only compliant cipher is supported for mobility tunnels - TLS_ECDHE_RSA_AES128_GCM_SHA256.
Deprecated ciphersuites in Cisco IOS XE 17.18.1: DHE-RSA-AES256-SHA256 and DHE-RSA-AES128-SHA	The following ciphersuites for DTLS connections are deprecated from Cisco IOS XE 17.18.1 onwards: • DHE-RSA-AES256-SHA256 • DHE-RSA-AES128-SHA
Changes in Inter-Release Controller Mobility (IRCM) Support between Cisco IOS XE and AireOS Wireless LAN Controller	Cisco IOS XE 17.18.1 is the last supported release for IRCM support between Cisco IOS XE and AireOS Wireless LAN Controller, with FIPS enabled. The non-FIPS mode will continue to be supported in Cisco IOS XE 17.18.1.
Configuration behavior discrepancy between CLI and YANG protocol regarding the creation of radio profile under the RF TAG	In the early development phase, radio profiles were not mapped by default. Later, the behavior changed to automatically link the default radio profile under an RF tag whenever a new RF tag was created. However, due to code limitations, a default radio profile cannot be created under the RF tag when the RF tag is created using NETCONF or WebUI. The radio profile must be linked manually while creating an RF tag using NETCONF or WebUI interfaces.

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 17.18.1

Bug ID	Description
CSCwn17412	FlexConnect local switching traffic becomes centralized randomly during WebAuth SSID, causing client gateway reachability loss
CSCwk26966	Cisco Aironet 3802 AP shows false radar detection on UNI-II only after upgrading to 17.12.3; not seen with Cisco Catalyst 9120 APs at same site
CSCwm58430	Cisco Catalyst 9115 APs become unresponsive and randomly reboot due to Beacon Stuck Reset Radio after upgrade to 17.12.4
CSCwn09549	Cisco Catalyst 9124 Mesh AP fails to join and intermittently disconnects from Cisco Catalyst 9124 Root AP due to dropped ADJ_RESPONSE packets
CSCwn10606	Cisco Catalyst 9120 AP intermittently fails to report RFID packets to controller, causing missing tag reports

CSCwn18885	Wi-Fi 6E/7 Cisco Catalyst 9136I AP reboots with Access Violation and reload reason 'unknown' without generating crash files
CSCwn44287	The CAPWAPd cores seen on multiple Cisco Wave 2 and Catalyst APs in AP-17.9.5-47 with core decode attached
CSCwn52205	IOX-APP starts before USB is detected when AP boots up after switch reload; extra logic needed to detect USB and create logical entry before starting IOX APP
CSCwn66225	Non-ROW AP transmits invalid TX power IE in beacons, breaking client connectivity for Ukraine country due to missing MAX Power table
CSCwn81268	IOX-APP starts before USB is detected when AP boots up after switch reload; needs increased system timeout for libvirtd
CSCwn82037	Cisco Catalyst 9120AP intermittently fails to report RFID packets to controller, resulting in missing tag reports
CSCwn83415	Cisco Catalyst 9124 MAP powered with 30W and joined to a Cisco Catalyst 9124 EWC RAP can enable Tri-Radio with EWC GUI, though Tri-Radio is not supported with 30W
CSCwn88092	Unable to view events for wireless clients in Client 360 section of Event Viewer, but events are visible under Issues and Events
CSCwn92652	Radio ucode crashes observed multiple times daily in 9105 APs operating in monitor mode
CSCwn96529	Unable to add country code "IN" for Cisco Catalyst C9136I-ROW AP in Site-Survey Mode, while other country codes work fine
CSCwo08220	Cisco Catalyst CW9162I-E AP disjoins from CONTROLLER when ECDHE-RSA DTLS ciphersuite is activated; not reproducible with DHE-RSA ciphersuite
CSCwo13129	UART msm kernel driver stopped working during DMA activity, resulting in kernel crash on Cisco Wireless 9176D AP in Local mode
CSCwo38789	Cisco Wireless 9176 AP faces wcpd crash due to memory leak in RRM module on version 17.15.2
CSCwo48539	Cisco Catalyst 9124 MAP powered with 30W and joined to a Cisco Catalyst 9124 EWC RAP can enable Tri-Radio with EWC GUI, even though Tri-Radio is not supported with 30W
CSCwo60793	IOX app channel down due to IOX app and CAF app state mismatch; CAF shows app running while IOX app is deactivated
CSCwo61838	Cisco Catalyst 9120 APs running 17.12.4 ESW13 crash due to OOM on GRPC process, with crash logs showing memory below threshold
CSCwo76564	Memory leak observed in ble_transport process on AP models Cisco Catalyst 9130, 9136, and 9166 running 17.18.0.32
CSCwp07242	Cisco Catalyst 9105 AP stops sending management frames over the air due to rxstuck, related to rx0 overflow error on 17.15.3
CSCwp27215	Cisco Catalyst Cisco Catalyst 9124 AP in Mesh mode shows poor iperf performance for wired clients in FlexConnect+Bridge setup
CSCwp34935	Cisco Wireless 9176 AP in site survey mode with non-US country code cannot enable radio, impacting wireless site surveys
CSCwp68123	802.11be APs downgrade DSCP 34 or AF41 QoS to Best Effort or Background for downstream traffic

	when over 20 clients are associated
CSCwn43094	Locally switched RLAN clients missing from controller client table when client is already associated as AP joins
CSCwn48978	AP configured for static IP continues to send ARP requests for DHCP IP address even after DHCP release packet
CSCwn55534	IP Theft observed on wireless controller when client receives a second DHCP offer after DORA, due to multiple DHCP servers
CSCwn61711	Cisco Catalyst 912X AP experiences PSM microcode watchdog fired and core dumps after about 12 days of continuous traffic
CSCwn66085	Increased radar detection DFS events on Cisco Catalyst 9166I-ROW APs after upgrading to 17.15.1
CSCwn73024	PKCS certificate enrollment fails to support special characters on WGB
CSCwn83397	Wired MAP client flapping between VLAN 0 and numbered native VLAN on RAP
CSCwn88567	Cisco Aironet 1815i AP: Syslog timestamps are not displayed correctly
CSCwn92047	Cisco Catalyst 9105 AP EWC does not start after reboot, when internal AP is configured as 802.x supplicant
CSCwn99070	Cisco Catalyst 9105 AP radio cores are not generated properly
CSCwo04476	Cisco Catalyst 9130AX AP encounters kernel panic
CSCwo05017	Unbounded /tmp causes OOM reset in Cisco Catalyst 9162 AP
CSCwo14129	COS AP crash due to soft lockup in 17.12.4
CSCwo16038	Cisco Catalyst 9124 AP WGB becomes unreachable connecting to Cisco Aironet 2800 Root AP when WMM is disabled
CSCwo34769	Cisco Catalyst 91xx AP in FlexConnect mode not advertising RSNxE in probe response, causing 4-way handshake failure for certain devices
CSCwo37756	Cisco Aironet 1815T AP unable to assign Internal DHCP IP address on LAN3 after upgrade to 17.12.4 and factory reset
CSCwo43801	Cisco AP duplicates DHCP request packets in FlexConnect mode with Central Switching WLAN, sending both to the server
CSCwo46493	Cisco Catalyst 9136 AP reboots during Dual Ethernet Failover when reconnecting wired 0 port, instead of seamless traffic transition
CSCwo53076	Syslog flooded with repeated " cli_h/avc" chatter messages during normal AP operation
CSCwo53891	Cisco Catalyst 91xx APs reboot with incorrect reason 'Controller Last Sent: Channel0 Detected' due to code mismatch between controller and AP
CSCwo72236	AP logs " RTNETLINK answers: No such file or directory" every 30 seconds, causing excessive syslog entries
CSCwo75325	Cisco Aironet 1832/1852 APs crash due to radio failures (Beacon Stuck) on 17.12.6 in SST testbed
CSCwo75806	AP intermittently delays reassoc response for over 200ms, causing clients to resend reassoc requests

CSCwo82821	Cisco Catalyst 9120AP encounters kernel panic at txq_hw_fill+0x394, leading to crash
CSCwo94810	IOT clients with TI Wi-Fi module (PIT truck) cannot associate with Cisco Catalyst 916x AP or Cisco Catalyst 9130 AP, or Cisco Wireless 917x AP
CSCwp39841	Cisco Catalyst 9120 AP crashes as kernel panic occurs due to NMI watchdog timeout
CSCwj80614	Clients are unable to connect due to assignment of IP address that is in use by stale client entry in device-tracking database in FlexConnect local switching
CSCwk58326	Controller sends multicast packets with previous WMI
CSCwk81946	Controller experiences kernel unresponsiveness due to TDL memory corruption
CSCwm67254	Accounting start and stop messages are missing CUI attributes
CSCwn11160	Controller running in High Availability in guest anchor sends traffic to the wrong tunnel after switchover for already connected clients
CSCwn36778	Cisco Catalyst 9800-80 controller displays low memory leak potentially in the 'ipv4_addr' field
CSCwn45380	Controller uses registry to initialize the trap queue length in SNMP
CSCwn46684	Controller unexpectedly reloads and becomes unresponsive during the upgrade process
CSCwn50926	Acct-Session-ID attribute missing from Access Request after client deletion, causing RADIUS server to drop requests and clients unable to connect
CSCwn51207	Cisco Catalyst 9800-40 controller becomes unresponsive after upgrade from 17.3.6 to 17.12.3, with crashes on High Availability Pair
CSCwn61980	Rogue AP is not displayed in UI or REST API when detected by dual band radio AP configured on same band
CSCwn77030	Controller does not process analytics action frames from MLD for MLO clients, resulting in missing PC Analytics information
CSCwn90360	Controller unable to start EAP process due to delayed packet transmission from AP, causing STA authentication issues
CSCwn90874	Guest anchor controllers show error when creating anchor-export-ACK in CWA with OWE scenario
CSCwn92477	Controller reboots during WNCd process due to assertion failure with invalid BSSID, causing kernel unresponsiveness
CSCwn92827	Secondary controller fails with rsync error after primary crash and cannot perform bulk sync, leading to outage
CSCwn98574	VRF name corruption causes client to get stuck at mobility while roaming, resulting in frequent disconnects after upgrade
CSCwo08428	COS-AP stale client entries cause AP to reach max number of clients per radio, affecting Cisco Catalyst 9120, 9130, and 9166 APs in local mode
CSCwo35645	NETCONF over SSH fails to return all records for wireless-client-oper, shows 'invalid XML' before completion
CSCwo37680	Controller initiates client deletion with CO_CLIENT_DELETE_REASON_DOT11_MAX_STA, even when

	AP client count is within limits
CSCwo39523	Cisco Wireless 9176I AP receives GPS/GNSS data but fails to provision country code, despite correct location info
CSCwo54553	Controller displays traceback messages when default-policy-tag APs block config change due to non-zero Ref-count
CSCwo61286	Audit session ID changes after inter-WNCd roam in CWA with PSK, causing authentication failures due to old session ID usage
CSCwo62157	Controller with CAPWAP enabled shows memory leak in tdl_mac_addr object under WNCd process
CSCwo62333	Cisco Catalyst 9800-L controller in FlexConnect/SDA fails to start MAB on association request if EAP_ID_RESP is missing
CSCwo68664	Cisco Catalyst 9800-L in SDA Wireless does not enforce EAP timeout, causing clients to remain stuck in MAB state
CSCwo80904	Cisco Catalyst 9164 and 9166 APs crash due to radio failures (Beacon Stuck) after controller upgrade to 17.15.3
CSCwp13687	Cisco Catalyst 9800-CL controller modifies script generating SSC to prevent RSA key issues impacting AP join
CSCwp26707	Controller fails to start L2 authentication for 11r clients with VLAN-persistent configured after upgrade to 17.12.5
CSCwp31397	DFS radar detection results in most APs being allocated the same channel and Tx power after mini-DCA calculation on the controller
CSCwp32113	Controller reloads due to kernel unresponsiveness with segmentation fault (11) in IGMPSN process on Catalyst 9800-80 controller
CSCvy53719	Cisco Catalyst 9800-80 displays stale, non-impacting " mce: [Hardware Error]" messages during IOS-XE 17.x boot-up
CSCwi48178	Cisco Catalyst 9800-40 shows WNCd SafeC Validation error for memcmp_s: dmax, resulting in tracebacks
CSCwm09484	WNCD crashed in CiscoSSL code on controller
CSCwn31021	Controller fails to correctly format AP Name and VLAN ID in Option 82; VLAN is truncated, and delimiter is misrepresented
CSCwn33501	Controller does not give output for #show ap summary sort name command on 9800-40/80 running 17.12.4
CSCwn45000	No output for " show ap name <AP Name> wlan dot11 5ghz" command when 802.11be and 5G radio policy enabled
CSCwn45670	Controller GUI FlexConnect configuration page fails to display after IOS XE 17.15.1 upgrade, showing " Operation GET Failed"
CSCwn85374	Memory usage in CloudM process increases over time until BinOS memory is exhausted
CSCwn94159	Controller with 6 GHz APs sees frequent DCA-induced channel bandwidth changes, causing client deletions and connectivity issues

CSCwn94511	The 'factory-reset all' command behaves as if secure option is enabled, deleting OS and configuration, leading to ROMMON boot
CSCwn96363	Remove redundant counters from " show wireless stats ap name <ap-name> dot11 5GHz" output for easier monitoring
CSCwo07767	Controller's active chassis gets stuck in active recovery state on 17.12.4 after RP/RMI connectivity flaps
CSCwo09824	Cisco Wireless 9176 AP is unable to join controller after GUAP process; controller repeatedly closes connection
CSCwo19011	Controller observes unexpected SISF reboot with WNCD core
CSCwo20395	Controller's rogue classification rules not applying configured classifications to detected devices
CSCwo29017	The wncmgrd kernel unresponsiveness after issuing 'show ap config slots' on Controller-80-K9 running 17.12.4
CSCwo30925	Cisco Wi-Fi 6 and above APs do not support disabling WMM on radios with 11n/ac/ax, disabling WMM causes client connectivity failures
CSCwo33572	Failed to collect RA tracing logs on Cisco IOS XE Release 17.9.5 using standard or alternate methods
CSCwo52310	Wireless cloud service consumes 100% CPU during geolocation derivation in large scale setups with many APs and CDP neighbors
CSCwo53638	Client error: High Availability data path setup failed on standby device in RA trace logs
CSCwo64967	Mobility tunnel with data-link encryption intermittently disconnects when WMI address fourth octet is 255
CSCwo67294	Controller unexpectedly reloads due to corrupted value in IGMP Layer 2 Snooping process, leading to segmentation fault
CSCwo67413	Controller pushes aWIPS profiles from FQDN-only setup for intrusion detection
CSCwo86312	Controller shows mismatch between client counts from " show client" commands and SNMP walk totals for WLANs
CSCwo89539	Controller unexpectedly reloads when adding " location civic-location-id" to multiple interfaces
CSCwo98083	Access points are unreachable in inventory on Cisco Connected Cloud 2.3.7.9 due to incorrect TDL value update
CSCwo98644	RRM does not update default channel or power levels when controller is IPv6-only, adding IPv4 restores normal operation
CSCwp03988	Controller reloads unexpectedly due to unsuccessful copy of the MAC address while configuring AP channel and power levels
CSCwo41248	Controller displays misleading error when configuring two radios on same UNII band (100-144). Only one 5-GHz radio is allowed in this band
CSCwp06711	Controller overwrites static AP location with Location Tag after upgrade, impacting DHCP Option 82 and client IP assignment
CSCwp12959	Wireless clients may be excluded after one authentication failure or not excluded as expected, contrary to documentation

CSCwp21187	Controller unexpectedly reboots due to mDNS packet being punted from data-plane to control-plane on version 17.15.03
CSCwp25552	BSSID-mac dispatched as 00:00:00:00:00:00 for slot 1 WLAN 1 via xpath, not reflected in **show ap wlan** summary
CSCwp59171	Users unable to add allowed user on Lobby admin page, receiving " Error in configuring Allowed users" message
CSCwp93598	Memory leak found in controller process related to specific database string, recurring after upgrading to 17.12.5

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 Catalyst 9800 Series Wireless Controllers, Release 17.18.1. An issue that is open for an earlier release and is still unresolved applies to all future releases until it is resolved.

Table 4. Open issues in Cisco Catalyst 9800 Series Wireless Controllers, Release 17.18.1

Bug ID	Description
CSCwp80992	L2 traffic does not pass and local ethernet traffic not forwarded in P2P fixed, due to STP loop detection
CSCwo53622	IW9167EH, IW9165, CW9178I wired interface MTU in show command mismatch from actual value
CSCwo88306	High packet loss observed when 5 or more mobility clients are present with mixed QoS traffic
CSCwo94611	The number of APs connected does not get updated when an AP goes down
CSCwo95065	Incorrect AP role displayed in URWB statistics for second coordinator in P2MP topology
CSCwo95337	Multiple coordinator topology is not displayed properly in monitoring
CSCwo97129	Selection of incompatible AP mode (sniffer, monitor, bridge) is allowed when URWB is active
CSCwo98652	AP slot 1 radio in URWB mode, not allowing to change dual-radio mode, needed for tri-radio configuration
CSCwp21963	Number of URWB Ethertype and channel list entries in a radio profile are not validated
CSCwp26522	IW9167E slot2 as client serving on 5G band hit beacon stuck
CSCwp39875	Coordinator cannot join the controller when the AP switches from FlexConnect mode to local mode
CSCwp63972	Multicast from an upstream network is not received by Wi-Fi client in central switching on access point over URWB link
CSCwp84004	AP fails to validate and reject empty Cluster ID, leading to continuous crashes after reload
CSCwp93224	Maximum controller network-key length should be 64 for brownfield compatibility instead of 63
CSCwq20961	Mobility clients with multiple mobiles occasionally do not join controller using MPO CoS 6

Bug ID	Description
CSCwo90297	Flex Wi-Fi client associated to the secondary mobile of vehicle fail to ping infra side client
CSCwq02929	Show AP command not working for 5ghz with slot 0
CSCwk79990	Cisco Catalyst 9800-L encounters kernel unresponsiveness due to Intel Reset Request
CSCwo66875	Cisco Catalyst 9130AXI Access Points crash randomly during Access Point renaming
CSCwp14628	Cisco Aironet 3800 Access Points display client authentication issue after Access Point migration to controller running version 17.15.3
CSCwp20385	Cisco Catalyst 9136 Access Point wired 0 interface gets stranded and RX packets are not processed
CSCwp20530	Controller does not forward downstream packets to wireless client after switchover
CSCwp21518	Cisco Catalyst 9164I and Cisco Catalyst IW9167IH Access Points experience Radio Firmware crash
CSCwp65769	Wave 2 Access Points using fast transition with 802.1X authentication send incorrect M2 message during re-key on session timeout
CSCwq12151	Cisco Catalyst 9130AXI Kernel Panic
CSCwq12607	Cisco Catalyst 9120AX Access Point unexpected reload due to radio firmware beacon TX stuck
CSCwq23255	COS Access Point Workgroup Bridge does not forward multicast traffic for groups that did not send IGMP join, like OSPF
CSCwq27429	Version 17.9.3 – Neighbor Access Points not seen on Cisco Catalyst 9800-40 even though Access Point populates neighbor details
CSCwq47324	Fabric Mode Access Point drops downstream fragmented traffic
CSCwn55495	Cisco Catalyst 9800-40 controller displays random CPU spikes on EZMAN
CSCwo49512	Access Points do not maintain RF Load Balancing after High Availability or SSO switchover on version 17.12.4 with Cisco Catalyst 9800 Wireless LAN Controller
CSCwo92511	Controller has inconsistent default MTU settings for mobility tunnels
CSCwp39409	Controller reboots unexpectedly due to assertion failure in WNCd process
CSCwp60602	Version 17.9.3 – Slot values show " ok" for status description in REST API response body
CSCwp61261	SNMP OID sends a different trap each time it is queried
CSCwp63176	Cisco IOx app channel down due to state mismatch between IOx and CAF apps on Cisco Catalyst 9136 Access Point
CSCwp95190	Cisco Catalyst 9800 controller unable to handle new client connections due to memory failure
CSCwq23630	Clients stuck in IP-LEARN state for extended period and not active on Access Point
CSCwq31446	Configuration syntax for FlexConnect site tags is out of order; " no local site" not specified before flex site configurations

Bug ID	Description
CSCwq33181	Controller does not advertise 5A03BA0000 in 802.11 beacon frames when configuring " open-roaming-oi allow-all beacon"
CSCwq34135	Cisco Wireless 9178 AP do not take clients on 2.4-GHz probe requests from wireless clients
CSCwq44728	Controller does not form HA after ISSU and APSP installation due to version mismatch
CSCwq46069	Only one AP's client appears when querying client-list-details-per-ap without filters, despite multiple clients on other APs

Known issues

The following are the known issues for Cisco IOS XE 17.18.1:

SNMP authentication failure on Cisco Catalyst CW9800M, CW9800H2, or CW9800H1 hardware platforms

Upgrading the controller software on Cisco Catalyst CW9800M, CW9800H2, or CW9800H1 hardware platforms from 17.14.1, 17.15.1, or 17.15.2 release to any later release:

- Causes SNMP user authentication failure.
- After the upgrade, the mobility tunnels go down and do not re-establish.

Conditions:

Regarding the SNMP issue:

- The controller is hosted on Cisco Catalyst CW9800M, CW9800H2, or CW9800H1, with the 17.14.1, 17.15.1. or 17.15.2 image loaded on the controller.
- SNMP users are configured on the controller and static SNMP engine ID is not configured.
- An upgrade is made to a later release, such as 17.15.3.

Regarding the mobility issue:

- The controller is hosted on Cisco Catalyst CW9800M, CW9800H2, or CW9800H1, with 17.14.1, 17.15.1. or 17.15.2 image loaded on the controller.
- Mobility tunnels are already established, and mobility MAC is not configured. If High Availability is configured, the mobility MAC is already configured for it to work.
- An upgrade is made to a later release, such as 17.15.3.

Workaround:

For the SNMP issue, before you upgrade, follow these steps:

1. Remove all the configured SNMP users.

   For example,

   ```
   Device(config)# no snmp-server user user-name grp v3
   ```

2. Configure static engine ID.

   For example,

   ```
   Device(config)# snmp-server engineID local 800000090300F8E94F0077FF
   ```

3. Configure the SNMP users that were removed earlier.

   For example,

   ```
   Device(config)# snmp-server user user-name grp v3 auth sha cisco1234 priv aes 128
   cisco1234
   ```

4. Verify that the engine ID has been updated for all users.

   For example,

   ```
   Device# show snmp user
   User name: user-name
   Engine ID: 800000090300F8E94F0077FF <<<<<<<<<
   storage-type: nonvolatile active
   Authentication Protocol: SHA
   Privacy Protocol: AES128
   Group-name: grp
   ```

5. Perform the upgrade.

For mobility tunnel issue, follow these steps:

1. Configure mobility MAC address on the controller being upgraded.

   ```
   Device# config terminal
   Device(config)# wireless mobility mac-address mac-address
   ```

2. Update the peer mobility MAC addresses accordingly on each peer controller.

   ```
   Device# config terminal
   Device(config)# wireless mobility group member mac-address mac-address
   ```

   Momentarily, the mobility tunnel will go down.

3. Perform the upgrade.

GNSS-based APs do not use geolocation derivation from neighboring APs after upgrade

GNSS-based APs automatically attempt to obtain a GPS lock after the controller and APs reboot, as long as a GPS module is connected.

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 17.18.1

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 17.18.1	3.4 3.3 3.2 3.1 3.0 * all with latest patches	3.10 MR	8.10 latest MR 8.5 latest MR	See Cisco Catalyst Center Compatibility Information.	11.0.0

GUI system requirements

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

Table 6. Hardware requirements

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:

- 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.x, 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.x.
- For images: If upgrading from 17.9.6 or lower, 17.12.4 or lower, or 17.15.1 or lower, to 17.18.x, 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.x 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>
    ```

  - 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.
- 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
```

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.x

Table 7. Upgrade Path to Cisco IOS XE Dublin 17.18.x

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.x.
16.11.x	–	Upgrade first to 16.12.5 or 17.3.x and then to 17.18.x.
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.x.	Upgrade first to 17.3.5 or later or 17.6.x or later, and then to 17.18.x.
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.x.	Upgrade first to 17.3.5 or later and then to 17.18.x.
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.x.	Upgrade first to 17.3.5 or later and then to 17.18.x.
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.x.	Upgrade directly to 17.18.x.
17.3.4c or later	Upgrade to 17.9.6 or later or 17.12.x or later, and then to 17.18.x.	Upgrade directly to 17.18.x.
17.4.x	Upgrade first to 17.6.x and then to 17.18.x.	Upgrade directly to 17.18.x.

Current software	Upgrade path for deployments with 9130 or 9124	Upgrade path for deployments without 9130 and 9124
17.5.x	Upgrade first to 17.6.x and then to 17.18.x.	Upgrade directly to 17.18.x.
17.6.x	Upgrade to 17.9.6 or later or 17.12.x or later, and then to 17.18.x.	Upgrade directly to 17.18.x.
17.7.x	Upgrade to 17.9.6 or later or 17.12.x or later, and then to 17.18.x.	Upgrade directly to 17.18.x.
17.8.x	Upgrade to 17.9.6 or later or 17.12.x or later, and then to 17.18.x.	Upgrade directly to 17.18.x.
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.x.	Upgrade directly to 17.18.x.
17.9.6 or later	Upgrade directly to 17.18.x	Upgrade directly to 17.18.x.
17.10.x	Upgrade to 17.12.x or later, and then to 17.18.x	Upgrade directly to 17.18.x.
17.11.x	Upgrade to 17.12.x or later, and then to 17.18.x	Upgrade directly to 17.18.x.
17.12.x	Upgrade directly to 17.18.x.	Upgrade directly to 17.18.x.
17.13.x	Upgrade directly to 17.18.x.	Upgrade directly to 17.18.x.
17.14.x	Upgrade directly to 17.18.x.	Upgrade directly to 17.18.x.
17.15.x	Upgrade directly to 17.18.x.	Upgrade directly to 17.18.x.
17.16.x	Upgrade directly to 17.18.x.	Upgrade directly to 17.18.x.
17.17.x	Upgrade directly to 17.18.x.	Upgrade directly to 17.18.x.
8.9.x or any 8.10.x version prior to 8.10.171.0	Upgrade first to 8.10.171.0 or later, 17.3.5 or later, or 17.6.x or later, then to 17.9.6 or later or 17.12.x or later, and then to 17.18.x	Upgrade directly to 17.18.x.

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 17.18.x

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

- C9800-80-universalk9_wlc.17.18.x.SPA.bin
- C9800-40-universalk9_wlc.17.18.x.SPA.bin
- C9800-L-universalk9_wlc.17.18.x.SPA.bin

Image names (CW9800M, CW9800H1/CW9800H2)

- CW9800H-wlc-universalk9.17.18.x.SPA.bin
- CW9800M-wlc-universalk9.17.18.1.SPA.bin

Image names (9800-CL):

- **Cloud**: C9800-CL-universalk9.17.18.x.SPA.bin
- **Hyper-V/ESXi/KVM**: C9800-CL-universalk9.17.18.x.iso, C9800-CL-universalk9.17.18.x.ova
- **KVM**: C9800-CL-universalk9.17.18.x.qcow2
- **NFVIS**: C9800-CL-universalk9.17.18.x.tar.gz

Software installation commands

To install and activate a specified file, and to commit changes to be persistent across reloads, run the following command:

```
device# install add file filename [activate |commit]
```

To separately install, activate, commit, end, or remove the installation file, run the following command:

```
device# install ?
```

Note: We recommend that you use the GUI for installation.

Commands	Description
add file tftp: *filename*	Copies the install file package from a remote location to a device and performs a compatibility check for the platform and image versions
activateauto-abort-timer	Activates the file and reloads the device; the auto-abort-timer keyword automatically rolls back image activation
Commit	Makes changes that are persistent over reloads
rollback to committed	Rolls back the update to the last committed version
Abort	Cancels file activation and rolls back to the version that was running before the current installation procedure started
Remove	Deletes all unused and inactive software installation files

Licensing

Cisco wireless licenses

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

The Cisco wireless licenses consist of the following tiers:

- Cisco wireless essentials: The tier that provides fundamental features and functionalities that are essential to manage a network.
- Cisco wireless advantage: The tier that supports additional features and capabilities and includes all the essential capabilities in addition to the advanced capabilities to manage a network.

For more information, 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 17.18.1
Cisco Wireless Controller	See Supported hardware
Access Points	See Supported APs
Radio	• 802.11ac • 802.11a • 802.11g • 802.11n • 802.11be (Wi-Fi 7)
Security	Open, PSK (WPA2-AES), 802.1X (WPA2-AES) (EAP-FAST, EAP-TLS)
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

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)

Client type and name	Driver or software version
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
Dell Inspiron 13-5368 Signature Edition	Windows 10 Home (18.40.0.12)
FUJITSU Lifebook E556 Intel 8260 (Intel Dual Band Wireless-AC 8260 (802.11n))	Windows 8 (19.50.1.6)

Client type and name	Driver or software version
Lenovo Yoga C630 Snapdragon 850 (Qualcomm AC 2x2 Svc)	Windows 10 Home
Lenovo ThinkPad Yoga 460 (Intel Dual Band Wireless-AC 9260)	Windows 10 Pro (21.40.0)
Note: For clients using Intel wireless cards, we recommend that you 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
Apple iPhone 7 MN8J2LL/A	iOS 11.2.5
Apple iPhone 8	iOS 13.5
Apple iPhone 8 Plus	iOS 14.1

Client type and name	Driver or software version
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
Huawei P40	Android 10
LG v40 ThinQ	Android 9.0
One Plus 8	Android 11

Client type and name	Driver or software version
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
Vocera Smart Badges V5000	5.0.6.35
Zebra MC40	Android 4.4.4
Zebra MC40N0	Android 4.1.1

Client type and name	Driver or software version
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
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

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

Platform	Description
Cisco Catalyst CW9800M Wireless Controller	The Cisco Catalyst CW9800M Wireless Controller is the next generation Cisco Catalyst 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 Cisco Catalyst CW9800M Wireless 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.
Cisco Catalyst CW9800H1 and CW9800H2 Wireless Controllers	The Cisco Catalyst CW9800H1 and CW9800H2 Wireless Controllers are the next-generation Cisco Catalyst CW9800 Series 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.

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.

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

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
COLORCHIP-C040-Q020-CWDM4-03B	Supported	–	–	–	–	–
DWDM-SFP10G-30.33	Supported	Supported	–	–	–	–
DWDM-SFP10G-61.41	Supported	Supported	–	–	–	–
FINISAR-LR - FTLX1471D3BCL (The FINISAR SFPs are not Cisco specific and some of the features, such as DOM, may not work properly.)	Supported	Supported	Supported	–	–	–
FINISAR-SR - FTLX8574D3BCL	Supported	Supported	Supported	–	–	–
GLC-BX-D	Supported	Supported	Supported	Supported	Supported	Supported
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

SFP name	C9800-80-K9	C9800-40-K9	C9800-L-F-K9	CW9800H1	CW9800H2	CW9800M
GLC-SX-MMD	Supported	Supported	Supported	Supported	Supported	Supported
GLC-T	Supported	–	–	–	–	–
GLC-TE	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	–	–	–	–	–
QSFP-40G-ER4	Supported	–	–	–	Supported	–
QSFP-40G-LR4	Supported	–	–	–	Supported	–
QSFP-40G-LR4-S	Supported	–	–	–	Supported	–
QSFP-40G-CSR4	–	–	–	–	Supported	–
QSFP-40G-SR4	Supported	–	–	–	Supported	–
QSFP-40G-SR4-S	Supported	–	–	–	Supported	–
QSFP-40GE-LR4	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-CUO-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	–

SFP name	C9800-80-K9	C9800-40-K9	C9800-L-F-K9	CW9800H1	CW9800H2	CW9800M
QSFP-H40G-AOC15M	–	–	–	–	Supported	–
QSFP-H40G-AOC20M	–	–	–	–	Supported	–
QSFP-H40G-AOC25M	–	–	–	–	Supported	–
QSFP-H40G-AOC30M	–	–	–	–	Supported	–
SFP-10G-AOC10M	Supported	Supported	–	–	–	–
SFP-10G-AOC1M	Supported	Supported	–	Supported	Supported	Supported
SFP-10G-AOC2M	Supported	Supported	–	Supported	Supported	Supported
SFP-10G-AOC3M	Supported	Supported	–	Supported	Supported	Supported
SFP-10G-AOC5M	Supported	Supported	–	Supported	Supported	Supported
SFP-10G-AOC7M	Supported	Supported	–	Supported	Supported	Supported
SFP-10G-ER	Supported	Supported	–	Supported	Supported	Supported
SFP-10G-LR	Supported	Supported	Supported	Supported	Supported	Supported
SFP-10G-LR-S	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
SFP-10G-SR-S	Supported	Supported	Supported	Supported	Supported	Supported
SFP-10G-SR-I	–	–	–	Supported	Supported	Supported
SFP-10G-SR-X	Supported	Supported	Supported	–	–	–
SFP-10G-ZR			–	–	–	–
SFP-10G-ZR-I	–	–	–	Supported	Supported	Supported
SFP-10G-T-X	–	–	–	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 name	C9800-80-K9	C9800-40-K9	C9800-L-F-K9	CW9800H1	CW9800H2	CW9800M
SFP-10/25G-BXD-I	–	–	–	Supported	–	Supported
SFP-10/25G-BXU-I	–	–	–	Supported	–	Supported
SFP-H25G-CU1M	–	–	–	Supported	–	Supported
SFP-H25G-CU5M	–	–	–	Supported	–	Supported
SFP-25G-AOC1M	–	–	–	Supported	–	Supported
SFP-25G-AOC2M	–	–	–	Supported	–	Supported
SFP-25G-AOC3M	–	–	–	Supported	–	Supported
SFP-25G-AOC5M	–	–	–	Supported	–	Supported
SFP-25G-AOC7M	–	–	–	Supported	–	Supported
SFP-25G-AOC10M	–	–	–	Supported	–	Supported
SFP-H10GB-ACU10M	Supported	Supported	Supported	Supported	Supported	Supported
SFP-H10GB-ACU7M	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	–	–	–
SFP-H10GB-CU2M	Supported	Supported	Supported	Supported	Supported	Supported
SFP-H10GB-CU3M	Supported	Supported	Supported	Supported	Supported	Supported
SFP-H10GB-CU5M	Supported	Supported	Supported	Supported	Supported	Supported
SFP-H10GB-CU1-5M	Supported	Supported	–	Supported	Supported	Supported
Finisar-LR (FTLX1471D3BCL)	–	–	Supported	Supported	Supported	Supported
Finisar-SR (FTLX8574D3BC)	–	–	–	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
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

Source	Destination	Protocol	Destination port	Source port	Description
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
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 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 9172 (I) Series Wi-Fi 7 Access Points • Cisco Wireless 9172 (H) 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)

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 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

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