Release Notes for Cisco Wireless Controllers and Lightweight Access Points, Cisco Wireless Release 8.7.102.0

First Published: 2018-04-20

Last Modified: 2019-05-16

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.

Revison History

Table 1: Revision History

Modification Date	Modification Details
January 30, 2019	Added a note about issues related to Cisco Wave 1 AP flash and the solution to address them in the Upgrading Cisco Wireless Release section.
October 30, 2018	Open Caveats—Added CSCvi97023, CSCvj95336, CSCvi49059 Resolved Caveats—Added CSCvh65876, CSCvf66680, CSCvf66696, CSCve64652, CSCvf66723, CSCvh21953
July 24, 2018	Added the CIMC Utility Upgrade for 5520 and 8540 Controllers section.

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 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 8.7.102.0

This section provides a brief introduction to the new features and enhancements introduced in this release.

Note For complete listing of all the documentation published for Cisco Wireless Release 8.7, see the Documentation Roadmap:

https://www.cisco.com/c/en/us/td/docs/wireless/doc-roadmap/doc-roadmap-release-87.html

Cisco Wave 2 AP Features

- **Managing BLE Beacons in Cisco Wave 2 APs**—BLE beacons are battery-powered, low-cost transmitters integrated with Cisco Wave 2 AP radios and can be used to transmit proximity-based, context-aware messages to enhance location services for mobile devices.

  For more information, see the "Managing BLE Beacons in Cisco Wave 2 APs" section in the *Cisco Wireless Controller Configuration Guide*.

- **802.1X Support for EAP-TLS and EAP-PEAP**—In this release, 802.1X support is extended to EAP-TLS and PEAP methods along with EAP-FAST method in Cisco Wave 2 APs.

  Prior to this release, EAP-FAST was the only supported 802.1X AP switchport authentication method.

  EAP-TLS and PEAP methods are supported only in Cisco Wave 2 APs. Cisco Wave 1 APs support only EAP-FAST method.

  For more information, see the "AP 802.1X Supplicant" section in the *Cisco Wireless Controller Configuration Guide*.

- **AUX Ethernet Port Enabled on Cisco Wave 2 APs**—The second Ethernet port, also called the AUX port, of Cisco Aironet 1850, 2800, and 3800 Series APs is, by default, used as a link aggregation (LAG) port. It is possible to use this LAG port as a LAN port when LAG is disabled. When the AUX port is configured as a LAN port, you can either use the AP group setting to configure the LAN port for a group of APs or use the LAN override functionality to configure the LAN port for each AP separately.

  For more information, see the "Converting Cisco Wave 2 AP AUX Port to LAN Port (CLI)" section in the *Cisco Wireless Controller Configuration Guide*.

- The following features, which are already supported in Wave 1 APs, are supported in Wave 2 APs in this release:
  - DHCP Option 60
  - Limit clients per AP radio or per WLAN per AP radio
  - Passive clients
  - Proxy ARP
  - FlexConnect Ethernet fallback
  - AAA override of VLAN name, VLAN name ID template for FlexConnect local authentication
  - AAA override for bidirectional rate limit per client or BSSID
  - Management Frame Protection

IPv4 DNS-Based Access Control List Filtering for BYOD

This feature extends FlexConnect ACL to accept internet domain names in addition to the existing IP addresses in its rules. This provides the flexibility of matching traffic based on the destination URL rather than the IP addresses associated with the URL.

In this release, this feature is also supported on Software-Defined Accesss Wireless (Fabric).

For more information, see the "FlexConnect ACLs" section in the *Cisco Wireless Controller Configuration Guide*.

Enhancement to High Availability Monitoring and Management

Monitoring and management of high availability standby WLC is enhanced to display the serial number and fan status of the standby WLC:

- GUI—The new statistics are displayed on the **Monitor** > **Redundancy** > **Peer Statistics** page.
- CLI—The **show redundancy peer-system statistics** command displays the new statistics.

Encrypted Mobility Tunnel

A secure link called the encrypted mobility tunnel, which is based on the mobility tunnel and is encrypted using CAPWAP DTLS protocol, can be established between an anchor and a foreign Cisco WLC. The encrypted mobility tunnel feature is supported in high availability (HA) client SSO scenarios.

For more information, see the "Encrypted Mobility Tunnel" chapter in the *Cisco Wireless Controller Configuration Guide*.

Enhancement to RxSOP Threshold Configuration

Prior to this release, if you configured RxSOP threshold on Cisco WLC CLI to a custom value, the Cisco WLC GUI would reflect the threshold value as *AUTO*. In this release, an option is provided on Cisco WLC GUI to configure a custom RxSOP threshold value.

For more information, see the "Receiver Start of Packet Detection Threshold (Rx-SOP)" section in the *Cisco Wireless Controller Configuration Guide*.

Enable Cisco CleanAir, Disable BLE Detection by Default

Prior to this release, if Cisco CleanAir was enabled, by default, the BLE beacon was included in the list of interferences to be detected. In this release, the functionality is changed wherein the BLE beacon is, by default, excluded from the list of interferences to be detected. This change in functionality is made to eliminate unwanted off-channel scans to improve performance. If you want the BLE beacon to be detected, you must explicitly add it to the list of interferences to be detected.

NMSP by AP Groups with Subscription List from CMX

In this release, support is added to send only the required Network Mobility Services Protocol (NMSP) data to Cisco Connected Mobile Experiences (CMX) (applicable to both on-premise and cloud-based Cisco CMX). Cisco CMX can subscribe to NMSP data of specific APs or AP groups based on the active services in Cisco WLC.

For more information, see the "NMSP by AP Groups with Subscription List from CMX" section in the *Cisco Wireless Controller Configuration Guide*.

Software Release Types and Recommendations

Table 2: 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 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 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 3: Upgrade Path to Cisco WLC Software Release 8.7.102.0

Current Software Release	Upgrade Path to Release 8.7.102.0
8.5.x.x	You can upgrade directly to Release 8.7.102.0
8.6.x.x	You can upgrade directly to Release 8.7.102.0

Upgrading Cisco Wireless Release

This section describes the guidelines and limitations that you need to be aware of when you are upgrading the Cisco WLC software and the procedure to upgrade to this release.

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.
- This release supports additional configuration options for 802.11r FT enable and disable. The additional configuration option is not valid for releases earlier than Release 8.4. If you downgrade from Release 8.7 to Release 8.2 or an earlier release, the additional configuration option is invalidated and defaulted to FT disable. When you reboot Cisco WLC with the downgraded image, invalid configurations are printed on the console. We recommend that you ignore this because there is no functional impact, and the configuration defaults to FT disable.
- If you downgrade from Release 8.7 to a 7.x release, the trap configuration is lost and must be reconfigured.
- 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 Cisco WLC to download a new image or to reboot Cisco WLC after the download of the new image. You can forcefully reboot Cisco WLC by entering the **reset system forced** command.
- It is not possible to download some of the older configurations from Cisco WLC 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.
- If you upgrade from Release 8.0.110.0 to a later release, the **config redundancy mobilitymac** *mac-addr* command's setting is removed. You must manually reconfigure the mobility MAC address after the upgrade.

- 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.
- If you are upgrading from a 7.4.x or an earlier release to a release later than 7.4, the Called Station ID type information is mapped to the RADIUS Accounting Called Station ID type, which, by default, is set to apradio-mac-ssid. You can configure the RADIUS Authentication Called Station ID type information by using the **config radius auth callStationIdType** command.
- When a client sends an HTTP request, the Cisco WLC intercepts it for redirection to the login page. If the HTTP GET request that is intercepted by the Cisco WLC is longer than 2000 bytes, the Cisco WLC drops the packet. Track the Caveat ID CSCuy81133 for a possible enhancement to address this restriction.
- When downgrading from one release to another, you might lose the configuration from your current release. The workaround is to reload the previous Cisco WLC configuration files that are saved in the backup server, or to reconfigure Cisco WLC.
- When you upgrade Cisco WLC to an intermediate release, wait until all the APs that are associated with Cisco WLC are upgraded to the intermediate release before you install the latest Cisco WLC 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 Cisco WLC 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 Cisco WLC is also automatically upgraded. When an AP is loading software, each of its LEDs blinks in succession.
- Cisco WLCs support standard SNMP MIB files. MIBs can be downloaded from the software download page on Cisco.com.
- The Cisco WLC software is factory installed on your Cisco WLC and is automatically downloaded to the APs after a release upgrade and whenever an AP joins a Cisco WLC. 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 Cisco WLC 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 Cisco WLC 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 Cisco WLC 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 Cisco WLC.
- 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 Cisco WLC.

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 Cisco WLC or any AP during the upgrade process. If you do this, the software image might get corrupted. Upgrading Cisco WLC 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 Cisco WLC must not be reset during this time.
- To downgrade from this release to Release 6.0 or an earlier release, perform either of these tasks:
  - Delete all the WLANs that are mapped to interface groups, and create new ones.
  - Ensure that all the WLANs are mapped to interfaces rather than interface groups.
- After you perform the following functions on Cisco WLC, 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 WLC Software (GUI)

Procedure

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

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

Step 2 Follow these steps to obtain Cisco Wireless software:

a) Browse to Cisco Software Central at: https://software.cisco.com/download/navigator.html.
b) Click **Software Download**.
c) On the **Download Software** page, choose **Wireless** > **Wireless LAN Controller**.

The following options are displayed. Depending on your Cisco WLC platform, select one of these options:

- **Integrated Controllers and Controller Modules**
- **Mobility Express**
- **Standalone Controllers**

d) Select the Cisco WLC model number or name.
e) Click **Wireless LAN Controller Software**.
f) The software releases are labeled as described here to help you determine which release to download. Click a Cisco WLC 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.

g) Click the filename <*filename.aes*>.
h) Click **Download**.
i) Read the Cisco End User Software License Agreement and click **Agree**.
j) Save the file to your hard drive.
k) Repeat steps *a* through *j* to download the remaining file.

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

Step 4 (Optional) Disable the Cisco WLC 802.11 networks.

Note For busy networks, Cisco WLCs on high utilization, and small Cisco WLC 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 Cisco WLC.

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 Cisco WLC.

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

Step 18 (Optional) To verify that the Cisco WLC software is installed on your Cisco WLC, on the Cisco WLC 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 4: 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 5: 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 6: Resolved Caveats for Release 3.0(4d)

Caveat ID	Description
CSCvd86049	**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). **Conditions**: C220-M4 or C240-M4 **Workaround**: No workaround is available. 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.
CSCvf78458	**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). **Conditions**: C220-M4 or C240-M4 **Workaround**: No workaround is available. 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. Once upgraded, reset the BIOS settings to default or manually change Package C-State limit to C0/C1.

Interoperability with Other Clients

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

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

Table 7: Test Bed Configuration for Interoperability

Hardware or Software Parameter	Hardware or Software Configuration Type
Release	8.7.102.0
Cisco WLC	Cisco 5520 Wireless Controller
Access Points	AIR-CAP3802E-B-K9, AIR-AP1852E-B-K9, AIR-CAP3602E-A-K9

Hardware or Software Parameter	Hardware or Software Configuration Type
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 8: Client Types

Client Type and Name	Version
Laptop	
Intel 6300	15.16.0.2
Intel 6205	15.16.0.2
Intel 7260	18.33.3.2
Intel 7265	19.10.1.2
Intel 3160	18.40.0.9
Intel 8260	19.10.1.2
Broadcom 4360	6.30.163.2005
Dell 1520/Broadcom 43224HMS	5.60.48.18
Dell 1530 (Broadcom BCM4359)	5.100.235.12
Dell 1560	6.30.223.262
Dell 1540	6.30.223.215
Samsung Chromebook	55.0.2883.103
HP Chromebook	55.0.2883.103
MacBook Pro	OSX 10.11.6
MacBook Air	OSX 10.11.5
Macbook Pro with Retina Display	OSX 10.12
Macbook New 2015	OSX 10.12.4
Printers	
HP Color LaserJet Pro M452nw	2.4.0.125
Tablets	

Client Type and Name	Version
Apple iPad2	iOS 10
Apple iPad3	iOS 10
Apple iPad mini with Retina display	iOS 10
Apple iPad Air	iOS 10
Apple iPad Air 2	iOS 11
Apple iPad Pro	iOS 11
Samsung Galaxy Tab Pro SM-T320	Android 4.4.2
Samsung Galaxy Tab 10.1- 2014 SM-P600	Android 4.4.2
Samsung Galaxy Note 3 - SM-N900	Android 5.0
Microsoft Surface Pro 3	Windows 8.1
	Driver: 15.68.3093.197
Microsoft Surface Pro 2	Windows 8.1
	Driver: 14.69.24039.134
Microsoft Surface Pro 4	Windows 10
	Driver: 15.68.9040.67
Google Nexus 9	Android 6.0.1
Google 10.2" Pixel C	Andriod 7.1.1
Toshiba Thrive AT105	Android 4.0.4
Mobile Phones	
Cisco 7926G	CP7925G-1.4.5.3.LOADS
Cisco 7925G-EX	CP7925G-1.4.8.4.LOADS
Cisco 8861	Sip88xx.10-2-1-16
Cisco-9971	sip9971.9-4-1-9
Cisco-8821	sip8821.11-0-3ES2-1
Apple iPhone 4S	iOS 10.2.1
Apple iPhone 5	iOS 10.2.1
Apple iPhone 5s	iOS 10.2.1
Apple iPhone 5c	iOS 10.3.1
Apple iPhone 6	iOS 10.3.1
Apple iPhone 6 Plus	iOS 10.3.1
Apple iPhone 6s	iOS 10.2.1
Apple iPhone 7	iOS 11.0.3

Client Type and Name	Version
Apple iPhone X	iOS 11.1.2
HTC One	Android 5.0
OnePlusOne	Android 4.3
OnePlus3	Android 6.0.1
Samsung Galaxy S4 T-I9500	Android 5.0.1
Sony Xperia Z Ultra	Android 4.4.2
Nokia Lumia 1520	Windows Phone 8.10.14219.341
Google Nexus 5	Android 6.0.1
Google Nexus 5X	Android 8.0.0
Google Pixel	Android 7.1.1
Samsung Galaxy S5-SM-G900A	Android 4.4.2
Samsung Galaxy S III	Android 4.3
Samsung Galaxy S4	Android 5.0.1
Samsung Galaxy S5	Android 4.4.2
Samsung Galaxy S6	Android 7.0
Samsung Galaxy S7	Android 7.0
Samsung Galaxy Nexus GTI9200	Android 4.4.2
Samsung Galaxy Mega SM900	Android 4.4.2
LG G4	Android 5.1
Xiaomi Mi 4c	Android 5.1
Xiaomi Mi 4i	Android 6.0.1

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 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
- 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.

- Local 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 features that are not supported on various Cisco Aironet AP platforms:

Key Features Not Supported in Cisco Aironet 1540, 1560, 1800i, 1810 OEAP, 1810W, 1815, 1830, 1850, 2800, and 3800 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/8-6/b_feature_matrix_for_802_11ac_wave2_access_points.html.

Table 9: Key Features Not Supported in Cisco Aironet 1540, 1560, 1800i, 1810 OEAP, 1810W, 1815, 1830, 1850, 2800, and 3800 Series APs

Operational Modes	• Autonomous Bridge and Workgroup Bridge (WGB) mode • Mesh mode **Note** Supported on 1540 and 1560 APs. • Flex + Mesh • LAG behind NAT or PAT environment
Protocols	• Full Cisco Compatible Extensions (CCX) support • Rogue Location Discovery Protocol (RLDP) • Telnet • Internet Group Management Protocol (IGMP)v3
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)

FlexConnect Features	• Split Tunneling
	• PPPoE
	• Multicast to Unicast (MC2UC)
	• Traffic Specification (TSpec)
	  • Cisco Compatible eXtensions (CCX)
	  • Call Admission Control (CAC)
	• VSA/Realm Match Authentication
	• Link aggregation (LAG)
	• 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 10: Key Features Not Supported in Cisco Aironet 1800i, 1810 OEAP and 1810W Series APs

Operational Modes	Cisco 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 11: 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
- Flex+Mesh

Key Features Not Supported on Cisco Aironet 1560 Mesh APs

- Noise-tolerant fast convergence
- Flex+Mesh

Caveats

Open Caveats

Table 12: Open Caveats

Caveat ID Number	Description
CSCvb26809	WLC should use port MAC for non LAG and box MAC for LAG
CSCvc62540	Smart Licensing "Next Communication Attempt" pre-dates the Controller time after reboot
CSCvf89335	3700 AP stopped working with Memory Allocation Failure CAPWAP
CSCvf99887	MAP gigabit port being learnt in mesh management VLAN instead of client VLAN
CSCvg44450	2800AP is not able to process the ARP Response
CSCvg83836	Clients cannot pass traffic with 1810W MAB FlexConnect local switching RLAN
CSCvg91770	1810W AP stops to send data frame intermittently
CSCvg98078	AP with FlexConnect AVC visibility Tx frames with sequence jumps causing client to not process packets
CSCvh11212	WLC with Internal DHCP not sending NAK

Caveat ID Number	Description
CSCvh51835	WGB client not getting IP address from the VLAN returned as AAA override
CSCvh54235	Cisco 3800 AP FW stopped working on Radio 0
CSCvh54459	AP console display logs "DTX DUMP"
CSCvh58148	Cisco Wave 2 AP uses invalid CAPWAP data keep-alive source port
CSCvh58467	Kernel Panic with PC at skb_release_data+0xe0/0x230
CSCvh59002	AP702w Continuous Pak ownership errors /w Freeing pak:xx in the radio TX or RX ring, owner:FACD1010
CSCvh62827	aIOS: Wireless client cannot communicate each other with dynamic VLAN
CSCvh63417	d0: *** sensord died (src/dspm_main.c:1662/0) - slot 0 ***
CSCvh72867	Radio reset with transmitter seems to have stopped, FST06
CSCvh77719	External MDNS resolution fails with WLC 'link local bridging' enabled
CSCvh81618	When adding a member to the static RF Group, WLC shows group size has exceeded
CSCvh83207	AP 2800: FIQ stopped working
CSCvh86970	ATF Mesh MIB Memory Leak observed during SNMPWALK from Root
CSCvh87451	1832 Rx not working with AP not responding to probe requests
CSCvh88719	DFS blacklist timer is reset if AP connection to WLC flaps.
CSCvh91290	Wave 2 AP needs to send XID broadcast on client association for FlexConnect local switching
CSCvh94458	Wave 1 APs last reload reason shows "Invalid image opcode"
CSCvh96132	Too many channel changes on XOR 5 GHz
CSCvh96956	AP2800 cannot convert CAPWAP DSCP to 802.11e UP value correctly
CSCvh97636	3800/2800/1832 FlexConnect APs stop redirecting CWA clients after WLAN change
CSCvh97977	WLC Local Policy: Client local profiling assigns incorrect interface to client
CSCvh98496	Fan failure errors seen after upgrade to 8.3.133.10 build
CSCvh99287	OEAP drops wired client traffic after N+1 failover
CSCvi01675	New Mobility with Cisco Catalyst 3650 Switch as MA and Cisco 5520 WLC as Anchor: Guest users cannot reach DG
CSCvi01918	RRM stall; 3702 RF neighbor list empty on both WLC and AP on 5 GHz
CSCvi02150	WLC stopped working at about 80 to 85 % memory utilization

Caveat ID Number	Description
CSCvi03114	1852 series APs stopped working due to Kernel Panic
CSCvi07269	WLC does not respond to TCP SYC message from Linux Server to establish SSH session
CSCvi07565	3800 AP: Client EAP TLS not working with Zebra RF Gun which sends certificate in fragments
CSCvi09095	High QBSS, beacon stop, radio reset seen on 8.5.120.0 after upgrade
CSCvi11609	DNS snooping not working for URL ACL after upgrade to Release 8.5
CSCvi12046	2800 AP: FlexConnect AP WLAN-VLAN mapping on AP does not match with GUI configuration
CSCvi13589	Locally generated webadmin certificate shows as 3rd party after upgrade
CSCvi14638	Rogue BSSID containment count display incomplete
CSCvi17380	TxFSM stuck on Radio 0 with TCQVerify patch
CSCvi23899	WLC clients not getting IPv6 Global addresses under scale scenarios
CSCvi25420	Wave 1 AP always sends RTS at 6 data rate when data rate is supported
CSCvi25532	Standby 8540 WLC reloads unexpectedly with rmgrMain due to IPC timeout
CSCvi25724	Wave 1 APs stopped working due to bad CPQ
CSCvi29775	8510 DP0 CORE 9 DP unresponsive
CSCvi30627	Config missing after WLC failover
CSCvi30899	AP fails to join the WLC when QA country code is used (–E AP)
CSCvi30993	Release 8.5 loses neighbor AP field on WLC GUI; neighbor and rogue APs
CSCvi32951	Cisco Wave 2 APs go offchannel if scan deferral value is greater than 255 milliseconds.
CSCvi33984	HA pair does not sync VLAN support configuration for mesh APs
CSCvi38539	AP stops forwarding IPv6 Router Advertisements to random clients
CSCvi42919	702w AP: Radio resets with ath_ACIF_radio_dead message
CSCvi43963	AP1562D to AP1562D bridge does not transmit fragmented traffic
CSCvi44661	2700 AP runs out of buffers for bpid 2
CSCvi45149	Client Stats and RSSI/SNR reset for clients when Accounting is disabled on WLANs
CSCvi48503	Standby WLC constinuously reboots with "Reason: XMLs were not trasferred from Active to Standby"

Caveat ID Number	Description
CSCvi49059	[FALL WLC BUNDLE] NO CVE Cisco Wireless LAN Controller Privilege Escalation Vulnerability
CSCvi50929	3504 WLC stopped working
CSCvi51372	Client unable to reach RUN state on anchor WLC with 802.1x + ISE NAC
CSCvi51536	AP is not sending TCP fragments over the air
CSCvi51711	WLC processes SNMP requests but does not transmit responses
CSCvi51858	WLC is not sending proper VSA list at acct-stop when client moves to another SSID
CSCvi53601	New Mobility Anchor Controller unexpectedly reboots with Task Name: mcListen
CSCvi56024	WLC stops processing web-auth.
CSCvi56046	1560 RAP after reboot will lose the VLAN support configuration
CSCvi56589	SSO Secondary does not boot after upgrade
CSCvi56738	IW3702 on auto-bridge mode is not preserving channel width that is more than 20 MHz
CSCvi57169	SDA-Wireless AAA Override VNID ID is lost when roaming from one AP Group to another
CSCvi57213	1832 AP stopped working with "PC is at __napi_complete+0x28/0x60"
CSCvi59432	Creation Time of Local Net User set to Jan 1 00:00:00 1970
CSCvi61401	WLC remote access failing after upgrade
CSCvi61741	Cisco 2802 AP stopped working due to an FIQ/NMI reset and no backtraces are generated
CSCvi62746	Client cannot pass IPv6 traffic for 15 seconds after associating
CSCvi63043	Hyperlocation disabled, but WLC overfloods log with hyperlocation messages
CSCvi63785	WLC becomes inaccessible via HTTPS when creating CSR for webauth on Cisco vWLC
CSCvi97023	Cisco Wireless LAN Controller Cross-Site Scripting Vulnerability
CSCvj95336	Cisco Wireless LAN Controller Software Information Disclosure Vulnerability

Resolved Caveats

Table 13: Resolved Caveats

Caveat ID Number	Description
CSCux41096	Need a way to show the client exclusion list on the AP
CSCuy90135	RxSop values configured from CLI, changes back to "AUTO"
CSCvc66046	Selective client packet capture support for 2800 and 3800 series APs
CSCvc66728	WLC: Traceback pattern #2 in apfProcessAssocReq
CSCve14291	AP1830: The **show version** command shows old software version as "AP running image" and longer up-time
CSCve64652	Cisco Access Point 802.11r Fast Transition Denial of Service Vulnerability
CSCvf32557	FlexConnect local switching standalone mode EoGRE client connecting as simple client
CSCvf52731	New Mobility member status shows as unknown when editing mobility member IP address
CSCvf65133	Dynamic interface template fails to apply on Cisco WLC with DHCP Option 82 setting
CSCvf66680	Cisco WLC Control And Provisioning of Wireless Access Points Information Disclosure
CSCvf66696	Cisco WLC Control & Provisioning of Wireless Access Points Protocol Denial of Service Vulnerability
CSCvf66723	Cisco Wireless LAN Controller Directory Traversal Vulnerability
CSCvf68405	Provision 128 characters LMA name in PMIPv6 with IP address, CLI cannot display it
CSCvf72787	SDA: WLC stopped working at emWeb while configuring Fabric
CSCvf74866	Webauth scaling improvements: Fix problem with GUI going unresponsive with HTTPS redirect
CSCvf80409	1815 AP is not sending all traffic after period under load
CSCvf81907	Webauth on MAC authentication failure is not part of the **show tech-support** command.
CSCvf84806	FIQ/NMI Reset AP2800 PC __pci_bus_size_bridges+0x274/0x768 LR warn_slowpath_common+0x58/0x94
CSCvg06111	WLC "in sync" with NTP while authentication is ignored with invalid keys
CSCvg16095	Incorrect values of RSSI, SNR are being reported to WSA
CSCvg18543	3700 AP Tx jammed and radio reloads unexpectedly
CSCvg19242	Cisco 1700, 2700, and 3700 AP log incorrect PHY in sniffer mode for 802.11ac

Caveat ID Number	Description
CSCvg21910	Deleting one SSID will affect another SSID created on the same radio interface
CSCvg23810	PMTU change to 1500 from a lesser value is not reflected in AP
CSCvg26841	SNMP walk on bsnMeshNodeTable returns no data for IW3700 AP in Flex+Bridge Mode
CSCvg27613	DHCP Proxy enabled and removing DHCP Server Info from Dynamic interface disables WLAN
CSCvg34502	1542 AP not joining WLC with Costa Rica (CR) Country
CSCvg35220	3702 AP fails to correctly map data traffic to SGACL
CSCvg40339	2800 AP in sniffer mode is missing huge amount of data packets
CSCvg43654	Cisco Wave 2 APs in FlexConnect mode do not forward DHCP NAK to wireless client
CSCvg48395	TrustSec not working; Environment Data download failing on Cisco 3504 WLC platform
CSCvg53640	1830 AP Triggered FW assert for radio failure (beacons stuck)
CSCvg54772	Buff Leak messages on AP console again when AP changes channel
CSCvg56184	Wave 1 APs in sniffer mode show incorrect TID in captured traffic
CSCvg61878	Wave 1 AP does not send k9w8 in LLDP Packets leading to false classification
CSCvg64750	HA osapi_file.c:1030 Failed to open the file, %OSAPI-3-SOCK_SEND_FAILED: [SA]osapi_support
CSCvg67509	Cisco 1810W AP reloads unexpectedly over a kernel panic
CSCvg70787	3802 AP kernel panic PC is at skb_release_data+0xe0/0x230
CSCvg70903	WLAN session timeout does not default to dot1x reauth timeout when webauth is enabled via the GUI
CSCvg73797	2800/3800 AP: Command timeout at 0x8000 in FW
CSCvg74107	Cisco WLC reloads unexpectedly on Dot1x_NW_MsgTask due to Dynamic VLAN feature handling for 702 AP
CSCvg75189	Cisco 1800 AP: Radio failure and firmware freeze
CSCvg78210	AP syslog config does not change level from AP syslog to informational; it remains in emergencies
CSCvg82156	2802E AP with Radio1 stopped working
CSCvg87401	1542 AP stopped working in Flex + Mesh mode
CSCvg91734	Cisco 1852/1832 AP: AP data traffic stall in HD environment

Caveat ID Number	Description
CSCvg94522	TxFSM stuck on Radio 0 with new signature
CSCvg94718	Standby WLC reloads unexpectedly on spamApTask
CSCvg94720	AP: Sending EAP packets unencrypted at session timeout
CSCvg94780	Cisco WLC stopped working
CSCvg96183	Proxy ARP always enabled in Beacon IE for FlexConnect mode AP irrespective of ARP cache config
CSCvg96852	Cisco 1815W SnifferMode AP beacons allows clients to join and black-hole traffic
CSCvg96857	WLC SSH session exits with **show mesh** commands in Release 8.6 and later releases
CSCvg97013	Cisco 8540 WLC reloads unexpectedly on Task Name: emWeb on 8.5.110.0
CSCvh15852	WLC GUI/SSH not accessible - emweb consuming 100% cpu
CSCvh16413	WLC System Crash with apfRogueTask_0
CSCvh17281	WLC sends 802.11r in beacons for WebAuth SSID (L2 open security) and client 802.11r roaming fails
CSCvh19127	AP1815I: No response from wired side
CSCvh20238	Cisco 2800 and 3800 APs joining the WLC in FlexConnect mode fail to update Flex ACL in group policies
CSCvh21953	Cisco Aironet 1560, 1800, 2800 and 3800 Series Access Point Denial of Service Vulnerability
CSCvh23473	AP1572 shows incorrect regulatory power level for Qatar domain
CSCvh27557	Cisco 1562 AP limited to 54 Mbps in 2.4-GHz backhaul
CSCvh28229	Incorrect count for cLApWlanStatsOnlineUserNum when SSID is changed
CSCvh30447	MAP changes its statically assigned non-backhaul channel after it rejoins RAP
CSCvh30872	Decrypt errors on 1532 AP
CSCvh32590	1852 AP: Observed a radio core on loading the image, 5G @0x0099B20C,
CSCvh32630	FT Auth Response is incorrect when PMF is enabled
CSCvh32971	Management Via Wireless not working
CSCvh33064	Config logging trace information setting not restored correctly
CSCvh49623	XML parse error during booting and WLC stopped working
CSCvh50166	2802E AP without dart connector being considered as RRF candidate and assigned 5-GHz role

Caveat ID Number	Description
CSCvh51873	WLC stopped working with Task Name: emWeb due to DATACORRUPTION-DATAINCONSISTENCY
CSCvh51936	WLC 3504 flooding with emc1403 0-007c: Read failure of Status Register error msg
CSCvh55157	WLC reuses Acct-Session-Id when client changes WLANs
CSCvh58266	WLC stopped working with Task Name: ccxL2RoamTask 0x162ad5d l2roamGetRrmNeighborList+77
CSCvh58486	WLC stopped working with Task Name: emWeb osapiMsgQueueDetailClear+42/usmDbMsgQueueDetailClear+27
CSCvh59834	Cannot change the role of XOR radio from Auto to Manual on 2802E AP without DART
CSCvh60627	3504 WLC stopped working with taskname 'osapiReaper'
CSCvh60970	WLC stopped working with Task Name: emWeb osapiMutexDumpAllLocked+890 after timezone setting of AP
CSCvh61939	1562 MAP is not forwarding BPDUs sent by the RAP when using Ethernet bridging
CSCvh62112	1832 and 1852 APs stopped working due to memory leak in 4k slab with Spectrum Intelligence enabled
CSCvh65876	Cisco Wireless LAN Controller Software GUI Privilege Escalation Vulnerability
CSCvh66793	1815W AP continuously logs; missing case for op class XXX in ieee80211_mbo_operating_class_to_chan
CSCvh66816	WCPD stopped working with 1815w AP in RlanportControl element
CSCvh67549	Cisco 8540 WLC Data Plane reloads unexpectedly on __udp_input
CSCvh67590	WLC delay packets due to high DP packet buffers in use
CSCvh72613	AP stopped working when running the **show controller d1 atf cfs client** command
CSCvh73146	Cisco WLC stopped working due to clientTroubleShootingTask
CSCvh73674	1562 MAP not sending Air Quality reports to WLC
CSCvh73821	Cisco WLC stopped working when the **show run-config** command is run
CSCvh78149	1815 AP: idle clients are not removed after 24 hours
CSCvh79344	Cisco WLC is returning values for 'cLSiIdrDeviceSignature' OID with a length greater than 32 bytes
CSCvh79685	Cisco WLC warning messages DP Packet pool and WQE pool is not normal
CSCvh82671	Webauth redirection not working with guest anchor WLAN

Caveat ID Number	Description
CSCvh83197	1560 AP will create a loop when failing over to wireless and wired connection comes back
CSCvh83328	WLC stops working in loop while trying to download old configuration from TFTP
CSCvh85082	1562-I AP failed to decode discovery response and stopped working
CSCvh85830	Cisco WLC blocks client MAC authentication for incorrect WLAN profile
CSCvh92524	Cisco WLC stopped working with EoGRE rule added in CLI
CSCvh95762	**show traplog** command: Client Enhanced Traps Sent are not included in Number of Traps Since Last Reset
CSCvh98439	WLC stopped working while executing **config client deauthenticate** *mac* command
CSCvi04088	ASCOM and Cisco 8821 phones unable to make calls on 3802 AP
CSCvi06528	VLAN priority tag inside the EoGRE packet set to non-zero when 802.1p set to none
CSCvi07460	Cisco WLC is incorrectly returning '5' for snmpwalk on bsnMobileStationApMode OID
CSCvi07609	Cisco 5520 WLC experiences fatal dataplane issue at broffu_fp_dapi_cmd.c:4588
CSCvi09424	Layer 3 roam fails back to L2 Anchor with MAC Filtering MAB
CSCvi11287	Cisco 2800 AP consistently reboots around 1 second after joining the Cisco WLC
CSCvi14641	Cisco 2802 and 3802 APs cannot connect with 100-Mbps LAN speed
CSCvi17786	EoGRE client does not receive IP and stays in DHCP_REQ
CSCvi29553	Cisco WLC NMSP status unstable when WLC is added to 3 CMX
CSCvi31343	Cisco 5520 WLC HA pair stops working on broffu_SocketReceive
CSCvi34440	Cisco 3504 secondary WLC stops working repeatedly
CSCvi38017	Standby Cisco WLC continuously reboots after upgrade

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