Release Notes for Cisco Catalyst 9800 Series Wireless Controller, Cisco IOS XE 17.18.4a

Contents

Cisco Catalyst 9800 Series Wireless Controller, Cisco IOS XE 17.18.4a 3
New software features 3
Notice of upcoming changes in the Cisco IOS XE 17.18.4a release and beyond 3
Resolved issues 5
Open issues 7
Compatibility 9
Supported hardware 24
Related content 34
Communications, services, and additional information: 35
Legal information 35

© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Catalyst 9800 Series Wireless Controller, Cisco IOS XE 17.18.4a

Cisco Catalyst 9800 Series Wireless Controllers comprise next-generation wireless controllers (referred to as controller in this document) built for intent-based networking.

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

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

This document describes the new software features that were introduced or enhanced, change in behavior, issues, supported hardware, and so on, for Cisco IOS XE 17.18.4a.

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 17.18.4a

Product impact	Feature	Description
Ease of Use	AP gRPC Connection Serviceability	AP gRPC Connection Serviceability improves operational visibility into the lifecycle and health of gRPC connections originating from wireless access points. By exposing connection state, failure reasons, retry behavior, and relevant diagnostics, the feature enables customers and support teams to identify connectivity problems faster, reduce dependence on debug-heavy workflows, and shorten service-restoration time. Its product value is primarily measured through lower diagnostic effort, faster incident resolution, and fewer escalations.

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.

Notice of upcoming changes in the Cisco IOS XE 17.18.4a 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.

© 2026 Cisco and/or its affiliates. All rights reserved.

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.

  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.

© 2026 Cisco and/or its affiliates. All rights reserved.

- **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**:

  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 2. Resolved issues in Cisco Catalyst 9800 Series Wireless Controllers, Release 17.18.4a

Bug ID	Description
CSCwt87294	mDNS Cache-Flush behavior not consistent
CSCwv81329	After ISSU upgrade WLAN Profile missing in 11ax VAP list and present only on 11be list
CSCwu04279	System instability and potential service disruption after invalid GPM load
CSCwp27601	Radio 1 FW crash observed while running longevity with ~20+ clients on 3802 AP

© 2026 Cisco and/or its affiliates. All rights reserved.

Bug ID	Description
CSCwr94814	9115 AP unexpected reload due to Radio firmware beacon TX stuck
CSCws68479	Missing support for certain bands and channels in wifi6/6e regdb
CSCwt19011	9166 17.15.4b AP in SDA mode not forwarding IPv4 ARP upstream or other IPv4 packets after DHCP
CSCwt19092	9179 running 17.18.2 reporting more than 4 DFS in less than 1 hour
CSCwt19490	9800 WLC: Stale client IP used in RADIUS accounting causes ISE IP\u2013SGT/SXP overwrite
CSCwt33908	PHY OFF error assert causing AP crash during longevity tests
CSCwt50389	Ascom Myco2 phones are not able to connect to 9176 APs due to EAP_ID_REQ or M2 not acked by AP
CSCwt65349	CW9172I AP crashes with ar_wal_mlo_ipc.c assert and watchdog panic
CSCwt78829	Memory Leak in python Process on Wireless Active Testing (WAT) AP with TEAgent IOx Application
CSCwt80663	Tier E countries + RAF not working
CSCwt88263	Pre-commit CDT failure-12 | AP crash kmem_cache_free+0x150/0x2c8
CSCwt92054	9176 not processing CTS packets when configured with datarate 36M and channel width 40M or higher
CSCwu04935	9178: AP continuously reloading with \" NSS CAPWAP tunnel creation failed\" log when vlan-tag is enabled
CSCwu06998	9120 kernel panic crash at cpktq_pdeq / pktq_pdeq running 17.18.2
CSCwu08256	AP unable to join back to the controller after dropping from the controller
CSCwu18918	AP not completing DHCPv6 after dropping from the controller
CSCwu24663	9176 APs crash files with no stack traces on 17.18.3
CSCwo16038	Cisco Catalyst 9124 AP workgroup Bridge becomes unreachable connecting to Cisco 2800 Root Access Point when Wi-Fi Multimedia (WMM) is disabled
CSCwp27756	Some 6GHz WLANs don't come up after reconnecting to controller
CSCwr97166	Regdb update to fix all issues caught using new scripts
CSCws03721	9120/9115/9105 AP does not ACK frames sent from iOS devices follow up of CSCwj91255
CSCwt47537	Kernel: BUG: KFENCE: memory corruption in | use-after-free write in | use-after-free read in. In ap version 17.12.6.28
CSCwt51709	COS APs initiate DHCP process even when static IP is configured, causing intermittent DHCP Fallback issues
CSCwt68617	FT-SAE in Flex Standalone mode does not allow client association
CSCwt77092	AP - KFENCE memory corruption events lead to RCU stalls and HW watchdog reset
CSCwt77136	continuous KFENCE IPv6 MLD memory corruption leads to RCU stalls and HW watchdog reset

© 2026 Cisco and/or its affiliates. All rights reserved.

Bug ID	Description
CSCwu17010	9120 AP forwards HE PHY Capability bitset with 40 / 80 MHz supported when configured 20 MHz only channel width
CSCwu04310	Fragmented packets in CAPWAP mobility tunnel led to dataplane crash on CW9800-M/H platforms
CSCws23072	RRM Crashes and tracebacks observed on CW9800 Platform
CSCwt07093	APs not being able to connect due capwap messages being queued due to fragments drop
CSCwt13732	WNCD process is getting terminated unexpectedly, causing WLC to crash (Critical process wncd has failed (rc 0))
CSCwt26718	eCA upgrade operation failed due to non response from wncmgrd.
CSCwt52815	WLC fails to update associated Channel width for client after it is changed on AP radio.
CSCwt94577	CW9800-M/H wireless controller may reload due to CPP datapath crash in CAPWAP mobility path
CSCwt98619	CW9800L PID is missing in ISSU comp_matrix file

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 17.18.4a. An issue that is open for an earlier release and is still unresolved applies to all future releases until it is resolved.

Table 3. Open issues in Cisco Catalyst 9800 Series Wireless Controllers, Release 17.18.4a

Bug ID	Description
CSCwo60803	9167 WGB cannot pass traffic after PSK SSID association
CSCwk79990	9800-L encounters kernel unresponsiveness due to IntelResetRequest
CSCws42581	Memory corruption in L2 multicast while handling dynamic multicast router ports and group
CSCwt91818	C9800 WLC crash during APSP installation
CSCwu14554	9105/9172H RLAN AP not passing multicast traffic for central switching
CSCwu58946	802.1X Authentication Failure - EAP Request Identity Not Forwarded by AP over the air
CSCwu92593	AP 9176I IPV6 RA packet drop using SLAAC
CSCwu96599	9120 AP not transmitting downlink pkt to IW9167E
CSCwv27458	AP crashed due to kernel panic with different PC and LR
CSCwv33856	WLC experiences a WNCD process leak due to CAPWAP messages
CSCwv38974	9800 crash due to unexpected values in 6ghz channel power payload

© 2026 Cisco and/or its affiliates. All rights reserved.

Bug ID	Description
CSCwv40106	aWIPS functionality broken post upgrade to Release 17.15.5
CSCwv41569	SSID Broadcast Failure with Overnight Calendar Profile Schedule
CSCwq11176	SafeC Validation traceback @ewlc_app_safec_constraint_handler observed on 9800-80 with V17_18_01PRD16
CSCwu20316	9800 showing dot1x pmf client deauth as CLIENT_DELETE_REASON_CLIENT_EAP_TIMEOUT_FAILURE
CSCwu24905	CW9166 COS AP crash due to: NSS firmware crashed
CSCwu25771	C916x nssmgrctl driver failure during bootup - setup_tunnel: tunnel 0 destroy failed 116
CSCwu34251	The WLC is not reporting AP neighbors
CSCwu42825	Wifi7 syslogs are generating in WLC in large numbers
CSCwu50245	9130 has beacon rate programmed to 6 Mbps despite 5 GHz legacy rates excluding 6 Mbps on one of the slots, causing DOT11_STATUS_DENIED_RATES
CSCwu50455	AP C9124AXE shows solid amber LED
CSCwu52741	C9120 COS AP crash PC is at rhb_init_rfic_mdata_ptrs LR is at rhb_init_cfg80211
CSCwu52776	C9120 COS AP crash due to: RHL Probe failure, reboot to recover
CSCwu78805	Unexpected reboot due to Punt keep alive failure WLC 9800 Switch
CSCwu86004	9800 deauthenticates client when receiving DHCP RELEASE from client.
CSCwu98499	9105AW WGB mode, ports 1/2/3 do not go up in 17.15/17.18
CSCwv03367	9172I APs on 17.18.3 radios crashing regulary
CSCwv20470	Clients obtain an IP address from the VLAN mapped under the Policy Profile instead of the VLAN assigned through AAA Override , triggered by roaming
CSCwv22511	Client detail for some Associated Client doesn't show info element when using Cisco Spaces Connector
CSCwv31549	Incorrect Client Exclusion reasons on bsnStationBlacklistingReasonCode traps
CSCwv38891	FRA shows as managed by DNAC even when AI-RRM is not configured.
CSCwv38912	XOR radio is being switched between monitor and client serving mode using client-aware FRA when its not configured
CSCwv40607	WAT reports wrong DNS IPs from previous connections in ThousandEyes

© 2026 Cisco and/or its affiliates. All rights reserved.

Compatibility

Compatibility matrix

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

Table 4. Compatibility Matrix for Cisco Catalyst 9800 Series Wireless Controllers, Release 17.18.4a

Cisco Catalyst 9800 Series Wireless Controller Software	Cisco Identity Services Engine	Cisco AireOS-IRCM Interoperability	Cisco Catalyst Center	Cisco CMX
IOS XE 17.18.4a	3.4 3.3 3.2 3.1 3.0 * all with latest patches	8.10 latest MR 8.5 latest MR	See Cisco Catalyst Center Compatibility Information.	11.1.1

Software requirements

Operating Systems:

- Windows 10 or later
- macOS X 10.11 or later

Browsers:

- Google Chrome: Version 59 or later (on Windows and Mac)
- Microsoft Edge: Version 40 or later (on Windows)
- Safari: Version 10 or later (on Mac)
- Mozilla Firefox: Version 60 or later (on Windows and Mac)

  Note that Firefox version 63.x is not supported.

The controller GUI uses Virtual Terminal (VTY) lines for processing HTTP requests. At times, when multiple connections are open, the default number of VTY lines of 15 set by the device might get exhausted. Therefore, we recommend that you increase the number of VTY lines to 50.

To increase the VTY lines in a device, run the following commands in the following order:

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

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

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

© 2026 Cisco and/or its affiliates. All rights reserved.

Before you upgrade

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

- Customers planning to upgrade using ISSU should review the known defect CSCwv81329 before proceeding. Other upgrade methods are not affected by this issue.
- To ensure a smooth upgrade and prevent potential boot loop issues with APs, review the following Field Notice and technical documentation. It is critical to complete these actions prior to initiating your upgrade.
    - FN74383: Field Notice
    - Validate and Recover Catalyst APs on 17.12
- **Upgrading from Cisco IOS XE 17.18.3 to 26.1.1**:
  WLANs configured with WPA3 Enterprise (non-SuiteB) using the GCMP-256 cipher, which are currently supported on Wi-Fi 7 in release 17.18.3, will be administratively shut down upon upgrading to release 26.1.1. This occurs because the GCMP-256 cipher is not supported for these specific WLAN types in version 26.1.1. Consequently, affected WLANs will cease to broadcast and will not be operational immediately following the upgrade.

  The affected WLAN types are:
    - WPA3 Enterprise (802.1X SHA256) with GCMP-256 cipher
    - WPA3 FT (802.1X) with GCMP-256 cipher

  Workaround: To restore service for these WLANs post-upgrade, you must manually remove the GCMP-256 cipher configuration from the affected WLANs. Once the configuration is removed, the WLANs can be brought back to an operational state.

  Ensure validation of cipher compatibility before upgrading to avoid service disruption.
- 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 or higher, the controller WebUI does not support images greater than 1.5 GB.

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

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

  For more information, see CSCwm08044 and CSCwm07499.

© 2026 Cisco and/or its affiliates. All rights reserved.

- 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>
```

    - Restart the CAPWAP process using **capwap ap restart** command. This allows the AP to use the correct backup image after the restart (reload is not required.)

```
Device# capwap ap restart
```

    The AP will lose connection to the controller during the join process. When the AP joins the new controller, it will see a new image in the backup partition. So, the AP will not download a new image from the controller.
- The use of MTU lower than 1500 on G0 (OOB) interface that may cause fragmentation for RADIUS packets for client authentication, is not supported.
- While upgrading to Cisco IOS XE 17.3.x and later releases, if the **ip http active-session-modules none** command is enabled, you will not be able to access the controller GUI using HTTPS. To access the GUI using HTTPS, run the following commands in the order specified below:

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

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

© 2026 Cisco and/or its affiliates. All rights reserved.

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.
- The Cisco Centralized Key Management (CCKM) feature was deprecated in Cisco IOS XE 17.10.x but currently remains supported. However, support for CCKM will be removed in a future release. Therefore, we recommend that you migrate to Fast Transition (FT) with 802.1X authentication and validate the configuration with supported key caching mechanisms.
- To migrate public IP address from 16.12.x to 17.x. ensure that you configure the service internal command. If you do not configure the service internal command, the IP address does not get carried forward.
- RLAN support with Virtual Routing and Forwarding (VRF) is not available.
- Unidirectional Link Detection (UDLD) protocol is not supported.
- When you encounter the SNMP error SNMP_ERRORSTATUS_NOACCESS 6, it means that the specified SNMP variable is not accessible.

© 2026 Cisco and/or its affiliates. All rights reserved.

- 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 17.18.4a

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 5. Upgrade Path to Cisco IOS XE Dublin 17.18.4a

Current software	Upgrade path for deployments with 9130, 9124, or 916x	Upgrade path for deployments without 9130 and 9124
16.10.x	– **Note**: The Cisco Catalyst 9130 and 9124 APs are not supported in 16.10.x and 16.11.x releases.	Upgrade first to 16.12.5 or 17.3.x and then to 17.18.4a.
16.11.x	–	Upgrade first to 16.12.5 or 17.3.x and then to 17.18.4a.
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 17.18.4a.	Upgrade first to 17.3.5 or later or 17.6.x or later, and then to 17.18.4a.
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 17.18.4a.	Upgrade first to 17.3.5 or later and then to 17.18.4a.

© 2026 Cisco and/or its affiliates. All rights reserved.

Current software	Upgrade path for deployments with 9130, 9124, or 916x	Upgrade path for deployments without 9130 and 9124
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 17.18.4a.	Upgrade first to 17.3.5 or later and then to 17.18.4a.
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 17.18.4a.	Upgrade directly to 17.18.4a.
17.3.4c or later	Upgrade to 17.9.6 or later or 17.12.x or later, and then to 17.18.4a.	Upgrade directly to 17.18.4a.
17.4.x	Upgrade first to 17.6.x and then to 17.18.4a.	Upgrade directly to 17.18.4a.
17.5.x	Upgrade first to 17.6.x and then to 17.18.4a.	Upgrade directly to 17.18.4a.
17.6.x	Upgrade to 17.9.6 or later or 17.12.x or later, and then to 17.18.4a.	Upgrade directly to 17.18.4a.
17.7.x	Upgrade to 17.9.6 or later or 17.12.x or later, and then to 17.18.4a.	Upgrade directly to 17.18.4a.
17.8.x	Upgrade to 17.9.6 or later or 17.12.x or later, and then to 17.18.4a.	Upgrade directly to 17.18.4a.
17.9.1 to 17.9.5	Upgrade to 17.9.6 or later or 17.12.x or later, and then to 17.18.4a. **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 17.18.4a.
17.9.6 or later	Upgrade directly to 17.18.4a.	Upgrade directly to 17.18.4a.
17.10.x	Upgrade to 17.12.x or later, and then to 17.18.4a.	Upgrade directly to 17.18.4a.
17.11.x	Upgrade to 17.12.x or later, and then to 17.18.4a.	Upgrade directly to 17.18.4a.
17.12.x	Upgrade directly to 17.18.4a.	Upgrade directly to 17.18.4a.
17.13.x	Upgrade directly to 17.18.4a.	Upgrade directly to 17.18.4a.
17.14.x	Upgrade directly to 17.18.4a.	Upgrade directly to 17.18.4a.
17.15.x	Upgrade directly to 17.18.4a.	Upgrade directly to 17.18.4a.
17.16.x	Upgrade directly to 17.18.4a.	Upgrade directly to 17.18.4a.
17.17.x	Upgrade directly to 17.18.4a.	Upgrade directly to 17.18.4a.

© 2026 Cisco and/or its affiliates. All rights reserved.

Current software	Upgrade path for deployments with 9130, 9124, or 916x	Upgrade path for deployments without 9130 and 9124
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 17.18.4a.	Upgrade directly to 17.18.4a.

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 17.18.4a

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

- C9800-80-universalk9_wlc.17.18.4a.SPA.bin
- C9800-40-universalk9_wlc.17.18.4a.SPA.bin
- C9800-L-universalk9_wlc.17.18.4a.SPA.bin

Image names (CW9800M, CW9800H1/CW9800H2, CW9800L)

- CW9800H-wlc-universalk9.17.18.4a.SPA.bin
- CW9800M-wlc-universalk9.17.18.4a.SPA.bin
- CW9800L-wlc-universalk9.17.18.4a.SPA.bin

Image names (9800-CL):

- **Cloud**: C9800-CL-universalk9.17.18.4a.SPA.bin
- **Hyper-V/ESXi/KVM**: C9800-CL-universalk9.17.18.4a.iso, C9800-CL-universalk9.17.18.4a.ova
- **KVM**: C9800-CL-universalk9.17.18.4a.qcow2
- **NFVIS**: C9800-CL-universalk9.17.18.4a.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]
```

© 2026 Cisco and/or its affiliates. All rights reserved.

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 6. Test configuration for interoperability

Hardware or software parameter	Hardware or software type
Release	Cisco IOS XE 17.18.4a
Cisco Wireless Controller	See Supported hardware
Access Points	See Supported APs

© 2026 Cisco and/or its affiliates. All rights reserved.

Hardware or software parameter	Hardware or software type
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 7. Client types

Client type and name	Driver or software version
Laptops	
Acer Aspire E 15 E5-573-3870 (Qualcomm Atheros QCA9377)	Latest
Apple MacBook Air 11 inch	Latest
Apple MacBook Air 13 inch	Latest
MacBook Pro Retina	Latest
MacBook Pro Retina 13 inch early 2015	Latest
MacBook Pro OS X	Latest
MacBook Air	Latest
MacBook Air 11 inch	Latest
MacBook M1 Chip	Latest
MacBook M1 Chip	Latest
MacBook Pro M2 Chip	Latest
MacBook Pro M2 Chip	Latest
MacBook Pro M3 chip	macOS Tahoe 26.4.1

© 2026 Cisco and/or its affiliates. All rights reserved.

Client type and name	Driver or software version
MacBook/Mac-Mini Pro M4 chip	macOS Tahoe 26.4.1
MacBook/Mac-Mini Pro M4 Pro chip	macOS Tahoe 26.4.1
MacBook Air M5 chip	macOS Tahoe 26.4.1
MacBook Pro M5 chip	macOS Tahoe 26.4.1
MacBook Neo	macOS Tahoe 26.4.1
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)	Latest
Dell Latitude 3480 (Qualcomm DELL wireless 1820)	Latest
Dell Inspiron 15-7569 (Intel Dual Band Wireless-AC 3165)	Latest
Dell Latitude E5540 (Intel Dual Band Wireless AC7260)	Latest
Dell Latitude E5430 (Intel Centrino Advanced-N 6205)	Latest
Dell Latitude E6840 (Broadcom Dell Wireless 1540 802.11 a/g/n)	Latest
Dell XPS 12 v9250 (Intel Dual Band Wireless AC 8260)	Latest
Dell Latitude 5491 (Intel AX200)	Latest
Dell XPS Latitude12 9250 (Intel Dual Band Wireless AC 8260)	Latest
Dell Inspiron 13-5368 Signature Edition	Latest
FUJITSU Lifebook E556 Intel 8260 (Intel Dual Band Wireless-AC 8260 (802.11n))	Latest
Lenovo Yoga C630 Snapdragon 850 (Qualcomm AC 2x2 Svc)	Latest
Lenovo ThinkPad Yoga 460 (Intel Dual Band Wireless-AC 9260)	Latest
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	

© 2026 Cisco and/or its affiliates. All rights reserved.

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

© 2026 Cisco and/or its affiliates. All rights reserved.

Client type and name	Driver or software version
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
Apple iPhone 14	iOS 26.4.1
Apple iPhone 14 Pro	iOS 26.4.1
Apple iPhone 15	iOS 26.4.1
Apple iPhone 15 Pro	iOS 26.4.1
Apple iPhone 16	iOS 26.4.1
Apple iPhone 16e	iOS 26.4.1
Apple iPhone 16 Pro	iOS 26.4.1
Apple iPhone 17	iOS 26.4.1
Apple iPhone 17 Pro	iOS 26.4.1
Apple iPhone 17e	iOS 26.4.1
Apple iPhone Air	iOS 26.4.1
ASCOM i63	Build v 3.0.0
ASCOM Myco 3	Android 9
Cisco IP Phone 8821	11.0.6 SR4
Cisco 840/s	Latest
Cisco 860	Latest
Cisco 9821	Latest
Cisco 7800 series desk phones	Latest
Cisco 8800 series desk phones	Latest
Cisco 9800 series desk phones	Latest
Drager Delta	VG9.0.2
Drager M300.3	VG3.0

© 2026 Cisco and/or its affiliates. All rights reserved.

Client type and name	Driver or software version
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
Google Pixel 8	Android 15
Google Pixel 9	Android 15
Google Pixel 10	Android 15
Huawei Mate 20 pro	Android 9.0
Huawei P20 Pro	Android 10
Huawei P40	Android 10
LG v40 ThinQ	Android 9.0
One Plus 8	Android 11
Oppo Find X2	Android 10
Redmi K20 Pro	Android 10
Samsung Galaxy S9+ - G965U1	Android 10.0
Samsung Galaxy S10 Plus	Android 11.0
Samsung S10 (SM-G973U1)	Android 11.0
Samsung S10e (SM-G970U1)	Android 11.0
Samsung Galaxy S20 Ultra	Android 10.0
Samsung Galaxy S21 Ultra 5G	Android 13.0
Samsung Galaxy S22 Ultra	Android 13.0
Samsung Galaxy S23	Android 15.0
Samsung Galaxy S23 Ultra	Android 15.0
Samsung Galaxy S24	Android 15.0

© 2026 Cisco and/or its affiliates. All rights reserved.

Client type and name	Driver or software version
Samsung Galaxy S24 Ultra	Android 15.0
Samsung Galaxy S25	Android 15.0
Samsung Galaxy S25 Ultra	Android 15.0
Samsung Fold 2	Android 10.0
Samsung Galaxy Z Fold 3	Android 13.0
Samsung Note20	Android 12.0
Samsung G Note 10 Plus	Android 11.0
Samsung Galaxy A01	Android 11.0
Samsung Galaxy A21	Android 10.0
Sony Experia 1 ii	Android 11
Sony Experia	Android 11
Xiaomi Mi 9T	Android 9
Xiaomi Mi 10	Android 11
Spectralink 84 Series	7.5.0.x257
Spectralink 87 Series	Android 5.1.1
Spectralink Versity Phones 92/95/96 Series	Android 10.0
Spectralink Versity Phones 9540 Series	Android 8.1.0
Vocera Badges B3000n	4.3.3.18
Vocera Smart Badges V5000	5.0.6.35
Zebra MC40	Android 4.4.4
Zebra MC40N0	Android 4.1.1
Zebra MC92N0	Android 4.4.4
Zebra MC9090	Windows Mobile 6.1
Zebra MC55A	Windows 6.5
Zebra MC75A	OEM ver 02.37.0001
Zebra TC51	Android 6.0.1
Zebra TC52	Android 10.0

© 2026 Cisco and/or its affiliates. All rights reserved.

Client type and name	Driver or software version
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	Latest
Intel AX 211	Latest
Intel AX 210	Latest
Intel AX 200	Latest
Intel 11AC	Latest
Intel AC 9260	Latest
Intel Dual Band Wireless AC 8260	Latest
Samsung S21 Ultra	Latest
QCA WCN6855	Latest
PhoenixContact FL WLAN 2010	Latest

© 2026 Cisco and/or its affiliates. All rights reserved.

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 8. Supported virtual and hardware platforms

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

© 2026 Cisco and/or its affiliates. All rights reserved.

Platform	Description
	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 9. Supported host environments for public and private cloud

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

Supported PIDs and ports

The following table lists the supported Cisco Catalyst 9800 Series Wireless Controller hardware models.

The base PIDs are the model numbers of the controller.

The bundled PIDs indicate the orderable part numbers for the base PIDs that are bundled with a particular network module. Running the **show version**, **show module**, or **show inventory** command on such a controller (bundled PID) displays its base PID.

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

Table 10. 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

© 2026 Cisco and/or its affiliates. All rights reserved.

Controller model	Description
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 11. Supported SFP models

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

© 2026 Cisco and/or its affiliates. All rights reserved.

SFP name	C9800-80-K9	C9800-40-K9	C9800-L-F-K9	CW9800H1	CW9800H2	CW9800M	CW9800L
GLC-T	Supported	–	–	–	–	–	–
GLC-TE	Supported	Supported	Supported	Supported	Supported	Supported	Supported
GLC-ZX-SMD	Supported	Supported	Supported	Supported	Supported	Supported	–
QSFP-100G-LR4-S	Supported	–	–	–	–	–	–
QSFP-100G-SR4-S	Supported	–	–	–	–	–	–
QSFP-40G-BD-RX	Supported	–	–	Supported	Supported	Supported	–
QSFP-40G-ER4	Supported	–	–	–	Supported	–	–
QSFP-40G-LR4	Supported	–	–	–	Supported	–	–
QSFP-40G-LR4-S	Supported	–	–	–	Supported	–	–
QSFP-40G-LR4-S-RF	–	–	–	Supported	Supported	Supported	–
QSFP-40G-CSR4	–	–	–	–	Supported	–	–
QSFP-40G-SR4	Supported	–	–	–	Supported	–	–
QSFP-40G-SR4-S	Supported	–	–	–	Supported	–	–
QSFP-40G-SR-BD				Supported	Supported	Supported	
QSFP-40GE-LR4	Supported	–	–	–	–	–	–
QSFP-H40G-ACU7M				Supported	Supported	Supported	
QSFP-H40G-ACU10M	–	–	–	–	Supported	–	–
QSFP-H40G-CU1M	–	–	–	–	Supported	–	–
QSFP-H40G-CU2M	–	–	–	–	Supported	–	–
QSFP-H40G-CU3M	–	–	–	–	Supported	–	–
QSFP-H40G-CU4M	–	–	–	–	Supported	–	–
QSFP-H40G-CU5M	–	–	–	–	Supported	–	–
QSFP-H40G-CU0-5M	–	–	–	–	Supported	–	–
QSFP-H40G-AOC1M	–	–	–	–	Supported	–	–

© 2026 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-AOC2M	–	–	–	–	Supported	–	–
QSFP-H40G-AOC3M	–	–	–	–	Supported	–	–
QSFP-H40G-AOC5M	–	–	–	–	Supported	–	–
QSFP-H40G-AOC7M	–	–	–	–	Supported	–	–
QSFP-H40G-AOC10M	–	–	–	–	Supported	–	–
QSFP-H40G-AOC15M	–	–	–	–	Supported	–	–
QSFP-H40G-AOC20M	–	–	–	–	Supported	–	–
QSFP-H40G-AOC25M	–	–	–	–	Supported	–	–
QSFP-H40G-AOC30M	–	–	–	–	Supported	–	–
SFP-10G-AOC10M	Supported	Supported	–	–	–	–	Supported
SFP-10G-AOC1M	Supported	Supported	–	Supported	Supported	Supported	Supported
SFP-10G-AOC2M	Supported	Supported	–	Supported	Supported	Supported	Supported
SFP-10G-AOC3M	Supported	Supported	–	Supported	Supported	Supported	Supported
SFP-10G-AOC5M	Supported	Supported	–	Supported	Supported	Supported	Supported
SFP-10G-AOC7M	Supported	Supported	–	Supported	Supported	Supported	Supported
SFP-10G-BXD-I	–	–	–	Supported	Supported	Supported	Supported
SFP-10G-BXU-I	–	–	–	Supported	Supported	Supported	Supported
SFP-10G-CSR-S	–	–	–	Supported	Supported	Supported	–
SFP-10G-ER	Supported	Supported	–	Supported	Supported	Supported	–
SFP-10G-LR	Supported	Supported	Supported	Supported	Supported	Supported	Supported
SFP-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	–

© 2026 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-LRM	Supported	Supported	Supported	–	–	–	–
SFP-10G-SR	Supported	Supported	Supported	Supported	Supported	Supported	Supported
SFP-10G-SR-S	Supported	Supported	Supported	Supported	Supported	Supported	Supported
SFP-10G-SR-I	–	–	–	Supported	Supported	Supported	Supported
SFP-10G-SR-X	Supported	Supported	Supported	–	–	–	–
SFP-10G-ZR			–	Supported	Supported	Supported	–
SFP-10G-ZR-I	–	–	–	Supported	Supported	Supported	Supported
SFP-10G-T-X	–	–	–	Supported	Supported	Supported	–
SFP-25G-CSR-S				Supported	Supported	Supported	
SFP-25G-SR-S	–	–	–	Supported	–	Supported	–
SFP-25G-ER-I	–	–	–	Supported	–	Supported	–
SFP-10/25G-LR-I	–	–	–	Supported	–	Supported	–
SFP-10/25G-LR-S	–	–	–	Supported	–	Supported	–
SFP-10/25G-CSR-S	–	–	–	Supported	–	Supported	–
SFP-10/25G-BXD-I	–	–	–	Supported	–	Supported	Supported
SFP-10/25G-BXU-I	–	–	–	Supported	–	Supported	Supported
SFP-H25G-CU1M	–	–	–	Supported	–	Supported	–
SFP-H25G-CU5M	–	–	–	Supported	–	Supported	–
SFP-25G-AOC1M	–	–	–	Supported	–	Supported	–
SFP-25G-AOC2M	–	–	–	Supported	–	Supported	–
SFP-25G-AOC3M	–	–	–	Supported	–	Supported	–
SFP-25G-AOC5M	–	–	–	Supported	–	Supported	–
SFP-25G-AOC7M	–	–	–	Supported	–	Supported	–
SFP-25G-AOC10M	–	–	–	Supported	–	Supported	–
SFP-H10GB-ACU10M	Supported	Supported	Supported	Supported	Supported	Supported	Supported
SFP-H10GB-ACU7M	Supported	Supported	Supported	Supported	Supported	Supported	Supported

© 2026 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-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 12. 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

© 2026 Cisco and/or its affiliates. All rights reserved.

Source	Destination	Protocol	Destination port	Source port	Description
Any	Cisco Catalyst 9800 Series Wireless Controller	UDP	161	Any	SNMP agent
Any	Any	UDP	5353	5353	mDNS
Any	Cisco Catalyst 9800 Series Wireless Controller	UDP	69	69	TFTP
Any	DNS Server	UDP	53	Any	DNS
Any	Cisco Catalyst 9800 Series Wireless Controller	TCP	830	Any	NetConf
Any	Cisco Catalyst 9800 Series Wireless Controller	TCP	443	Any	REST API
Any	WLC Protocol	UDP	1700	Any	Receive CoA packets
AP	Cisco Catalyst 9800 Series Wireless Controller	UDP	5246	Any	CAPWAP Control
AP	Cisco Catalyst 9800 Series Wireless Controller	UDP	5247	Any	CAPWAP Data
AP	Cisco Catalyst 9800 Series Wireless Controller	UDP	5248	Any	CAPWAP MCAST
AP	Cisco Catalyst Center	TCP	32626	Any	Intelligent capture and RF telemetry
AP	AP	UDP	16670	Any	Client Policies (AP-AP)
Cisco Catalyst 9800 Series Wireless Controller	Cisco Catalyst 9800 Series Wireless Controller	UDP	16666	16666	Mobility Control
Cisco Catalyst 9800 Series Wireless Controller	SNMP	UDP	162	Any	SNAMP Trap
Cisco Catalyst 9800 Series Wireless Controller	RADIUS	UDP	1812/1645	Any	RADIUS Auth
Cisco Catalyst 9800 Series Wireless Controller	RADIUS	UDP	1813/1646	Any	RADIUS ACCT

© 2026 Cisco and/or its affiliates. All rights reserved.

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

AP type	AP names
Indoor Access Points	• Cisco Catalyst 9105AX (I/W) Access Points • Cisco Catalyst 9115AX (I/E) Access Points • Cisco Catalyst 9120AX (I/E/P) Access Points • Cisco Catalyst 9130AX (I/E) Access Points • Cisco Catalyst 9136AX Access Points

© 2026 Cisco and/or its affiliates. All rights reserved.

AP type	AP names
	• Cisco Catalyst 9162 (I) Series Access Points • Cisco Catalyst 9164 (I) Series Access Points • Cisco Catalyst 9166 (I/D1) Series Access Points • Cisco Wireless 9171 (I) Series Wi-Fi 7 Access Points • Cisco Wireless 9172 (I/H) Series Wi-Fi 7 Access Points • Cisco Wireless 9174 (I/E) Series Wi-Fi 7 Access Points • Cisco Wireless 9176 (I/D1) Series Wi-Fi 7 Access Points • Cisco Wireless 9178 (I) Series Wi-Fi 7 Access Points • Cisco Wireless 9179 (F) Series Wi-Fi 7 Access Points • Cisco Aironet 1815 (I/W/M/T), 1830 (I), 1840 (I), and 1852 (I/E) Access Points • Cisco Aironet 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 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.

© 2026 Cisco and/or its affiliates. All rights reserved.

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

© 2026 Cisco and/or its affiliates. All rights reserved.

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.

© 2026 Cisco Systems, Inc. All rights reserved.