Release Notes for Cisco Wireless Controllers and Lightweight Access Points, Cisco Wireless Release 8.10.190.0

First Published: 2023-09-30

Last Modified: 2024-02-29

About the Release Notes

This release notes document describes what is new or changed in this release, instructions to upgrade to this release, and provides information about the open and resolved caveats for this release. Unless otherwise noted, in this document, Cisco Wireless Controllers are referred to as *controllers*, and Cisco lightweight access points are referred to as *access points* or *APs*.

Supported Cisco Wireless Controller Platforms

The following controller platforms are supported in this release:

- Cisco 3504 Wireless Controller
- Cisco 5520 Wireless Controller
- Cisco 8540 Wireless Controller
- Cisco Virtual Wireless Controller (vWLC) on the following platforms:
  - VMware vSphere Hypervisor (ESXi) Version 5.x and 6.x
  - Hyper-V on Microsoft Server 2012 and later versions (support introduced in Release 8.4)
  - Kernel-based virtual machine (KVM) (support introduced in Release 8.1). After KVM is deployed, we recommend that you do not downgrade to a Cisco Wireless release that is earlier than Release 8.1).
- Cisco Wireless Controllers for High Availability for Cisco 3504 Wireless Controller, Cisco 5520 Wireless Controller, and Cisco 8540 Wireless Controller
- Cisco Mobility Express

Note In a network that includes Cisco Catalyst Center (formerly Cisco DNA Center) and Cisco AireOS controller, and the controller fails provisioning with **Error NA serv CA certificate file transfer failed** error, as a workaround, we recommend you reboot the affected AireOS controller.

Supported Cisco Access Point Platforms

The following Cisco AP platforms are supported in this release:

- Cisco Catalyst 9105 Access Points
- Cisco Catalyst 9130 Access Points
- Cisco Catalyst 9120 Access Points
- Cisco Catalyst 9117 Access Points
- Cisco Catalyst 9115 Access Points
- Cisco Aironet 700 Series Access Points
- Cisco Aironet 700W Series Access Points
- Cisco AP803 Integrated Access Point
- Integrated Access Point on Cisco 1100, 1101, and 1109 Integrated Services Routers
- Cisco Aironet 1700 Series Access Points
- Cisco Aironet 1800 Series Access Points
- Cisco Aironet 1810 Series OfficeExtend Access Points
- Cisco Aironet 1810W Series Access Points
- Cisco Aironet 1815 Series Access Points
- Cisco Aironet 1830 Series Access Points
- Cisco Aironet 1840 Series Access Points
- Cisco Aironet 1850 Series Access Points
- Cisco Aironet 2700 Series Access Points
- Cisco Aironet 2800 Series Access Points
- Cisco Aironet 3700 Series Access Points
- Cisco Aironet 3800 Series Access Points
- Cisco Aironet 4800 Series Access Points
- Cisco ASA 5506W-AP702
- Cisco Aironet 1530 Series Access Points
- Cisco Aironet 1540 Series Access Points
- Cisco Aironet 1560 Series Access Points
- Cisco Aironet 1570 Series Access Points
- Cisco Industrial Wireless 3700 Series Access Points
- Cisco Catalyst IW6300 Heavy Duty Series Access Points

- Cisco 6300 Series Embedded Services Access Points

Cisco AP803 is an integrated access point module on the Cisco 800 Series Integrated Services Routers (ISRs). For more information about the stock-keeping units (SKUs) for the AP803 Cisco ISRs, see:

http://www.cisco.com/c/en/us/products/routers/800-series-routers/brochure-listing.html.

For more information about the integrated access point on Cisco 1100 ISR, see the product data sheet:

https://www.cisco.com/c/en/us/products/collateral/routers/1000-series-integrated-services-routers-isr/datasheet-c78-739512.html.

For information about the Cisco Wireless software releases that support specific Cisco access point modules, see the "Software Release Support for Specific Access Point Modules" section in the *Cisco Wireless Solutions Software Compatibility Matrix* document.

What's New in Release 8.10.190.0

There are no new features that are introduced in this release. For more information about updates in this release, see the Unfixed and Fixed Issues in Release 8.10.190.0 section in this document.

Note For a complete list of all the documentation published for Cisco Wireless Release 8.10, see the Documentation Roadmap at: https://www.cisco.com/c/en/us/td/docs/wireless/doc-roadmap/doc-roadmap-release-810.html

Software Release Types and Recommendations

Table 1: Release Types

Release Type	Description	Benefit
Maintenance Deployment (MD)	Software releases that provide bug-fix support and ongoing software maintenance. These releases are categorized as Maintenance Deployment (MD). These releases are long-living releases with ongoing software maintenance.	Provides you with a software release that offers stability and long support duration with periodic maintenance releases (MRs).
Early Deployment (ED)	Software releases that provide new features and new hardware platform support in addition to bug fixes. These releases are categorized as Early Deployment (ED). These releases are short-lived releases.	Allows you to deploy the latest features and new hardware platforms or modules.

For detailed release recommendations, see the *Guidelines for Cisco Wireless Software Release Migration Bulletin* at:

http://www.cisco.com/c/en/us/products/collateral/wireless/8500-series-wireless-controllers/bulletin-c25-730741.html.

Table 2: Upgrade Path to Cisco Wireless Release 8.10.190.0

Current Software Release	Upgrade Path to Release 8.10.190.0
8.5.x	You can upgrade directly to Release 8.10.190.0.
8.6.x	You can upgrade directly to Release 8.10.190.0.
8.7.x	You can upgrade directly to Release 8.10.190.0.
8.8.x	You can upgrade directly to Release 8.10.190.0.
8.9.x	You can upgrade directly to Release 8.10.190.0.
8.10.x	You can upgrade directly to Release 8.10.190.0.

Upgrading a Cisco Wireless Release

This section describes the guidelines and limitations that you must be aware of when you are upgrading the Cisco Wireless release and the procedure to upgrade.

Guidelines and Limitations

- An existing WLAN with *?* in its name continues to be supported with this upgrade. However, you cannot include *?* in the name when creating a new WLAN.
- If an AP locks out the console due to default management user credentials, you must configure the controller AP global credential with non-default username and password to get access to the AP console.
- WPA3 upgrade and downgrade guidelines:
  - If you want to upgrade from Release 8.5 to 8.10 and have WPA1 configured with none of the WPA1 AKM valid for Release 8.10, the WPA1 configuration is disabled after the upgrade.
  - If you downgrade from Release 8.10 to Release 8.5, if any AKM for SAE is configured, the AKM validation fails after the downgrade. The security is set to WPA2 and AKM to 802.1X. However, PMF configuration is retained, which results in an error.
  - FT set to enabled state and PMF set to Required state is allowed in Release 8.10 because PMF and FT configurations are decoupled. However, in Release 8.5, this configuration invalid. Therefore, upon downgrading to Release 8.5, the WLAN might be disabled.
- Software downgrade guidelines for Release 8.10:
  - If you plan to downgrade the Cisco controller from Release 8.10 software, we recommend you to downgrade to Release 8.5.151.0 or later release to prevent the controller configuration files from being corrupted.
  - If you have configured new country codes in Release 8.10 and if you plan to downgrade to an earlier release, then we recommend that you remove the new country code configurations prior to the downgrade. For more information, see CSCvq91895.

- Before downgrading or upgrading the Cisco Controller to another release check for APs or AP modes support. Ensure that only supported APs are connected and also the APs are moved to supported modes on the release that the controller is upgraded or downgraded to.
- Legacy clients that require RC4 or 3DES encryption type are not supported in Local EAP authentication.
- If you downgrade to Release 8.0.140.0 or 8.0.15x.0, and later upgrade to a later release and and also have the multiple country code feature configured, then the configuration file could get corrupted. When you try to upgrade to a later release, special characters are added in the country list causing issues when loading the configuation. For more information, see CSCve41740.

Note Upgrade and downgrade between other releases does not result in this issue.

- After downloading the new software to the Cisco APs, it is possible that a Cisco AP may get stuck in an upgrading image state. In such a scenario, it might be necessary to forcefully reboot the controller to download a new controller software image or to reboot the controller after the download of the new controller software image. You can forcefully reboot the controller by entering the **reset system forced** command.
- It is not possible to download some of the older configurations from the controller because of the Multicast and IP address validations. See the "Restrictions on Configuring Multicast Mode" section in the *Cisco Wireless Controller Configuration Guide* for detailed information about platform support for global multicast and multicast mode.
- When a client sends an HTTP request, the controller intercepts it for redirection to the login page. If the HTTP GET request that is intercepted by the controller is longer than 2000 bytes, the controller drops the packet. Track the Caveat ID CSCuy81133 for a possible enhancement to address this restriction.
- When downgrading from one release to an earlier release, you might lose the configuration from your current release. The workaround is to reload the previous controller configuration files that are saved in the backup server, or to reconfigure the controller.
- When you upgrade a controller to an intermediate release, wait until all the APs that are associated with the controller are upgraded to the intermediate release before you install the latest controller software. In large networks, it can take some time to download the software on each AP.
- You can upgrade to a new release of the controller software or downgrade to an earlier release even if FIPS is enabled.
- When you upgrade to the latest software release, the software on the APs associated with the controller is also automatically upgraded. When an AP is loading software, each of its LEDs blinks in succession.
- Controllers support standard SNMP MIB files. MIBs can be downloaded from the software download page on Cisco.com.
- The controller software that is factory-installed on your controller and is automatically downloaded to the APs after a release upgrade and whenever an AP joins a controller. We recommend that you install the latest software version available for maximum operational benefit.
- Ensure that you have a TFTP, HTTP, FTP, or SFTP server available for the software upgrade. Follow these guidelines when setting up a server:
    - Ensure that your TFTP server supports files that are larger than the size of controller software image. Some TFTP servers that support files of this size are tftpd32 and the TFTP server within Cisco

  Prime Infrastructure. If you attempt to download the controller software image and your TFTP server does not support files of this size, the following error message appears:

  ```
  TFTP failure while storing in flash
  ```

  - If you are upgrading through the distribution system network port, the TFTP or FTP server can be on the same subnet or a different subnet because the distribution system port is routable.

- The controller Bootloader stores a copy of the active primary image and the backup image. If the primary image becomes corrupted, you can use the Bootloader to boot with the backup image.

  With the backup image stored before rebooting, from the **Boot Options** menu, choose **Option 2: Run Backup Image** to boot from the backup image. Then, upgrade with a known working image and reboot controller.

- You can control the addresses that are sent in the Control and Provisioning of Wireless Access Points (CAPWAP) discovery responses when NAT is enabled on the Management Interface, using the following command:

  config network ap-discovery nat-ip-only {**enable** | **disable**}

  The following are the details of the command:

  enable—Enables use of NAT IP only in a discovery response. This is the default. Use this command if all the APs are outside the NAT gateway.

  disable—Enables use of both NAT IP and non-NAT IP in a discovery response. Use this command if APs are on the inside and outside the NAT gateway, for example, Local Mode and OfficeExtend APs are on the same controller.

Note To avoid stranding of APs, you must disable the AP link latency (if enabled) before you use the disable option in the **config network ap-discovery nat-ip-only** command. To disable AP link latency, use the **config ap link-latency disable all** command.

- Do not power down the controller or any AP during the upgrade process. If you do this, the software image might get corrupted. Upgrading the controller with a large number of APs can take as long as 30 minutes, depending on the size of your network. However, with the increased number of concurrent AP upgrades supported, the upgrade time should be significantly reduced. The APs must remain powered, and controller must not be reset during this time.

- After you perform the following functions on the controller, reboot it for the changes to take effect:

  - Enable or disable LAG.

  - Enable a feature that is dependent on certificates (such as HTTPS and web authentication).

  - Add a new license or modify an existing license.

Note Reboot is not required if you are using Right-to-Use licenses.

  - Increase the priority of a license.

    - Enable HA.
    - Install the SSL certificate.
    - Configure the database size.
    - Install the vendor-device certificate.
    - Download the CA certificate.
    - Upload the configuration file.
    - Install the Web Authentication certificate.
    - Make changes to the management interface or the virtual interface.

- Cisco AireOS 3504 Controller: If the controller has been running for more than 450 days, ensure that you free up the flash memory before downloading the software image to the controller. For more information, see CSCwh98302.
- Before 8.10.190 release, during the SNMPv3 setup process you could use the same password for both the authentication and the encryption keys on the Cisco AireOS 5520 wireless controller. With the 8.10.190 release, you cannot use the same password for both the keys. This is a functionality that exists in the Cisco Catalyst 9800 series controllers.

Upgrading Cisco Wireless Software (GUI)

Procedure

Step 1 Upload your controller configuration files to a server to back up the configuration files.

Note We highly recommend that you back up your controller configuration files prior to upgrading the controller software.

Step 2 Follow these steps to obtain controller software:

a) Browse to the Software Download portal at: https://software.cisco.com/download/home.
b) Search for the controller model.
c) Click **Wireless LAN Controller Software**.
d) The software releases are labeled as described here to help you determine which release to download. Click a controller software release number:

    - Early Deployment (ED)—These software releases provide new features and new hardware platform support as well as bug fixes.
    - Maintenance Deployment (MD)—These software releases provide bug fixes and ongoing software maintenance.
    - Deferred (DF)—These software releases have been deferred. We recommend that you migrate to an upgraded release.

e) Click the filename <*filename.aes*>.
f) Click **Download**.

g) Read the Cisco End User Software License Agreement and click **Agree**.
h) Save the file to your hard drive.
i) Repeat steps *a* through *h* to download the remaining file.

Step 3 Copy the controller software file <*filename.aes*> to the default directory on your TFTP, FTP, SFTP, or USB server.

Step 4 (Optional) Disable the controller 802.11 networks.

Note For busy networks, controllers on high utilization, and small controller platforms, we recommend that you disable the 802.11 networks as a precautionary measure.

Step 5 Choose **Commands** > **Download File** to open the **Download File to Controller** page.

Step 6 From the **File Type** drop-down list, choose **Code**.

Step 7 From the **Transfer Mode** drop-down list, choose **TFTP**, **FTP**, **SFTP**, **HTTP**, or **USB**.

Step 8 Enter the corresponding server details as prompted.

Note Server details are not required if you choose HTTP as the transfer mode.

Step 9 Click **Download** to download the software to the controller.

A message indicating the status of the download is displayed.

Note Ensure that you choose the **File Type** as **Code** for both the images.

Step 10 After the download is complete, click **Reboot**.

Step 11 If you are prompted to save your changes, click **Save and Reboot**.

Step 12 Click **OK** to confirm your decision to reboot the controller.

Step 13 If you have disabled the 802.11 networks, reenable them.

Step 14 (Optional) To verify that the controller software is installed on your controller, on the controller GUI, click **Monitor** and view the **Software Version** field under **Controller Summary**.

CIMC Utility Upgrade for 5520 and 8540 Controllers

The AIR-CT5520-K9 and AIR-CT8540-K9 controller models are based on Cisco UCS server C series, C220 and C240 M4 respectively. These controller models have CIMC utility that can edit or monitor low-level physical parts such as power, memory, disks, fan, temperature, and provide remote console access to the controllers.

We recommend that you upgrade the CIMC utility to a version that has been certified to be used with these controllers. Controllers that have older versions of CIMC installed are susceptible to rebooting without being able to access FlexFlash, with the result that the manufacturing certificates are unavailable, and thus SSH and HTTPS connections will fail, and access points will be unable to join. See: CSCvo33873. The recommended version addresses this FlexFlash problem.

The certified CIMC images are available at the following locations:

Table 3: CIMC Utility Software Image Information

Controller	Current CIMC Version	Recommended CIMC Version	Link to Download the CI Software Image
Cisco 5520 Wireless Controller Cisco 8540 Wireless Controller	2.x	4.1(2m) from November, 2023 onwards.	**1.** Upgrade to 3.0(4r) • 5520—https://softw download/hom 286281345/typ 283850974/rel 3.0(4r) • 8540—https://softw download/hom 286281356/typ 283850974/rel 3.0(4r) **Note** We rec that yo upgrad firmwa 2.x to 3 using T SCP pr only. **2.** Upgrade from 3.0(4 4.1(2k) https://software.cisco.c download/home/286281 283850974/release/3.0(**Note** We recomm to upgrade firmware f 2.0(13i) to using TFT protocols o
Cisco 5520 Wireless Controller (C220 M4) Cisco 8540 Wireless Controller (C240 M4)	3.x or 4.x	4.1(2m) from November, 2023 onwards.	https://software.cisco.c download/home/286281 283850974/release/3.0(

- For more details regarding the CIMC upgrade path, see the Cisco UCS Rack Server Upgrade Matrix.
- CIMC Release Notes
  - **3.0(4)—** https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/release/notes/b_UCS_C-Series_Release_Notes_3_0_4.html

- **4.1(2)—** https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/release/notes/b_release-notes-for-cisco-ucs-rack-server-software-release-4_1_2.html

Table 4: Key fixes in Release 4.1(2k)

CSCvv60351	Mutex issues in flexflash driver code (fixed in 4.1(2f))
CSCvv71216	FlexFlash SD card goes missing and reappears repeatedly and frequently (fixed in 4.1(2f))

Interoperability with Other Clients

This section describes the interoperability of controller software with other client devices.

The following table describes the configuration that is used for testing the client devices.

Table 5: Test Bed Configuration for Interoperability

Hardware or Software Parameter	Hardware or Software Configuration Type
Release	8.10.x
Cisco Wireless Controller	Cisco 3504 Wireless Controller
Access Points	Cisco 9130, 9120 and 3800 APs
Radio	802.11ax (2.4 GHz or 5 GHz), 802.11ac, 802.11a, 802.11g, 802.11n (2.4 GHz or 5 GHz)
Security	Open, WPA3-SAE/OWE (WPA3 Supported Clients), WPA2+WPA3 (Mixed Mode) PSK (WPA2-AES), 802.1X (WPA2-AES)(EAP-PEAP)
RADIUS	Cisco ISE 2.6 Cisco ISE 2.7
Types of tests	Association, Traffic (TCP/UDP/ICMP) and Roaming between APs

The following table lists the client types on which the tests were conducted. Client types included laptops, handheld devices, phones, and printers.

Table 6: Client Types

Client Type and Name	Driver / Software Version
Wi-Fi 6 Devices (Mobile Phone and Laptop)	
Apple iPhone 11	iOS 14.1
Apple iPhone SE 2020	iOS 14.1
Dell Intel AX1650w	Windows 10 (21.90.2.1)
DELL LATITUDE 5491 (Intel AX200)	Windows 10 Pro (21.40.2)

Client Type and Name	Driver / Software Version
Samsung S20	Android 10
Samsung S10 (SM-G973U1)	Android 9.0 (One UI 1.1)
Samsung S10e (SM-G970U1)	Android 9.0 (One UI 1.1)
Samsung Galaxy S10+	Android 9.0
Samsung Galaxy Fold 2	Android 10
Samsung Galaxy Flip Z	Android 10
Samsung Note 20	Android 10
Laptops	
Acer Aspire E 15 E5-573-3870 (Qualcomm Atheros QCA9377)	Windows 10 Pro (12.0.0.832)
Apple Macbook Air 11 inch	OS Sierra 10.12.6
Apple Macbook Air 13 inch	OS Catalina 10.15.4
Apple Macbook Air 13 inch	OS High Sierra 10.13.4
Macbook Pro Retina	OS Mojave 10.14.3
Macbook Pro Retina 13 inch early 2015	OS Mojave 10.14.3
Dell Inspiron 2020 Chromebook	Chrome OS 75.0.3770.129
Google Pixelbook Go	Chrome OS 84.0.4147.136
HP chromebook 11a	Chrome OS 76.0.3809.136
Samsung Chromebook 4+	Chrome OS 77.0.3865.105
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 (18.32.0.5)
DELL Latitude E5540 (Intel Dual Band Wireless AC7260)	Windows 7 Professional (21.10.1)
DELL XPS 12 v9250 (Intel Dual Band Wireless AC 8260)	Windows 10 (19.50.1.6)
DELL Latitude 5491 (Intel AX200)	Windows 10 Pro (21.40.2)
DELL XPS Latitude12 9250 (Intel Dual Band Wireless AC 8260)	Windows 10 Home (21.40.0)
Lenovo Yoga C630 Snapdragon 850 (Qualcomm AC 2x2 Svc)	Windows 10(1.0.10440.0)
Lenovo Thinkpad Yoga 460 (Intel Dual Band Wireless-AC 9260)	Windows 10 Pro (21.40.0)

Client Type and Name	Driver / Software Version
Note For clients using Intel wireless cards, we recommend you to update to the latest Intel wireless drivers if advertised SSIDs are not visible.	
Tablets	
Apple iPad Pro	iOS 13.5
Apple iPad Air2 MGLW2LL/A	iOS 12.4.1
Apple iPad Mini 4 9.0.1 MK872LL/A	iOS 11.4.1
Apple iPad Mini 2 ME279LL/A	iOS 12.0
Microsoft Surface Pro 3 – 11ac	Qualcomm Atheros QCA61x4A
Microsoft Surface Pro 3 – 11ax	Intel AX201 chipset. Driver v21.40.1.3
Microsoft Surface Pro 7 – 11ax	Intel Wi-Fi chip (HarrisonPeak AX201) (11ax, WPA3)
Microsoft Surface Pro X – 11ac & WPA3	WCN3998 Wi-Fi Chip (11ac, WPA3)
Mobile Phones	
Apple iPhone 5	iOS 12.4.1
Apple iPhone 6s	iOS 13.5
Apple iPhone 8	iOS 13.5
Apple iPhone X MQA52LL/A	iOS 13.5
Apple iPhone 11	iOS 14.1
Apple iPhone SE MLY12LL/A	iOS 11.3
ASCOM SH1 Myco2	Build 2.1
ASCOM SH1 Myco2	Build 4.5
ASCOM Myco 3 v1.2.3	Android 8.1
Drager Delta	VG9.0.2
Drager M300.3	VG2.4
Drager M300.4	VG2.4
Drager M540	DG6.0.2 (1.2.6)
Google Pixel 2	Android 10
Google Pixel 3	Android 11
Google Pixel 3a	Android 11
Google Pixel 4	Android 11
Huawei Mate 20 pro	Android 9.0
Huawei P20 Pro	Android 9.0

Client Type and Name	Driver / Software Version
Huawei P40	Android 10
LG v40 ThinQ	Android 9.0
One Plus 8	Android 10
Oppo Find X2	Android 10
Redmi K20 Pro	Android 10
Samsung Galaxy S7	Andriod 6.0.1
Samsung Galaxy S7 SM - G930F	Android 8.0
Samsung Galaxy S8	Android 8.0
Samsung Galaxy S9+ - G965U1	Android 9.0
Samsung Galaxy SM - G950U	Android 7.0
Sony Experia 1 ii	Android 10
Sony Experia xz3	Android 9.0
Xiaomi Mi10	Android 10
Spectralink 8744	Android 5.1.1
Spectralink Versity Phones 9540	Android 8.1
Vocera Badges B3000n	4.3.2.5
Vocera Smart Badges V5000	5.0.4.30
Zebra MC40	Android 5.0
Zebra MC40N0	Android Ver: 4.1.1
Zebra MC92N0	Android Ver: 4.4.4
Zebra TC51	Android 7.1.2
Zebra TC52	Android 8.1.0
Zebra TC55	Android 8.1.0
Zebra TC57	Android 8.1.0
Zebra TC70	Android 6.1
Zebra TC75	Android 6.1.1
Printers	
Zebra QLn320 Printer	LINK OS 6.3
Zebra ZT230 Printer	LINK OS 6.3
Zebra ZQ310 Printer	LINK OS 6.3
Zebra ZD410 Printer	LINK OS 6.3

Client Type and Name	Driver / Software Version
Zebra ZT410 Printer	LINK OS 6.3
Zebra ZQ610 Printer	LINK OS 6.3
Zebra ZQ620 Printer	LINK OS 6.3
Wireless Module	
Intel 11ax 200	Driver v21.40.1.3, v21.20.1.1
Intel AC 9260	Driver v21.40.0
Intel Dual Band Wireless AC 8260	Driver v19.50.1.6

Key Features Not Supported in Controller Platforms

This section lists the features that are not supported on various controller platforms:

Note In a converged access environment that has controllers running AireOS code, High Availability Client SSO and native IPv6 are not supported.

Key Features Not Supported in Cisco 3504 Wireless Controller

- Cisco WLAN Express Setup Over-the-Air Provisioning
- Mobility controller functionality in converged access mode
- VPN Termination (such as IPsec and L2TP)

Key Features Not Supported in Cisco 5520 and 8540 Wireless Controllers

- Internal DHCP Server
- Mobility controller functionality in converged access mode
- VPN termination (such as IPsec and L2TP)
- Fragmented pings on any interface

Key Features Not Supported in Cisco Virtual Wireless Controller

- Cisco Umbrella
- Software-defined access
- Domain-based ACLs
- Internal DHCP server
- Cisco TrustSec

- Access points in local mode
- Mobility or Guest Anchor role
- Wired Guest
- Multicast

Note FlexConnect locally switched multicast traffic is bridged transparently for both wired and wireless on the same VLAN. FlexConnect APs do not limit traffic based on IGMP or MLD snooping.

- FlexConnect central switching in large-scale deployments

Note

- FlexConnect central switching is supported in only small-scale deployments, wherein the total traffic on controller ports is not more than 500 Mbps.
- FlexConnect local switching is supported.

- Central switching on Microsoft Hyper-V deployments
- AP and Client SSO in High Availability
- PMIPv6
- Datagram Transport Layer Security (DTLS)
- EoGRE (Supported only in local switching mode)
- Workgroup bridges
- Client downstream rate limiting for central switching
- SHA2 certificates
- Controller integration with Lync SDN API
- Cisco OfficeExtend Access Points

Key Features Not Supported in Access Point Platforms

This section lists the key features that are not supported on various Cisco Aironet AP platforms. For detailed information about feature support on Cisco Aironet Wave 2 and 802.11ax APs, see:

https://www.cisco.com/c/en/us/td/docs/wireless/access_point/feature-matrix/ap-feature-matrix.html

Key Features Not Supported in Cisco Aironet 1800i, 1810 OEAP, 1810W, 1815, 1830, 1850, 2800, 3800, and 4800 Series APs

Table 7: Key Features Not Supported in Cisco Aironet 1800i, 1810 OEAP, 1810W, 1815, 1830, 1850, 2800, 3800, and 4800 Series APs

Operational Modes	• Autonomous Bridge and Workgroup Bridge (WGB) mode **Note** WGB is supported in Cisco Aironet 2800, 3800 Series APs. • Mesh mode **Note** Mesh mode is supported in Cisco Aironet 1815i, 1815m, 1830, 1850, 2800, 3800, and 4800 Series APs in Release 8.10.x. • LAG behind NAT or PAT environment
Protocols	• Full Cisco Compatible Extensions (CCX) support • Rogue Location Discovery Protocol (RLDP) • Telnet
Security	• CKIP, CMIC, and LEAP with Dynamic WEP • Static WEP for CKIP • WPA2 + TKIP **Note** WPA +TKIP and TKIP + AES protocols are supported.
Quality of Service	Cisco Air Time Fairness (ATF) **Note** ATF is supported in Cisco Aironet 2800, 3800, and 4800 Series APs in Release 8.10.
FlexConnect Features	• PPPoE • Multicast to Unicast (MC2UC) **Note** VideoStream is supported • Traffic Specification (TSpec) • Cisco Compatible eXtensions (CCX) • Call Admission Control (CAC) • VSA/Realm Match Authentication • SIP snooping with FlexConnect in local switching mode

Note For Cisco Aironet 1850 Series AP technical specifications with details on currently supported features, see the Cisco Aironet 1850 Series Access Points Data Sheet.

Key Features Not Supported in Cisco Aironet 1800i, 1810 OEAP, and 1810W Series APs

Table 8: Key Features Not Supported in Cisco Aironet 1800i, 1810 OEAP, and 1810W Series APs

Operational Modes	Mobility Express
FlexConnect Features	Local AP authentication
Location Services	Data RSSI (Fast Locate)

Key Features Not Supported in Cisco Aironet 1830, 1850, and 1815 Series APs

Table 9: Key Features Not Supported in Cisco Aironet 1830, 1850, and 1815 Series APs

Operational Modes	Mobility Express is not supported in Cisco 1815t APs.
FlexConnect Features	Local AP Authentication
Location Services	Data RSSI (Fast Locate)

Key Features Not Supported in Mesh Networks

- Load-based call admission control (CAC). Mesh networks support only bandwidth-based CAC or static CAC
- High availability (Fast heartbeat and primary discovery join timer)
- AP acting as supplicant with EAP-FASTv1 and 802.1X authentication
- AP join priority (Mesh APs have a fixed priority)
- Location-based services

Key Features Not Supported in Cisco Aironet 1540 Mesh APs

- Dynamic Mesh backhaul data rate.

Note We recommend that you keep the Bridge data rate of the AP as auto.

- Background scanning
- Noise-tolerant fast convergence

Key Features Not Supported on Cisco Aironet 1560 APs

- MAC Authentication FlexConnect Local Authentication
- Noise-tolerant fast convergence
- Static WEP

Key Features Not Supported on Cisco Catalyst IW6300 Heavy Duty Series AP and 6300 Series Embedded Services AP

- MAC Authentication FlexConnect Local Authentication
- Noise-tolerant fast convergence
- Static WEP

Unfixed and Fixed Issues in Release 8.10.190.0

Unfixed Issues in Release 8.10.190.0

Table 10: Unfixed Issues

Identifier	Headline
CSCwe63089	LED on AP's turning White randomly
CSCwe67810	COS-AP Flexconnect standalone disconnecting clients on DHCP renewal every 18 discovery req no reply
CSCwe76817	Cisco AP: CAPWAP MTU discovery issue
CSCwe80617	Wireless clients are unable to connect to 1830 AP after input or output error message
CSCwe82287	AP does not allow a PMF WPA3 client to associate after the client sent Deauthentication by itself.
CSCwe89429	2802AP dropped DHCP offer as AP is running out of memory
CSCwe91394	Aeroscout T15e Tags not reporting temp data due to extra bytes
CSCwe92462	Functional: Client Data Rate chart Chart skewed by Management rate rather than Data rate only
CSCwf07384	Wired client behind Cisco C9105 RLAN is not able to pass traffic
CSCwf13804	netlink_socket_receive multicast_group 1 return failure: No buffer space available errors are seen
CSCwf22246	Cisco Catalyst 9130 APs - Standardize calculation of mgmt frame count across AP chipsets
CSCwf32342	ARP forwarding for Fabric WLAN with passive client

Identifier	Headline
CSCwf53520	Cisco 1815 AP running version 17.9.2: Kernel panic crash observed
CSCwf63818	Cisco 1832 AP running version 17.9.2: Kernal Panic crash observed
CSCwf65794	Cisco 1852 AP reloads unexpectedly due to radio failure (radio recovery failed)
CSCwf83278	Cisco 9800 Ctlr: Client traffic fail with N+1 when AP sends CLIENT_DEL_STOP_REASSOC
CSCwf92148	9120 dual 5-GHz not disabling HE in slot 0 when WLAN configured had 11ax disabled slot 1 HE disabled

Fixed Issues in Release 8.10.190.0

Table 11: Fixed Issues

Identifier	Headline
CSCwe22861	Observing AID leak in Flex Cisco Wave 2 APs running 8.10.171.0
CSCwe30473	AP2800/3800/4800 Radio firmware reloads unexpectedly due to RC queue stuck
CSCwe73758	Cisco 9115 AX AP Beacon stuck on 5 GHz
CSCwe74653	AP not sending DELETE reason to the controller resulting in stale entries
CSCwe74874	C9120AP kernel panic with PC at ZN23CheckCapwapICMPNeedFrag4pushEiP6Packet
CSCwe87973	Cisco 3800 AP reloads unexpectedly due to FIQ/NMI reset / 8.10.183.0
CSCwe88418	Wireless Controller reporting SSH status wrongly for Access Points
CSCwe91264	AP reloads unexpectedly with PC is at get_partial_node.isra
CSCwe91301	AP reloads unexpectedly with PC & LR is at __udelay+0x30/0x48
CSCwf04748	AP reloads unexpectedly due to CALLBACK FULL Reset Radio
CSCwf11117	Cisco 9120 AP: rootAP deauths WGB continuously after roam
CSCwf15582	AP Radio reloads unexpectedly due to beacon stuck
CSCwf17655	Cisco 9130 AP running 17.3.7 radio crash
CSCwf18202	Cisco COS-APs are not encrypting EAP_ID_REQ after M1-M4
CSCwf25869	Radio core reloads unexpectedly due to TCQ stuck with frequent channel changes
CSCwf28105	Cisco 9130AX AP: Kernel Panic PC is at ol_ath_print_peer_refs+0x58/0x410 [qca_ol]
CSCwf29737	PMKID Generation mismatch when client roams from slot2 to other slot inter/intra AP

Identifier	Headline
CSCwf29742	Cisco 9120AP: Firmware Crashed While Running Multicast & Longeivity with 80+ clients(After 12 Hrs)
CSCwf45495	Cisco 9130 APs fail to start CAPWAP due to reset interface every 52s while DHCP process
CSCwf50177	C9105AXW - large number of bad blocks
CSCwf52815	Cisco COS-AP improve PMTU Discovery mechanism to be able to honor the ICMP unreachable MTU value
CSCwf64009	Cisco 1815 AP leaking RLAN VLAN traffic with looped port
CSCwf67316	2800/3800/4800/1560/IW6300 may not detect radar on the required levels after CAC time
CSCwf68131	C9105AXW -bad block monitoring and repair
CSCwf68209	AireOS/8.10 Ability to detect and delete stale without relying on DELETE payload from the AP
CSCwf95868	Single Band BCM WGB Radio 0 Tx power decrease by nearly 20dBm while configuring antenna number

Related Documentation

Wireless Products Comparison

- Use this tool to compare the specifications of Cisco wireless access points and controllers:

  https://www.cisco.com/c/en/us/products/wireless/wireless-lan-controller/product-comparison.html

- Product Approval Status:

  https://prdapp.cloudapps.cisco.com/cse/prdapp/jsp/externalsearch.do?action=externalsearch&page=EXTERNAL_SEARCH

- Wireless LAN Compliance Lookup:

  https://www.cisco.com/c/dam/assets/prod/wireless/wireless-compliance-tool/index.html

Cisco Wireless Controller

For more information about the controllers, lightweight APs, and mesh APs, see these documents:

- The quick start guide or the installation guide for your particular controller or access point
- Cisco Wireless Solutions Software Compatibility Matrix
- Cisco Legacy Wireless Solutions Software Compatibility Matrix
- Cisco Wireless Controller Configuration Guide
- Cisco Wireless Controller Command Reference
- Cisco Wireless Controller System Message Guide

For all controller software related documentation, see:

http://www.cisco.com/c/en/us/support/wireless/wireless-lan-controller-software/tsd-products-support-series-home.html

Cisco Mobility Express

- *Cisco Mobility Express Release Notes*
- *Cisco Mobility Express User Guide*
- *Cisco Aironet Universal AP Priming and Cisco AirProvision User Guide*

Cisco Aironet Access Points for Cisco IOS Releases

- *Release Notes for Cisco Aironet Access Points for Cisco IOS Releases*
- *Cisco IOS Configuration Guides for Autonomous Aironet Access Points*
- *Cisco IOS Command References for Autonomous Aironet Access Points*

Open Source Used in Controller and Access Point Software

Click this link to access the documents that describe the open source used in controller and access point software:

https://www.cisco.com/c/en/us/about/legal/open-source-documentation-responsive.html

Cisco Prime Infrastructure

Cisco Prime Infrastructure Documentation

Cisco Connected Mobile Experiences

Cisco Connected Mobile Experiences Documentation

Cisco Digital Network Architecture

https://www.cisco.com/c/en/us/support/wireless/dna-spaces/series.html

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 in the right pane of every online document.