Release Notes for Cisco Wireless Controllers and Lightweight Access Points, Cisco Wireless Release 8.5.110.0

First Published: 2017-12-12

Last Modified: 2021-02-12

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*.

Revision History

Table 1: Revision History

Modification Date	Modification Details
October 30, 2018	Resolved Caveats—Added CSCvf66680, CSCvf66696, CSCvf66723
August 23, 2018	Open Caveat—Added CSCvk44249
March 13, 2018	Supported Cisco Access Point Platforms section—Added information about support for Integrated Access Point on Cisco 1100 Integrated Services Router.
January 29, 2018	Key Features Not Supported in Cisco Virtual WLC section—Modified information about FlexConnect central switching.

Supported Cisco Wireless Controller Platforms

The following Cisco Wireless Controller platforms are supported in this release:

- Cisco 2500 Series Wireless Controllers (Cisco 2504 Wireless Controller)
- Cisco 3500 Series Wireless Controllers (Cisco 3504 Wireless Controller)
- Cisco 5500 Series Wireless Controllers (Cisco 5508 and 5520 Wireless Controllers)
- Cisco Flex 7500 Series Wireless Controllers (Cisco Flex 7510 Wireless Controller)
- Cisco 8500 Series Wireless Controllers (Cisco 8510 and 8540 Wireless Controllers)

- 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

Note Support introduced in Release 8.4.

  - Kernel-based virtual machine (KVM)

Note 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 2504 WLC, Cisco 3504 WLC, Cisco 5508 WLC, Cisco 5520 WLC, Cisco Wireless Services Module 2 (Cisco WiSM2), Cisco Flex 7510 WLC, Cisco 8510 WLC, and Cisco 8540 WLC.

Note AP Stateful Switchover (SSO) is not supported in Cisco 2504 WLCs.

- Cisco WiSM2 for Cisco Catalyst 6500 Series Switches
- Cisco Mobility Express Solution

Supported Cisco Access Point Platforms

The following Cisco AP platforms are supported in this release:

- Cisco Aironet 1600 Series Access Points
- 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 2600 Series Access Points
- Cisco Aironet 2700 Series Access Points
- Cisco Aironet 2800 Series Access Points

- Cisco Aironet 3500 Series Access Points
- Cisco Aironet 3600 Series Access Points
- Cisco Aironet 3700 Series Access Points
- Cisco Aironet 3800 Series Access Points
- Cisco Aironet 700 Series Access Points
- Cisco Aironet 700W Series Access Points
- Cisco AP802 Integrated Access Point
- Cisco AP803 Integrated Access Point
- Integrated Access Point on Cisco 1100 Integrated Services Router
- Cisco ASA 5506W-AP702
- Cisco Aironet 1530 Series Access Points
- Cisco Aironet 1540 Series Access Points
- Cisco Aironet 1550 Series Access Points with 128-MB memory

Note From Release 8.4, Cisco 1550 APs with 64-MB memory are not supported.

- Cisco Aironet 1560 Series Access Points
- Cisco Aironet 1570 Series Access Points
- Cisco Industrial Wireless 3700 Series Access Points

Note

- Cisco AP802 and AP803 are integrated access point modules on the Cisco 800 Series Integrated Services Routers (ISRs). For more information about the stock-keeping units (SKUs) for the AP802s and AP803s Cisco ISRs, see

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

  Before you use a Cisco AP802 series lightweight access point module with Cisco Wireless Release 8.5, you must upgrade the software in the Cisco 800 Series ISRs to Cisco IOS 15.1(4)M or later releases.

- For more information about Integrated Access Point on Cisco 1100 ISR, see the product data sheet at 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 8.5.110.0

Note For complete listing of all the documentation published for Cisco Wireless Release 8.5, see the Documentation Roadmap: https://www.cisco.com/c/en/us/td/docs/wireless/doc-roadmap/doc-roadmap-release-85.html

Encrypted Mobility Tunnel Support on WLC

A secure link called the Encrypted Mobility Tunnel, which is based on mobility tunnel and encrypted using CAPWAP DTLS protocol, can be established between an anchor and a foreign Cisco WLC. Using this feature, you can manage common SSID across common areas as well as encrypted private SSIDs at different locations.

For more information about this feature, see the Encrypted Mobility Tunnel Support on Cisco WLC chapter in the *Cisco Wireless Controller Configuration Guide*.

DHCP Option 82 for EoGRE Tunnel in Cisco Wave 2 APs

In this release, DHCP Option 82 for EoGRE Tunnel is supported in Cisco Wave 2 APs.

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 8.5.110.0

Current Software Release	Upgrade Path to 8.5.110.0 Software
8.3.x.0	You can upgrade directly to Release 8.5.110.0
8.4.100.0	You can upgrade directly to Release 8.5.110.0

Note If you are using Release 8.2.x, we recommend that you upgrade to Release 8.3.x and then upgrade to Release 8.5.x.

Upgrading Cisco WLC Software Release

Guidelines and Limitations

- If you are using Release 8.4 and want to upgrade to a later release, it is necessary that you upgrade to Release 8.5.105.0 and then move to a later release.

  Note This restriction is applicable only to Release 8.4 and not any other release.

- The image format of Cisco Aironet 1700, 2700, 3700, and IW3702 APs has been changed from ap3g2 to c3700. Therefore, if you are upgrading to Release 8.5 or a later release from Release 8.3 or an earlier release, these APs will download the image twice and reboot twice.
- Support for Dynamic WEP is reintroduced in Cisco Wave1 APs in this release.
- The AAA database size is increased from 2048 entries to 12000 entries for these Cisco WLCs: Cisco Flex 7510, 8510, 5520, and 8540. Therefore, if you downgrade from Release 8.5 to an earlier release that does not include this enhancement, you might lose most of the AAA database configuration, including management user information. To retain at least 2048 entries, including management user information, we recommend that you follow these downgrade instructions and back up the configuration file before proceeding with the downgrade:
  1. From Release 8.5, downgrade to one of the following releases, which support 2048 database size and include the enhancement.
     - Release 8.4.100.0 or a later 8.4 release
     - Release 8.3.102.0 or a later 8.3 release
     - Release 8.2.130.0 or a later 8.2 release
     - Release 8.0.140.0 or a later 8.0 release
  2. Downgrade to a release of your choice.
- In Release 8.5, the search functionality in the Cisco WLC Online Help for all WLCs is disabled due to memory issues encountered in these WLCs: Cisco 2504, 5508, and WiSM2.

- Release 8.4 and later releases support 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 8.5 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 8.5 to a 7.x release, the trap configuration is lost and must be reconfigured.
- If you downgrade from Release 8.5 to Release 8.1, the Cisco Aironet 1850 Series AP whose mode was Sensor prior to the downgrade is shown to be in unknown mode after the downgrade. This is because the Sensor mode is not supported in Release 8.1.
- If you have an IPv6-only network and are upgrading to Release 8.4 or a later release, ensure that you perform the following activities:
  - Enable IPv4 and DHCPv4 on the network—Load a new Cisco WLC software image on all the Cisco WLCs along with the supplementary AP bundle images on Cisco 2504 WLC, Cisco 5508 WLC, and Cisco WiSM2, or perform a predownload of AP images on the corresponding Cisco WLCs.
  - Reboot Cisco WLC immediately or at a preset time.
  - Ensure that all Cisco APs are associated with Cisco WLC.
  - Disable IPv4 and DHCPv4 on the network.
- 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 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.

- 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 CSCuy81133 for a possible enhancement to address this restriction.
- We recommend that you install Cisco Wireless Controller Field Upgrade Software (FUS), which is a special AES package that contains several system-related component upgrades. These include the bootloader, field recovery image, and FPGA or MCU firmware. Installing the FUS image requires special attention because it installs some critical firmware. The FUS image is independent of the runtime image. For more information about FUS and the applicable Cisco WLC platforms, see the Field Upgrade Software release notes listing.

Note If you are using Release 8.2.x, we recommend that you upgrade to Release 8.3.x and then upgrade to Release 8.5.x.

- If FIPS is enabled in Cisco Flex 7510 WLC, the reduced boot options are displayed only after a bootloader upgrade.

Note Bootloader upgrade is not required if FIPS is disabled.

- 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.
- It is not possible to directly upgrade to this release from a release that is earlier than Release 7.0.98.0.
- 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 the Cisco WLC is also automatically upgraded. When an AP is loading software, each of its LEDs blinks in succession.
- We recommend that you access the Cisco WLC GUI using Microsoft Internet Explorer 11 or a later version, or Mozilla Firefox 32 or a later version.
- 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.

- When you plug a Cisco WLC into an AC power source, the bootup script and power-on self test is run to initialize the system. During this time, press **Esc** to display the bootloader **Boot Options** menu. The menu options for the Cisco 5508 WLC differ from the menu options for the other Cisco WLC platforms.

  The following is the Bootloader menu for Cisco 5508 WLC:

```
Boot Options
Please choose an option from below:
1. Run primary image
2. Run backup image
3. Change active boot image
4. Clear Configuration
5. Format FLASH Drive
6. Manually update images
Please enter your choice:
```

  The following is the Bootloader menu for other Cisco WLC platforms:

```
Boot Options
Please choose an option from below:
1. Run primary image
2. Run backup image
3. Manually update images
4. Change active boot image
5. Clear Configuration
Please enter your choice:

Enter 1 to run the current software, enter 2 to run the previous software, enter 4 (on
 Cisco 5508 WLC),
or enter 5 (on Cisco WLC platforms other than 5508 WLC) to run the current software and
 set
the Cisco WLC configuration to factory defaults. Do not choose the other options unless
 directed to do so.
```

  Note See the Installation Guide or the Quick Start Guide of the respective Cisco WLC platform for more details on running the bootup script and the power-on self test.

- 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, choose **Option 2: Run Backup Image** from the **Boot Options** menu 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.

Changes in Images and Installation Procedure for Cisco 2504 WLC, Cisco 5508 WLC, and Cisco WiSM2

Due to an increase in the size of the Cisco WLC software image, the Cisco 2504 WLC, Cisco 5508 WLC, and Cisco WiSM2 software images are split into the following two images:

- Base Install image, which includes the Cisco WLC image and a subset of AP images (excluding some mesh AP images and AP80x images) that are packaged in the Supplementary AP Bundle image
- Supplementary AP Bundle image, which includes AP images that are excluded from the Base Install image. The APs that feature in the Supplementary AP Bundle image are:
  - Cisco AP802
  - Cisco AP803
  - Cisco Aironet 1530 Series AP
  - Cisco Aironet 1550 Series AP (with 128-MB memory)
  - Cisco Aironet 1570 Series APs
  - Cisco Aironet 1600 Series APs

Note There is no change with respect to the rest of the Cisco WLC platforms.

Image Details

The following table lists the Cisco WLC images that you have to download to upgrade to this release for the applicable Cisco WLC platforms:

Table 4: Image Details of Cisco 2504 WLC, 5508 WLC, and WiSM2

Cisco WLC	Base Install Image	Supplementary AP Bundle Image [1]
Cisco 2504 WLC	AIR-CT2500-K9-8-5-110-0.aes	AIR-CT2500-AP_BUNDLE-K9-8-5-110-0.aes
Cisco 5508 WLC	AIR-CT5500-K9-8-5-110-0.aes AIR-CT5500-LDPE-K9-8-5-110-0.aes	AIR-CT5500-AP_BUNDLE-K9-8-5-110-0.aes AIR-CT5500-LDPE-AP_BUNDLE-K9-8-5-110-0.aes
Cisco WiSM2	AIR-WISM2-K9-8-5-110-0.aes	AIR-WISM2-AP_BUNDLE-K9-8-5-110-0.aes

[1] AP_BUNDLE or FUS installation files from Release 8.5 for the incumbent platforms should not be renamed because the filenames are used as indicators to not delete the backup image before starting the download.

If renamed and if they do not contain “AP_BUNDLE” or “FUS” strings in their filenames, the backup image will be cleaned up before starting the file download, anticipating a bigger sized regular base image.

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*).

Note For Cisco 2504 WLC, Cisco 5508 WLC, and Cisco WiSM2, the Cisco WLC software image is split into two images, the Base Install image and the Supplementary AP Bundle image. Therefore, in order to upgrade, repeat Step 2 through Step 14 to complete the installation of both the Base Install image and the Supplementary AP Bundle image.

Download the Supplementary AP Bundle image only if you are using any of these APs: AP802, AP803, Cisco Aironet 1530 Series AP, Cisco Aironet 1550 Series AP (with 128-MB memory), Cisco Aironet 1570 Series APs, Cisco Aironet 1600 Series APs, or all of these APs.

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 For Cisco 2504 WLC, Cisco 5508 WLC, and Cisco WiSM2, the Cisco WLC software image is split into two images: the Base Install image and the Supplementary AP Bundle image. Therefore, in order to upgrade, repeat Step 2 through Step 14 to complete the installation of both the Base Install image and the Supplementary AP Bundle image.

Download the Supplementary AP Bundle image only if you are using any of these APs: AP802, AP803, Cisco Aironet 1530 Series AP, Cisco Aironet 1550 Series AP (with 128-MB memory), Cisco Aironet 1570 Series APs, Cisco Aironet 1600 Series APs, or all of these APs.

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 For Cisco WiSM2, check the port channel and re-enable the port channel, if necessary.

Step 18 If you have disabled the 802.11 networks, re-enable them.

Step 19 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**.

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 5: Test Bed Configuration for Interoperability

Hardware/Software Parameter	Hardware/Software Configuration Type
Release	8.5.110.0
Cisco WLC	Cisco 5508 and 5520 Wireless Controllers
Access Points	AIR-CAP3802E-B-K9, AIR-AP1852E-B-K9,AIR-CAP3602E-A-K9
Radio	802.11ac, 802.11a, 802.11g, 802.11n (2.4 GHz / 5.0 GHz)
Security	Open, PSK (WPA-TKIP-WPA2-AES), 802.1X (WPA-TKIP-WPA2-AES) (EAP-FAST, EAP-TLS)
RADIUS	ACS 5.3, ISE 2.2, 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 6: 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

Client Type and Name	Version
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 old	OSX 10.11.5
MacBook Air new	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	
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

Client Type and Name	Version
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
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 Pixcel	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 the different 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 2504 WLC

- Domain-based ACLs
- Autoinstall
- Controller integration with Lync SDN API
- Application Visibility and Control (AVC) for FlexConnect locally switched APs
- Application Visibility and Control (AVC) for FlexConnect centrally switched APs

Note AVC for local mode APs is supported.

- URL ACL
- Bandwidth Contract
- Service Port
- AppleTalk Bridging
- Right-to-Use Licensing
- PMIPv6
- EoGRE
- AP Stateful Switchover (SSO) and client SSO
- Multicast-to-Unicast
- Cisco Smart Software Licensing

Note

- The features that are not supported on Cisco WiSM2 and Cisco 5508 WLC are not supported on Cisco 2504 WLCs too.
- Directly connected APs are supported only in local mode.

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 WiSM2 and Cisco 5508 WLC

- Domain-based ACLs
- VPN Termination (such as IPSec and L2TP) —IPSec for RADIUS/SNMP is supported; general termination is not supported.
- Fragmented pings on any interface
- Right-to-Use Licensing
- Cisco 5508 WLC and Cisco WiSM2 cannot function as mobility controller (MC). However, it can function as guest anchor in a New Mobility environment.
- Cisco Smart Software Licensing

Key Features Not Supported on Cisco Flex 7510 WLC

- Domain-based ACL
- Cisco Umbrella—Not supported in FlexConnect locally switched WLANs; however, it is supported in centrally switched WLANs.
- Static AP-manager interface

Note For Cisco Flex 7510 WLCs, it is not necessary to configure an AP-manager interface. The management interface acts as an AP-manager interface by default, and the APs can associate with the controller on this interface.

- IPv6 and dual-stack client visibility

Note IPv6 client bridging and Router Advertisement Guard are supported.

- Internal DHCP server
- APs in local mode

Note A Cisco AP associated with a controller in local mode should be converted to FlexConnect mode or monitor mode, either manually or by enabling the autoconvert feature. From the Cisco Flex 7510 WLC CLI, enable the autoconvert feature by entering the **config ap autoconvert enable** command.

- Mesh (Use Flex + Bridge mode for mesh-enabled FlexConnect deployments)
- Cisco Flex 7510 WLC cannot be configured as a guest anchor controller. However, it can be configured as a foreign controller to tunnel the guest traffic to a guest anchor controller in a DMZ.
- 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 Internet Group Management Protocol (IGMP) or MLD snooping.

- PMIPv6
- Cisco Smart Software Licensing

Key Features Not Supported in Cisco 5520, 8510, 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

Note Cisco Smart Software Licensing is not supported on Cisco 8510 WLC.

Key Features Not Supported in Cisco Virtual WLC

- Cisco Umbrella
- Domain-based ACLs
- Internal DHCP server
- Cisco TrustSec
- Access points in local mode
- Mobility/Guest Anchor
- 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 in only 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

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

Table 7: 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 • 802.1x supplicant for AP authentication on the wired port • 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)
Location Services	Data RSSI (Fast Locate)

FlexConnect Features	• Bidirectional rate-limiting
	• 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 8: Key Features Not Supported in Cisco Aironet 1800i, 1810 OEAP and 1810W Series APs

Operational Modes	Mobility Express
FlexConnect Features	Local AP authentication

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

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 10: Open Caveats

Caveat ID Number	Description
CSCvd38006	Cisco 1600 AP Ping Loss on Ethernet interface
CSCvd91152	Cisco 3700 APs in FlexConnect reloads unexpectedly on 8.3.111.0 release
CSCve18359	Observed traceback on Cisco 1570 AP when changing AP mode to FlexConnect from Flex+Bridge
CSCve53395	WGB certificate installation for EAP-TLS requires CSR
CSCve72696	Sanity :SNMP walk for AP MIB Lwapp_ap_mib_2 failed
CSCve79470	Cisco Wave 2 APs sends RADIUS message directly even if Local Authentication is disabled
CSCvf08272	Blocked list timer is showing as "blacklist due to be cleared" but still blocked list timer remaining
CSCvf11072	ME: SUBNET_MISMATCH_IP_ADD_ON_MSCB mismatches while registering IP address x.x.x.x
CSCvf51131	DHCPv6 stateless not working

Caveat ID Number	Description
CSCvf65133	Dynamic interface template fails to apply on Cisco WLC with DHCP Option 82 setting
CSCvf66801	WLC setting the df bit to on on SNMP get response
CSCvf83391	Cisco 8.3 Release: AP reloads unexpectedly at TAMD ap-tam process
CSCvf96532	WLC anchor commands are missing from the backup
CSCvg00507	Cisco 3700 AP reloads unexpectedly- PID 104: Process "LWAPP Rogue Monitoring process"
CSCvg07617	AP1810W:Kernel Panic reloads unexpectedly PC is at _ZN17ContentHashFilter11clear_staleEv+0x1ac/0x1d0
CSCvg27599	Cisco WLC reloads unexpectedly sometime when client switches between FT enabled SSID and CCKM SSIDs
CSCvg44078	WLC unable to timeout clients; stale client entries
CSCvg74107	WiSM2 reloads unexpectedly on Dot1x_NW_MsgTask due to Dynamic VLAN feature handling for CAP 702
CSCvg96329	AP: system reboot invoked due to radio command timeout - no radio crash files generated
CSCvh04759	Cisco 3800,2800 APs: Beacon is stuck but AP did not detect any beacons stuck
CSCvk44249	WLC 5508 - foreign mapping is missing on a WLAN when restoring a backup

Resolved Caveats

Table 11: Resolved Caveats

Caveat ID Number	Description
CSCuw48090	Cisco 1602 AP 5-GHz radio stop transmitting / receiving frames
CSCux97132	AP starts the Channel Availability Check (CAC) timer after rolling back to a lower bandwidth
CSCuy61155	802.11b inconsistent probe response - band select enabled - 2.4GHz
CSCuz59858	Cisco 3500AP (SC1), client association failure - R2H Buffer full
CSCuz72195	AP bridge does not forward BPDUs or VTP frames
CSCva18887	ME : IOS AP flash corruption issue
CSCvb57793	AP does not fragment EAP cert correctly
CSCvc50775	Webauth redirection stop working when AP manager is configured on a dynamic interface

Caveat ID Number	Description
CSCvc71012	Error in retrieving number of mDNS policies when given command "show mdns policy service-group"
CSCvd09394	AP3700: Tx util values are not changed
CSCvd15449	FRA Probe suppression does not work for pre-association client
CSCvd21375	8.5.1.71 - Cisco 1560 AP RAP does not show (DFS scan in process) like CAP1815 does
CSCvd42321	Cisco 1832 AP drops the CAC SIP 486 packet
CSCvd64928	System stopped working on PMIPV6_Thread_0 during creation of LMA entry
CSCvd80240	FlexConnect AP sends associate response with wrong HT capabilities
CSCvd83486	Cisco IW3702UX AP will not join Cisco vWLC after 3+days
CSCvd90160	AP2800 sending announce as 0 in Reassociation response in FlexConnect Mode in FT and adaptive FT
CSCvd91770	Trust-DSCP-Upstream broken on Cisco 8.2.151.0 release
CSCvd95557	For Non-DPAA AP Model, client stuck in Authentication Mode while associating
CSCve13779	AP2802 Rogue Detection config changed back to "Enabled" after AP reboot
CSCve13886	WPS signature is getting disabled upon upload or download
CSCve18213	Foreign WLC leaks IPv6 and IPv4 multicast client traffic out of EoIP tunnel
CSCve28491	APs in Flex mode with interface configured to be trunk with multiple VLANs missing links to switch
CSCve31474	WGB HSR 802.11v neighbor report error message when Infrastructure MFP is enabled
CSCve33506	Client EAP-TLS handshake does not succeed with Low MTU
CSCve39780	ME controller is dropping some static IP client associations due to DHCP Policy timeout
CSCve44977	WLC 8.5.1.138 Dual Band radios showing incorrect suggested mode
CSCve47928	Cisco 8.5 release: AP is not joining the Cisco WLC after image upgrade
CSCve51301	Cisco 1850, 1830 AP: Stops beaconing
CSCve56210	Cisco 8.5.x Release: Observed command-timeout while XOR radio was in Sensor mode
CSCve56341	Msglog flooding with MUTEX_UNLOCK_FAILED: trace backs
CSCve56404	Cisco 8.5 release: Cisco XOR radio configured to Sensor mode using GUI has operational state down

Caveat ID Number	Description
CSCve57121	Cisco 3800 AP is not passing traffic
CSCve57918	WLC IGMP queries not sent consistently
CSCve59671	Cisco WLC and ME: RADIUS fail-over does not work when retransmit timeout is not set to default value
CSCve63755	Cisco WLC running 8.4.100.0: Cisco APs fail to join the WLC if it has LSC enabled on it
CSCve65242	Cisco 702w AP radio resets with reason code 71
CSCve68039	Some APs cannot join the WLC because the WLC misrecognizes the number of APs
CSCve68787	Cisco AP is not transmitting out the de-auth frame over the air that was received from the WLC
CSCve69973	Cisco 2800, 3800 - Throttle Assoc requests to WLC
CSCve72187	Micro-Macro transition configuration should be limited to within the defined range
CSCve75022	Cisco WLC does not apply QoS tag upstream from foreign to anchor
CSCve75339	Macro to micro transition threshold is not configurable on Mobility Express
CSCve75515	Configuration backup shows the time instead of the NAT IP
CSCve78449	Cisco 3700 AP: radio d1 reset: Tx jammed
CSCve81183	Cisco 2800, 3800 - Rx hang in 8.2.154.17 release
CSCve81269	Clients failed to get connected to the Cisco AP in Flex mode with message as AID already in use
CSCve81314	Clients fails to connect to AID with message as All AID are in use when the AP is in Local mode
CSCve83024	WLC power supply issues not showing up on 360 page
CSCve83915	"32 chars" match role string is not accepting in CLI unlike in GUI
CSCve84906	Traceback observed in Cisco WLC while something is fetched for Flex ACL with AVC
CSCve85321	WGB traffic disruption on missed beacons and no scan or roam
CSCve86627	Bridging interface mode get reset to 'access' when configure MeshAP from GUI
CSCve88087	Cisco Wave 2 AP: WMM parameters not pushed to radio FW
CSCve89376	Cisco Wave1 APs sends RA periodically when EoGRE tunnel profile is added to the AP
CSCve90032	WLC FEW: flooding logs with "Updating MS IPv6[1] Addr" logs

Caveat ID Number	Description
CSCve92127	WLC Data plane reloads unexpectedly on DP core 0 due to WDT
CSCve93715	Cisco 3802 AP reloads unexpectedly on -CAPWAPd
CSCve95309	'WL_IOCTL_SET_MGMT_SEND failed for apr1v0 error Bad address' messages on AP followed by Radio reset
CSCve96310	Cisco WLC installs certificate without a password. However, WebAuthentication fails.
CSCve96480	IOS AP stopped working when it is changed from sensor mode.
CSCve96870	WCPD out of memory; AP-COS reloads, or fails to send auth or DHCP response to client
CSCve98689	Repeated CDP-4-DUPLEX_MISMATCH is observed when 1852 and 3802 APs are connected to 3850 switch.
CSCve98892	DNS lookup for RADIUS/TACACS+ fails because it is queried before the physical port is up
CSCve99696	CPU ACLs are missing after the WLC reload.
CSCve99763	8.5.1.176 - Cisco 1815 APs MAP2s experience roaming issues ...
CSCvf00877	8.5: cmdtimeout when xor in sensor mode, band mismatch errors
CSCvf01433	Cisco 1852 AP fails to send multicast packets to wireless
CSCvf01576	Cisco 3504 WLC is not generating a crash file.
CSCvf02705	The IP-SGT binding is removed from SXP peer after a WLC redundancy switchover
CSCvf03024	The power constraint value is advertised as 3, though it is configured as 0
CSCvf04412	Cisco 2800/3800 AP acting as ME stopped working due to watchdog reset (OOM) after 23 days of up time
CSCvf05046	Cisco 1800,2800,3800 APs: correction in unit of antenna gain in show controller output
CSCvf05427	Cisco 2800/3800 AP cannot use the RX-SOP
CSCvf05776	Target assert XXXXXXXX WAITING FOR STOP EVENT on Cisco 1810 AP
CSCvf07062	Channel assignment leader shows junk value on standby WLC
CSCvf07189	8.5 Incorrect prompt after executing any CLI with (y/n) option
CSCvf07640	[5520] Setting an IPv6 address for primary-base on an AP from WLC cuts off last characters after ::
CSCvf07775	Cisco 2800,3800 AP - Kernel panic FIQ or NMI - Panic in click
CSCvf07776	Cisco 2800, 3800 AP - FIQ stopped working due to firmware core dump loop

Caveat ID Number	Description
CSCvf09441	PMIPv6 MAG is not initialized in the backend
CSCvf10157	Cisco WiSM2 stopped working with emWeb in 8.5.1.183 build
CSCvf10810	Partial collection failure for Mobility express
CSCvf12011	Webauth logout fails after standalone - connected
CSCvf12571	Cisco 2800,3800- CAPWAP tunnel does not restart automatically after configuring primary-base WLCName
CSCvf12728	Cisco 7510 WLC stopped working in SNMP task with no traceback
CSCvf15991	Client data traffic drops when AAA override and link-local-bridging are enabled due to timing issue
CSCvf16302	Flash on Lightweight IOS APs gets corrupted
CSCvf16340	After WLC upgraded to 8.3.133.0, CAP1810 shows "host/RAM_fw Build Ver Mismatch: H:0x47, F:0x5 !"
CSCvf16629	The OUI string updates properly in Cisco 5508 WLC but disappears after a reboot
CSCvf16842	Tunnel Gateway (TGW) in Cisco 3802 AP comes up only after the Heartbeat interval expires
CSCvf17085	The radio of Cisco 3800 series AP stopped working after an image reload
CSCvf17133	8.3.133.0:"config dhcp address-pool test 178.1.0.1 178.1.0.100" hits "Invalid scope specified."
CSCvf17294	Cisco 2800, 3800 APs running 8.2.154.61 release: wifi0 resets multiple times
CSCvf17488	Cisco WLC reloads unexpectedly with task name: mmMaListen on 8.4.100.0
CSCvf18505	When WLC adaptive/fastlane is disabled, the CCX IE is missing in probe response Wave 2 APs
CSCvf19717	Modification of Single host-multihost-mab enable/disable results in rlan removal
CSCvf19891	Cisco 3800 and 2800 series APs stopped working when an SKB from Linux host was freed twice.
CSCvf19926	8.3MR3:OSAPI-3-MSGQ_RUNNING_HIGH: [PA]osapi_msgq.c:926 Message queue BCAST-DATA-Q is nearing full.
CSCvf20997	Hotspot getting enabled with open security in WLC
CSCvf22342	Cisco 3800, 2800 AP running 8.2.154.64 release: TxFSM Stuck
CSCvf22697	Flooding "Invalid checkpoint client ID (0)" message on Standby WLC
CSCvf22977	Not able to delete RADIUS Auth server with RFC3576 enabled from CLI

Caveat ID Number	Description
CSCvf23182	Radio parameters become blank after setting channel width to 40-above
CSCvf23432	AP freeze: DOT11-3-OFF_CHN_QUEUE_STUCK: Flushing off channel queue requests Queue recovery acted
CSCvf25015	AP reloads unexpectedly with ENTROPY-0-ENTROPY_ERROR:unable to collect sufficient entropy
CSCvf25062	Cisco 3802AP on 8.3.124.17 release [cmd mismatch] wifi0: Host Cmd:0x9201 F/W Cmd:0x8001 Last:0x801d
CSCvf26207	Cisco 7510 WLC running 8.0.120.36 reloads unexpectedly while running airewave director debug
CSCvf27533	Cisco 3800 AP in a constant reboot loop
CSCvf28800	Cisco 2800 AP running 8.2.154.67 release: FIQ reloads unexpectedly due to aptrace
CSCvf28913	WLC FRA configuration menu very confusing
CSCvf29208	Cisco 1560-Mesh: Fixed backhaul rate issues.
CSCvf30035	Cisco WLC reloads unexpectedly due to SXP CORE not releasing lock
CSCvf30881	After changing the AP CAPWAP v4 to v6, AP name is changing to default MAC name
CSCvf31054	Continuous FIQ/NMI reloads unexpectedly for 3802 AP when XOR is in sensor mode
CSCvf31767	AP group entry duplicated, cannot delete AP group, access existing AP groups
CSCvf32021	WLC not marking TID in CAPWAP for TSPEC/TCLASS client after roam it is marked
CSCvf32864	Wired client behind MAP(iw3700) is not able to send traffic to destination
CSCvf33081	WLC running 8.3.121.0 is not accepting IPs for NetFlow exporter when ending between .224 - .255
CSCvf33168	FEW: all access-tunnels taken down when fabric interface deleted
CSCvf33937	System reloads unexpectedly due do_pingInet task
CSCvf34480	Cisco Wave 2 APs: losing flex-avc-profile config if one out of 2 WLAN disabled
CSCvf34744	Correct fix for CSCvc78546 (Zero 801.11e QoS for downstream voice when CAC disabled)
CSCvf37785	On an 1810W AP, multicast fails to pass on the LAN port when switchport configured for 1000M speed
CSCvf38154	Cisco 2800, 3800 APs- Dual DFS Fix that avoids False DFS triggers in HD environment
CSCvf38379	Cisco 8540, 5520 WLCs does not boot - "System could not find 68xx Nic Card"
CSCvf38544	WLC: Jamaica Country does not add -E Regulatory Domain support for Outdoor APs

Caveat ID Number	Description
CSCvf39106	WLC IPv4 CPU ACL mapping is removed after redundancy switchover or after WLC restart
CSCvf40071	WIPS engine gets disabled on 2800 after AP reboot
CSCvf41057	Clients QoS level changes automatically to silver from gold during local authentication
CSCvf41342	HA SSO - Apply Config failed on Standby, Reason:5
CSCvf41485	WLC reloads unexpectedly when entering 'show run-config' command
CSCvf41587	3800 AP rebooted after rejoining WLC (upgrade) due to watchdog reset with "wcpd" as reason.
CSCvf41909	XOR radio is not set to lowest Tx power after moving to 5-GHz band by FRA
CSCvf43759	Issue 'no bvi-vlanid' on WGB does not cast IAPP message to refresh BVI VLAN id on AP
CSCvf44061	SNMP get or walk on device for bsnAPBridgingSupport returns ENABLE for Cisco 2800, 3800 APs
CSCvf44285	8.3 does not allow use of spaces in FlexConnect group names, no APs showed on GUI for existing names
CSCvf44497	Cisco 2800, 3800 Flex- If there is no RSN IE, yet the AP is advertising both HT and VHT IEs
CSCvf44583	Cisco 2800, 3800 APs transmitting at MCS/802.11n rates to clients with WMM disabled
CSCvf45017	Remote LAN with 1810w in FlexConnect mode not showing client IP
CSCvf45989	WLC DP core 0 hung due to RML interrupt handler
CSCvf46715	Cisco 3800 AP running 8.3.124.31: Kernel panic observed
CSCvf47017	Cisco 2800, 3800 AP - not able to boot and get stuck "BootROM: Image checksum verification FAILED"
CSCvf47198	1542-Mesh: Fixed backhaul rate configuration does not work
CSCvf47744	Ping fails between routers after route setup with radio link
CSCvf47808	Key Reinstallation attacks against WPA protocol
CSCvf48180	Beacon stuck on 2.4GHz band radio
CSCvf49632	CAPWAPd reloads unexpectedly after enabling CAPWAP payload debug
CSCvf50387	new Cisco 1562 AP reloads unexpectedly due to: FIQ/NMI reset
CSCvf50747	When traffic is not initiated by the WLC, the WLC does not check ARP table

Caveat ID Number	Description
CSCvf51780	Cisco 3504 WLC reloads unexpectedly during external webauth redirection with MAX length URL
CSCvf52008	WLC's GUI hanged and unexpectedly rebooted
CSCvf52723	IOS AP FlexConnect local switching - client cannot pass traffic when using 802.1X + NAC
CSCvf52875	SNMP:Junk characters instead of server IP when image download is initiated from Prime Infrastructure
CSCvf55570	Clients unable to connect when CCKM and FT802.1X are enabled together
CSCvf55741	Cisco 1532 AP cannot use static IP address when configured as mesh AP (MAP)
CSCvf56076	Cal data stored for channels 40, 149 and 153 are incorrect
CSCvf56465	Cisco WLC does reflect 400 error codes
CSCvf56556	Guest User role cannot be called properly on the Cisco 2504 WLC platform
CSCvf57305	Issues with 1562s MAP taking a long time to join RAP
CSCvf57360	Cisco Wave2 AP clients constantly deleted with active voice traffic and optimized roaming enabled
CSCvf57859	Ceiling not working if DSCP sent is higher than metal policy of WLAN
CSCvf58977	RTU license count taking over Smart Account count
CSCvf59621	Cisco 3800, 2800 AP running 8.3.124.40 release: TxFSM Stuck
CSCvf59630	XOR radio does not move to 5GHz/Monitor bands after being marked redundant
CSCvf59685	Cisco 3602i/e AP reloads unexpectedly while failover occurs
CSCvf61646	802.11v BSS Transition Preferred Candidate List Not Included with Radio Policy Set to 802.11a Only
CSCvf61962	Cisco WLC reloads unexpectedly due high CPU usage by SNMP task
CSCvf61975	WLC reaper not creating proper crash file
CSCvf62670	AP1850/1830 : Stop Rx without beacon drop in noisy environment
CSCvf62929	WLC randomly marks wireless management frames with DSCP CS0 instead of CS6
CSCvf63464	AP show CLIs seen having previously joined controller CAPWAP tunneled WLAN entries
CSCvf65587	Cisco 2504 controller not accepting 50 AP evaluation license
CSCvf66680	Cisco WLC Control And Provisioning of Wireless Access Points Information Disclosure

Caveat ID Number	Description
CSCvf66696	Cisco WLC Control & Provisioning of Wireless Access Points Protocol Denial of Service Vulnerability
CSCvf66723	Cisco Wireless LAN Controller Directory Traversal Vulnerability
CSCvf67467	System reloads unexpectedly as Reaper Reset:Task wipsTask taking too much CPU
CSCvf68648	Dataplane reloads unexpectedly when using EoGRE tunnel
CSCvf68674	Node ptr_meshFileCfg.cfg.convMethod value = 3 is out of range for min = 0 and max = 2 upgrade
CSCvf69070	Aironet2802 marking upstream client traffic with incorrect DSCP values when WMM is disabled
CSCvf69071	Cisco 3504 WLC factory default license issue
CSCvf69955	Kernel Panic seen on 1542 Mesh APs
CSCvf71074	AP 1562 Failed to decode discovery response
CSCvf71136	Infra IPv6 AP drops off from the WLC every 4 to 12 hours
CSCvf72352	Rogue APs getting contained or containment pending automatically on the WLC
CSCvf72497	3600 AP dropping over dtls tunnel with 8540 wlc
CSCvf72997	1832 AP kernel panic
CSCvf75869	Cisco 2800, 3800 APs: radio0 reloads unexpectedly in longevity due to 3rd party FW issue(s)
CSCvf76161	ME: Primary AP running with 100% CPU Utilization
CSCvf76245	"debug client" sometimes reports wrong BSSID in (Re)association message
CSCvf76274	Cisco APs can no longer join the WLC; CAPWAP-3-DTLS_DB_ERR
CSCvf76739	Cisco 2800, 3800 AAA override VLAN does not work for native VLAN.
CSCvf77787	AP LAG fails using LACP with non-Cisco switches
CSCvf80317	FEW - map server AP entries dropped when WLC switches over
CSCvf82065	1562 AP unable to pass multicast joins from RAP to MAPs
CSCvf82117	WLC fails to send complete IPv6 client information to Prime Infrastructure
CSCvf82379	Standby 5508 WLC on 8.5.107.23 - reloads unexpectedly on haSSOServiceTask0
CSCvf83404	VLAN override on RLAN with FlexConnect Local Switching does not work
CSCvf83594	Client moving to RUN state from webauth reqd after reassoc request

Caveat ID Number	Description
CSCvf83733	WLC detects IDS Signature attack even if Signature Processing is disabled
CSCvf84211	WLC dataplane reloads unexpectedly due to core 0 hung and RML interrupt handling
CSCvf84540	Cisco 3700 AP: radio d1 reset: Tx jammed, probably beacon was not really sent by Hw
CSCvf84816	Cisco 1810WAP: Kernel Panic- crash files shows PC is at 0x4 LR is at ieee80211_free_node+0x264/0x4b4
CSCvf85758	Data path flaps on HA switchover
CSCvf86035	Cisco 1815w Kernel Panic PC wlan_channel_frequency+0x10/0x18 LR acfg_get_client_info+0x84/0x264
CSCvf86148	Cisco 3800 AP reloads unexpectedly while running 8.3.124.40 code
CSCvf87646	Cisco 2800,3800 APs in Sniffer mode - frequent kernel panics observed
CSCvf87731	Cisco 5508 WLC reloads unexpectedly during AP join failure
CSCvf88091	Clients behind 3rd Party WGB fail DHCP post upgrade to 8.0.150.0
CSCvf89334	OpenDNS information is lost when primary AP fails over to the new one
CSCvf92627	AP3802E- on 8.5.107.34 reloads unexpectedly due to watchdog reset(with reason: out to reboot with r)
CSCvf94574	Not able to create IPsec profile
CSCvf95036	Cisco 1850 radio firmware reloads unexpectedly at 0x009A4859
CSCvf95503	802.11r roam flexconnect local switch OTA FT-8021x fails intermittently on Cisco 1850AP
CSCvf97662	AP801/AP802 not support DTLS data encryption but it's configrable
CSCvg01352	IPv4 traffic drops with "Packet needs to be fragmented but DF bit is set" and MTU mismatch
CSCvg01740	Deauth reason pulled from association response code wrongly
CSCvg01874	Unable to add LSC CA Certificate on Cisco WLC GUI
CSCvg04022	Encrypt mobility enable/disable fails with HA from GUI
CSCvg04081	Rework CSCvd90160 for 8.5.x (Release-AP2800 sending anounce as 0 in Re-assoc response in Flex Mode)
CSCvg04758	Control Path flaps post switchover
CSCvg07438	AP3800: Low throughput due to packet drops in AP in both fragmented and non-fragmented packets

Caveat ID Number	Description
CSCvg08820	Client failed to join CAP1815 AP with A radio alone in local mode
CSCvg08894	Cisco 3802 AP reloads unexpectedly on Watchdog reset reason: capwapd 8.2.161.0 release
CSCvg10680	DTLS handshake takes more time to get established successfully
CSCvg10793	Key Reinstallation attacks against WPA protocol
CSCvg13374	CCO download DNS breaks after poll and and manually configuring to invalid DNS server
CSCvg14346	WLC- is flagging Misc_Reason 0x9 as an Invalid Apple Reason Code but displays proprietary failure
CSCvg18366	hostapd deleting client entry when client goes to FWD state in WCPD
CSCvg20439	1562 AP is dropping downlink unicast messages, making connectivity difficult across mesh link
CSCvg21845	Cisco WLC reloads unexpectedly on task name: SXP SOCK
CSCvg23317	[ECA-SIT]Join Request- PMTU -NOP Payload Parsing issue with Click APs
CSCvg29019	AP18xx : Bypassed scan in returning to DFS channel after a blocked-list timeout
CSCvg29907	AP 3800/2800 8.5.107.61 AP sending wrong BSSID in the Request,Identity packet
CSCvg31499	AP 3800,2800 8.5.107.57 and .61 when AP is in flex mode, AP reloads unexpectedly due hostapd process

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

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.