



Release Notes for Cisco Wireless Controllers and Lightweight Access Points, Cisco Wireless Release 8.8.130.0

First Published: 2020-03-13

About the Release Notes

This release notes document describes what is new or changed in this release, instructions to upgrade to this release, and 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*.

Content Hub

Explore the [Content Hub](#), the all-new product documentation portal in which you can use faceted search to locate content that is most relevant to you, create customized PDFs for ready reference, benefit from context-based recommendations, and much more.

Get started with the Content Hub at <https://content.cisco.com/> to craft a personalized documentation experience.

Do provide feedback about your experience with the Content Hub.

Supported Cisco Wireless Controller Platforms

The following Cisco Wireless 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 Servers 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 WLC, Cisco 5520 WLC, and Cisco 8540 WLC.
- Cisco Mobility Express Solution

Supported Cisco Access Point Platforms

The following Cisco AP platforms are supported in this release:

- 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 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



Note

- 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 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 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 8.8.130.0

There are no new features that are introduced in this release. For more information about updates in this release, see the Caveats section in this document.



Note For complete listing of all the documentation published for Cisco Wireless Release 8.8, see the Documentation Roadmap:

<https://www.cisco.com/c/en/us/td/docs/wireless/doc-roadmap/doc-roadmap-release-88.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 8.8.x

Current Software Release	Upgrade Path to Release 8.8.x
8.2.x	You must upgrade to an 8.5.x release and then upgrade to Release 8.8.x.
8.3.x	You must upgrade to an 8.5.x release and then upgrade to Release 8.8.x.
8.4.x	You must upgrade to an 8.5.x release and then upgrade to Release 8.8.x.
8.5.x	You can upgrade directly to Release 8.8.x.
8.6.x	You can upgrade directly to Release 8.8.x.
8.7.x	You can upgrade directly to Release 8.8.x.

Upgrading 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.



Caution

Before you upgrade to this release, we recommend that you go through the following documents to understand various issues related to Cisco Wave 1 AP flash and the solution to address them:

- Field Notice: <https://www.cisco.com/c/en/us/support/docs/field-notices/703/fn70330.html>
- Understanding Various AP-IOS Flash Corruption Issues: <https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/213317-understanding-various-ap-ios-flash-corru.html>

Guidelines and Limitations

- Legacy clients that require RC4 or 3DES encryption types are not supported in Local EAP authentication.
- If you downgrade from Release 8.8.x to Release 8.7, FlexConnect IPv6 ACLs are shown to be in their FlexConnect group.
- If you have an AVC profile with *default-class* setting and you downgrade from Release 8.8.x to an earlier release, the *default-class* setting is still present in the controller, although the earlier releases do not support this setting.
- If you want to downgrade from Release 8.8.x to Release 8.6.101.0 and if you have Wave 2 APs in Flex+Bridge mode, ensure that these APs are changed to Bridge mode before you perform the downgrade; else, the APs will have incorrect configuration after the downgrade process.
- If you are upgrading from Release 8.0.140.0 or 8.0.15x.0 to a later release and also have the multiple country code feature configured, the feature configuration is corrupted after the upgrade. For more information, see [CSCve41740](#).

- 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 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 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 controller or any AP during the upgrade process. If you do this, the software image might get corrupted. Upgrading 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 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.

- From Release 8.3 or a later release, ensure that the configuration file that you back up does not contain the < or > special characters. If either of the special characters is present, the download of the backed up configuration file fails.

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, or SFTP 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, or SFTP**.
- Step 8** In the **IP Address** field, enter the IP address of the TFTP, FTP, or SFTP server.
- Step 9** If you are using a TFTP server, the default value of 10 retries for the **Maximum Retries** field, and 6 seconds for the **Timeout** field should work correctly without any adjustment. However, you can change these values, if required. To do so, enter the maximum number of times the TFTP server attempts to download the software

in the **Maximum Retries** field and the amount of time (in seconds) for which the TFTP server attempts to download the software, in the **Timeout** field.

Step 10 In the **File Path** field, enter the directory path of the software.

Step 11 In the **File Name** field, enter the name of the software file *<filename.aes>*.

Step 12 If you are using an FTP server, perform these steps:

- a) In the **Server Login Username** field, enter the username with which to log on to the FTP server.
- b) In the **Server Login Password** field, enter the password with which to log on to the FTP server.
- c) In the **Server Port Number** field, enter the port number on the FTP server through which the download occurs. The default value is 21.

Step 13 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 14 After the download is complete, click **Reboot**.

Step 15 If you are prompted to save your changes, click **Save and Reboot**.

Step 16 Click **OK** to confirm your decision to reboot the controller.

Step 17 If you have disabled the 802.11 networks, reenable them.

Step 18 (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 Version 3.0(4d) 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 CIMC 3.0(4d) images are available at the following locations

Table 3: CIMC Utility Software Image Information

Controller	Link to Download the CIMC Utility Software Image
Cisco 5520 Wireless Controller	https://software.cisco.com/download/home/286281345/type/283850974/release/3.0%25284d%2529
Cisco 8540 Wireless Controller	https://software.cisco.com/download/home/286281356/type/283850974/release/3.0%25284d%2529

For information about upgrading the CIMC utility, see the "Updating the Firmware on Cisco UCS C-Series Servers" chapter in the *Cisco Host Upgrade Utility 3.0 User Guide*:

https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/c/sw/lomug/2-0-x/3_0/b_huu_3_0_1/b_huu_2_0_13_chapter_011.html

Updating Firmware Using the Update All Option

This section mentions specific details when using CIMC utility with Cisco 5520 or 8540 controllers. For general information about the software and UCS chassis, see *Release Notes for Cisco UCS C-Series Software, Release 3.0(4)* at:

https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/release/notes/b_UCS_C-Series_Release_Notes_3_0_4.html

Table 4: Open Caveats for Release 3.0(4d)

Caveat ID	Description
CSCvj80941	After upgrading CIMC to 3.04d, only after power reset, UCS-based controller is coming up.
CSCvj80915	Not able to logon to the CIMC GUI with the username and password that are configured from the controller.

Table 5: Resolved Caveats for Release 3.0(4d)

Caveat ID	Description
CSCvd86049	<p>Symptom: The system will stop working or reboot during OS operation with PROCHOT, MEMHOT, and DMI Timeout-related events reported in the System Event Log (SEL).</p> <p>Conditions: C220-M4 or C240-M4</p> <p>Workaround: No workaround is available.</p> <p>This bug fix changes the default BIOS option for ASPM (Active State Power Management) from 'L1 only' to 'Disabled', and the ASPM setting can no longer be modified. This change was made to help increase system stability and eliminate some system crash scenarios.</p>

Caveat ID	Description
CSCvf78458	<p>Symptom: The system will stop working or reboot during OS operation with PROCHOT, MEMHOT, and DMI Timeout-related events reported in the System Event Log (SEL).</p> <p>Conditions: C220-M4 or C240-M4</p> <p>Workaround: No workaround is available.</p> <p>This bug fix changes the BIOS option "Package C-State limit" default value from C6 Retention to C0/C1 to help increase system stability and eliminate some crash scenarios.</p> <p>Once upgraded, reset the BIOS settings to default or manually change Package C-State limit to C0/C1.</p>

Interoperability with Other Clients

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

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

Table 6: Test Bed Configuration for Interoperability

Hardware or Software Parameter	Hardware or Software Configuration Type
Release	8.8.x.
Cisco Wireless Controller	Cisco 5520 Wireless Controller
Access Points	AIR-CAP3802E-B-K9, AIR-AP1852E-B-K9
Radio	802.11ac, 802.11a, 802.11g, 802.11n (2.4 GHz or 5 GHz)
Security	Open, PSK (WPA-TKIP-WPA2-AES), 802.1X (WPA-TKIP-WPA2-AES) (EAP-FAST, EAP-TLS)
RADIUS	Cisco ACS 5.3, Cisco ISE 2.2, Cisco ISE 2.3
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, handheld devices, phones, and printers.

Table 7: Client Types

Client Type and Name	Driver / Software Version
Laptops	

Client Type and Name	Driver / Software Version
Acer Aspire 15 Windows 8 Home	Qc Atheros Qca9377 11.0.0.492
Acer Aspire E15 Windows 8	Qc Atheros Qca9377 15.1.1.1
Acer Aspire E 15 Windows 8.1	QC Atheros Qca9377 11.0.0.492
Acer Aspire E15 Windows 8.1 Pro	Qc Atheros Qca9377 11.0.0.492
Dell Inspiron 15 7569 Windows 10 Home	Ntel Ac 3165 18.32.0.5
Dell Latitude 6430 Windows 8.1 Pro	Intel 6205w8 15.16.0.2
Dell Latitude E5430 Windows 7	Intel Centrino N 6205 15.17.0.1
Dell Latitude E5450 Windows 7 Professional	Intel 7260 18.33.6.2
Dell Latitude E5540 Windows 7	Intel Dualband Ac7260 1.566.0.0
Dell Latitude E6430 Windows 7 Professional	Intel Centrino Ultm6300 15.9.2.1
Dell Latitude E6430 Windows 7 Professional	Intel 6250 15.11.0.7
Dell Latitude E6430 Windows 7 Professional	Intel 3160 6.30.223.215
Dell Latitude E7450 Windows 7 Professional	Broadcom 1560 15.1.1.1
Dell Latitude Windows 8.1 Pro	Intel Ac7260 18.33.3.2
Fujitsu Lifebook E556 Windows 10 Pro	Intel 8260 11.0.0.492
Lenovo Yoga 460 Windows 10 Pro	Intel Ac8260 19.1.0.4
Macbook Air Mac OS Sierra 10.12.3	Broadcom Bcm43xx 1.0 6.30.225.29.1
Macbook Air MacOS Sierra 10.12.6	Broadcom Bcm43xx 1.0 7.21.171.68.1a4
Macbook Air OS X Yosemite (10.10.5)	Broadcom Bcm43xx 1.0 7.15.166.24.3
Macbook Mac OS Sierra 10.12 Beta	Broadcom Bcm43xx 1.0 7.21.149.34.1a7
Macbook Pro Mac OS Sierra 10.12.4	Broadcom Bcm43xx 1.0 7.21.171.68.1a4
Macbook Pro OS X 10.8.5	Broadcom Bcm43xx 1.0 5.106.98.100.17
Macbook Pro Retina Mac OS Sierra 10.12.3	Broadcom Bcm43xx 1.0 7.15.166.24.3
Tablets	
Apple iPad	iOS 9.3.1
Apple iPad mini	iOS 12.0
Apple iPad mini 2	iOS 10.3.1
Apple iPad Air	iOS 10.1.1
Apple iPad Air 2	iOS 10.2.1
Mobile Phones	
Apple iPhone 4S	iOS 8.0
Apple iPhone 5	iOS 10.3.1

Client Type and Name	Driver / Software Version
Apple iPhone 5C	iOS 9.3.2
Apple iPhone 6 Plus	iOS 12.0
Apple iPhone SE	iOS 10.3.1
AT100	Toshiba Android 4.0.4
Cisco 7925G-EX	CP7925G-1.4.8.4.LOADS
Cisco 7926G	CP7925G-1.4.8.4.LOADS
Cisco 8821	sip8821.11-0-4-14
ET1	Android VERSION 2.3.4
ET5	Android 5.1.1
LG-D855	LG Android 5.0
Mediapad X1 7.0	Huawei Android 4.4.2
Moto X 2nd Gen	Motorola Android 5.0
One Plus One	One Plus Android 4.3
One Plus Three	One Plus Android 6.0.1
Samsung Galaxy S4	Samsung Android 4.2.2
Samsung Galaxy S4	Samsung Android 5.0.1
Samsung Galaxy S6	Samsung Android 7.0
Samsung Galaxy S6	Samsung Android 6.0.1
Samsung Galaxy S8	Samsung Android 7.0
Samsung Tab Pro	Samsung Android 4.4.2
SM-P600	Samsung Android 4.4.2
SM-T520	Samsung Android 4.4.2
TC510K	Zebra Android 6.0.1
TC8000	Zebra Android 4.4.3
8742	Spectralink Android 5.1.1
8744	Spectralink Android 5.1.1 2.5.0

Key Features Not Supported in Cisco WLC Platforms

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



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

Key Features Not Supported in Cisco 3504 WLC

- 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 WLCs

- 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 WLC

- 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 Cisco WLC 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
- Cisco WLC integration with Lync SDN API
- Cisco OfficeExtend Access Points

Key Features Not Supported in Access Point Platforms

This section lists the features that are not supported on various Cisco Aironet AP platforms:

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

For detailed information about feature support on Cisco Aironet Wave 2 APs, see:

https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-7/b_feature_matrix_for_802_11ac_wave2_access_points.html.

Table 8: Key Features Not Supported in Cisco Aironet 1800i, 1810 OEAP, 1810W, 1815, 1830, 1850, 2800, 3800, and 4800 Series APs

Operational Modes	<ul style="list-style-type: none"> • Autonomous Bridge mode • Mesh mode • LAG behind NAT or PAT environment
Protocols	<ul style="list-style-type: none"> • Full Cisco Compatible Extensions (CCX) support • Rogue Location Discovery Protocol (RLDP) • Telnet • Internet Group Management Protocol (IGMP)v3

Security	<ul style="list-style-type: none"> • CKIP, CMIC, and LEAP with Dynamic WEP • Static WEP for CKIP • WPA2 + TKIP <p>Note WPA +TKIP and TKIP + AES protocols are supported.</p>
Quality of Service	Cisco Air Time Fairness (ATF)
FlexConnect Features	<ul style="list-style-type: none"> • Split Tunneling • PPPoE • Multicast to Unicast (MC2UC) <p>Note VideoStream is supported</p> <ul style="list-style-type: none"> • Traffic Specification (TSpec) <ul style="list-style-type: none"> • 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 9: Key Features Not Supported in Cisco Aironet 1800i, 1810 OEAP and 1810W Series APs

Operational Modes	<ul style="list-style-type: none"> • Workgroup Bridge (WGB) mode • 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 10: Key Features Not Supported in Cisco Aironet 1830, 1850, and 1815 Series APs

Operational Modes	<ul style="list-style-type: none"> • Workgroup Bridge (WGB) mode • 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

Caveats

Open Caveats

Table 11: Open Caveats for Release 8.8.130.0

Caveat ID Number	Description
CSCvk53499	Cisco APs do not reconnect, error log: System reached max concurrent DTLS Handshakes
CSCvm63736	Erratic multicast throughput
CSCvm65411	Cisco 2700 AP radio resets with FC71 code
CSCvm68341	Cisco controller is sending duplicate interim accounting packets to ISE
CSCvm72007	Incorrect VLAN mapping when using MAC filtering and PSK
CSCvm93785	Cisco 2800, 3800 AP reloads unexpectedly on Click: Client update cache from write handler
CSCvn15777	Silent reload, high CPU util on emWeb process, with Lync Server enabled
CSCvn21425	Cisco 2800 3800 APs not responding to dot11 association frames
CSCvn56211	Cisco 702W AP radio resets, tracebacks and other radio buffer errors
CSCvn79255	Cisco controller reloads unexpectedly with task emweb after Opening VLAN Mappings on GUI
CSCvn91965	WLC reloads with reason DP Buffer shortage (CP detected)
CSCvn99809	Handling PAK scheduler during AID plumbing
CSCvo17872	Cisco 3800 AP running 8.5.140.0: FIQ/NMI reloads unexpectedly
CSCvo18663	Native VLAN Inheritance is changed after controller switchover
CSCvo24010	2.4 GHz Rogue clients stay in containment pending
CSCvo31548	Cisco IW3702 AP and 3702 AP WGB reloads unexpectedly on 15.3(3)JF9 with PEAP authentication
CSCvo37232	WLC - configuration of some WLANs is not listed in 'show run-config'
CSCvo48363	Cisco controller reloads unexpectedly when viewing multicast MGID in GUI
CSCvo51266	EAP TLS fails with WGB
CSCvp11765	Wireless client fail to associate to Cisco 1830 APs until reboot
CSCvp21915	RSN IE length mismatch between assoc and EAPOL-M2 frame

Caveat ID Number	Description
CSCvp41629	Regulatory domains of 802.11bg changes to -A after slot 0 switches 5 GHz
CSCvp58062	Cisco 1800 series AP Radio core dump due to beacon stuck FW hang
CSCvp66546	Cisco 702w AP Radio reset due to Tx stuck
CSCvp68494	Cisco 2800 AP reloads unexpectedly due to exception when having MU-MIMO clients in network
CSCvp82961	Cisco 2800 AP in local mode running 8.5.144.33: AID cannot be freed
CSCvr43311	Unable to set syslog login level to all the APs "Unable to set the Log Trap level"

Resolved Caveats

Table 12: Resolved Caveats in Release 8.8.130.0

Caveat ID Number	Description
CSCvh68195	8.8: 5520 Tracebacks observed 0x135956f 0x135af79 0x1362144 0x12ee263 0x3ba6c07dff 0x7f4ede3a439d
CSCvi48253	Self-signed certificates expire on 00:00 1 Jan 2020 UTC, cannot be created after that time
CSCvk66445	Cisco Wave 2 AP tags UP6 as DSCP63 on the Wired side in CAPWAP header on 8.8MR2
CSCvm22760	Dot1x supplicant config is not removed from Cisco Wave 1 AP, after disabled globally on controller.
CSCvm66185	During AP Boot the AP sends 3 dhcp releases causing BAD_ADDRESS on Windows Server 2016
CSCvm68624	Cisco Wave 1 AP console displays 'DTX DUMP' logs
CSCvm75937	Cisco controller reloads in TransferTask; flood of "Starting NA Connector" messages
CSCvn87656	Cisco Wave 2 APs reloads unexpectedly in the context of vendor driver @ click_packet_type_event_hook
CSCvo26217	Fabric Enabled Wireless: Cisco 5520 WLC does not reconnect to CP
CSCvo35484	RTS threshold is zero in show CAPWAP client config; excessive RTS sent; client connectivity problems
CSCvo59784	Cisco AP usage shows discrepancy through pages
CSCvp00688	Cisco 2800, 3800 AP radio reloads unexpectedly
CSCvp01439	Cisco 1815 AP leaking RLAN VLAN traffic when port looped

Caveat ID Number	Description
CSCvp25089	Multicast Traffic stops working when enabling Inline Tagging on CTS with Cisco Wave 1 APs
CSCvp26672	Cisco 702 APs fail to authenticate clients due to decrypt error on the AP
CSCvp30608	Cisco Wave2 AP with data DTLS encryption drop out of order CAPWAP data packets
CSCvp72309	Cisco 3800 AP stops passing traffic under client load Intel NIC 8260/8265 load in MU-MIMO deployment
CSCvp76453	Traceback : APF-3-NO_FRAMED_IP_ADDRESS: on Acct Start and Interim while running scale test
CSCvp86151	Cisco Wave1 APs radio reset with code 44, mostly seen on 2.4GHz radio
CSCvp92098	Cisco Wireless LAN Controller HTTP Parsing Engine Denial of Service Vulnerability
CSCvq00695	Cisco 3700 AP does not perform DFS CAC after radio is admin down for over a minute
CSCvq14112	Cisco 1832 AP showing up as "low power" when using a PWRINJ5
CSCvq23385	Cisco AP reloads unexpectedly on WCPD
CSCvq25654	Cisco 2702 AP sent deauthentication to multicast MAC address
CSCvq26205	Cisco 3504 controller on 8.10 release: system reloads unexpectedly with task dx_sync_task
CSCvq27679	Cisco 1572AP: Radio reset due to pak count mismatch, false detection
CSCvq59683	Cisco Wireless LAN Controller Path Traversal Vulnerability
CSCvq63117	Client can not send the traffic, when two clients in different VNID joins the network
CSCvq66030	Cisco IOS and Cisco IOS XE Software Web UI Cross-Site Request Forgery Vulnerability
CSCvq66811	Cisco Wave 1 AP goes out of memory and fails to reply to assoc/reassoc from clients
CSCvq81315	Cisco 2700 AP PCI0 reloads unexpectedly when Cisco CleanAir is enabled
CSCvq81388	Wave1 AP resetting 5GHz radio often with radio reset code 44, messages with "DTX marked with poison"
CSCvq83205	After AP-SSO failover, WLC fails to send EAPOL M1
CSCvq87566	Cisco Wave 2 APs drop client ARP packets with Cisco FlexConnect ARP caching disabled
CSCvr08411	Cisco 2800 APs in WGB mode not able to join 802.1x SSID
CSCvr28017	Cisco WLC does not show -A regulatory domain for 5 GHz radio with country code PA (Panama)

Caveat ID Number	Description
CSCvr33340	Wave 2 APs in FlexConnect mode sending Auth Request to AAA without Local Auth Enabled
CSCvr33658	Configured AP Group Hyperlocation NTP server configuration not being pushed to AP4800s
CSCvr35607	WLC displays login banner after login, not before login like in older codes
CSCvr36185	Cisco 2800 series APs are using 802.11n rates with WPA+TKIP only WLAN
CSCvr38675	Client connectivity failure seen after LAN link flap
CSCvr39587	MAPs failing mesh_sec_auth and excluding Parent upon RAP failure
CSCvr47668	Cisco 3504 controller port 5 not working unless LAG is enabled
CSCvr62819	Cisco 1815W AP on Cisco release 8.9.111.0 & 8.10.104.148 in OEAP mode - wired traffic fails
CSCvr71272	Cisco 3504 WLC: Free Timer Depletion leads to WLC unexpectedly reloading and clients cannot connect
CSCvr75831	Few Cisco Wave 1 AP client is loosing connectivity on roaming
CSCvr76299	Decipher Radio reset code 44 to more specific reason codes
CSCvr82520	Cisco Wave 1 AP Software reloads unexpectedly when configuring a long SNMP-server community string
CSCvr97368	HTTPS and SSH traffic dead slow with CTS inline tagging enabled
CSCvs01333	Cisco Controller sending incorrect certificate password for Cisco FlexConnect local auth EAP-TLS
CSCvs09716	Cisco AP is not handling EXPIRE_MIC_PAYLOAD message
CSCvs16432	Cisco AireOS Controller reloads unexpectedly on IPv6_Msg_Task
CSCvs22835	Cisco AP with SHA2 MIC certificate fails to join WLC with config ap cert-expiry-ignore mic enable
CSCvs27550	Cisco 1815 AP Kernel Panic pointing to Ethernet driver with large size packet traffic
CSCvs49779	HA: Cisco controller on 8.8 software rebooting due to peer Redundancy Port Keep Alives loss
CSCvs79813	Cisco Wave 1 APs still stuck in the downloading state

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 Cisco WLCs, lightweight APs, and mesh APs, see these documents:

- The quick start guide or installation guide for your particular Cisco WLC or access point
- [Cisco Wireless Solutions Software Compatibility Matrix](#)
- [Cisco Wireless Controller Configuration Guide](#)
- [Cisco Wireless Controller Command Reference](#)
- [Cisco Wireless Controller System Message Guide](#)

For all Cisco WLC 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 Mobility Services Engine

[Cisco Mobility Services Engine Documentation](#)

Cisco Connected Mobile Experiences

[Cisco Connected Mobile Experiences Documentation](#)

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 Marketplace](#).
- 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 web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.

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](http://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)

© 2020 Cisco Systems, Inc. All rights reserved.