Release Notes for Cisco Wireless Controllers and Lightweight Access Points, Cisco Wireless Release 8.5.131.0 and 8.5.135.0

First Published: 2018-06-06

Last Modified: 2021-02-12

Release Notes for Cisco Wireless Controllers and Lightweight Access Points, Cisco Wireless Release 8.5.131.0 and 8.5.135.0

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 *Cisco WLCs*, and Cisco lightweight access points are referred to as *access points* or *Cisco APs*.

Revision History

Table 1: Revision History

Modification Date	Modification Details
June 13, 2019	Removed CSCvj73875 from the resolved caveats list.
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	Resolved Caveats added to 8.5.131.0—CSCvh65876, CSCvf66680, CSCvf66696, CSCve64652, CSCvf66723, CSCvi49059, CSCvh21953 Resolved Caveats added to 8.5.135.0—CSCvi97023, CSCvj95336
August 23, 2018	Open Caveat—Added CSCvk44249
August 21, 2018	In the Upgrade Guidelines and Limitations section, added information about change in functionality due to CSCvm01415.
July 24, 2018	Added the CIMC Utility Upgrade for 5520 and 8540 Controllers section.
July 22, 2018	Included Release 8.5.135.0 • Updated Resolved Caveats

Modification Date	Modification Details
June 29, 2018	Open Caveats Section • Removed—CSCvj74716, CSCvj71000 Resolved Caveats section: • Added—CSCvj73875
June 20, 2018	Resolved Caveats section: • Added—CSCvj25842, CSCvj54432
June 15, 2018	Open Caveats section: • Added—CSCvj96316 • Removed—CSCvj72076, CSCvj58436

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.

- 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

  https://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 8.5.135.0

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

Note For complete listing of all the documentation that is 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

What's New in Release 8.5.131.0

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

Note For complete listing of all the documentation that is 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

ETSI New Regulatory Compliance Information

Cisco software is updated to meet the new requirements added to ETSI EN 301 893, the European standard for 5 GHz RLAN which comes in force from June 12, 2018.

For more information, see https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-7/b_upcoming_software_changes_to_meet_the_new_european_requirements_for_5ghz_rlan_equipment.html

Power Update for Cisco 1800 Series APs

Cisco PoE switches supporting 802.3af fails to provide power to Cisco 1800 Series APs. For more information, see CSCvj73077.

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 8.5.131.0

Current Software Release	Upgrade Path to 8.5.131.0 Software
8.2.16x.0 and later	You can upgrade directly to Release 8.5.131.0 **Note** Release 8.2.16x.0 is affected by CSCvf12068.This issue is addressed by upgrading to 8.5.131.0.
8.3.x.0	You can upgrade directly to Release 8.5.131.0

Current Software Release	Upgrade Path to 8.5.131.0 Software
8.4.100.0	You can upgrade directly to Release 8.5.131.0

Note If you are using Release 8.2.15x or earlier, we recommend that you upgrade to Release 8.2.16x or 8.3.x and then upgrade to Release 8.5.131.0.

Upgrading Cisco Wireless Release

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

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

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

Guidelines and Limitations

- In Release 8.5.135.0, the creation of Authorization server is deprecated. To create an Authorization server, you must create an Authentication server and duplicate it as an Authorization server. Due to this change in functionality, an alarm is generated in Cisco Prime Infrastructure 3.2 as follows:

  ```
  1.Successfully created Authentication server. 2.Failed to create
  authorization server:SNMP operation to Device failed: Set Operation
  not allowed for TACACS authorization server.1.Successfully created
  Accounting server.
  ```

  The workaround on Cisco PI is to uncheck the Authorization server on the Prime template.

  For more information about this change in functionality, see CSCvm01415.

- 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 For Cisco 2504 WLC, we recommend that you upgrade to FUS 1.9.0 release or a later release.

- 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

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-K9-8-5-131-0.aes	AIR-CT2500-AP_BUNDLE-K9-8-5-131-0.aes
Cisco 5508 WLC	AIR-CT5500-K9-8-5-131-0.aes AIR-CT5500-LDPE-K9-8-5-131-0.aes	AIR-CT5500-AP_BUNDLE-K9-8-5-131-0.aes AIR-CT5500-LDPE-AP_BUNDLE-K9-8-5-131-0.aes
Cisco WiSM2	AIR-WISM2-K9-8-5-131-0.aes	AIR-WISM2-AP_BUNDLE-K9-8-5-131-0.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**.

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 5: 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 6: 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 7: 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 8: Test Bed Configuration for Interoperability

Hardware or Software Parameter	Hardware or Software Configuration Type
Release	8.5.131.0
Cisco WLC	Cisco 5520 Wireless Controller
Access Points	AIR-AP2802I-B-K9, AIR-AP1852E-B-K9, AIR-AP1810W-B-K9, AIR-AP3802I-B-K9
Radio	802.11ac, 802.11a, 802.11g, 802.11n (2.4 GHz or 5 GHz)
Security	Open, PSK (WPA-TKIP-WPA2-AES), 802.1X (WPA-TKIP-WPA2-AES) (EAP-FAST, EAP-TLS)
RADIUS	Cisco ACS 5.3, Cisco ISE 2.2, Cisco ISE 2.3
Types of tests	Connectivity, traffic (ICMP), and roaming between two APs

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

Table 9: 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 10.12.6
MacBook Air	OSX 10.12.6
Macbook Pro with Retina Display	OSX 10.12.3
Macbook New 2015	OSX 10.12 beta
Tablets	
Amazon Kindle	Android 6.2.2
Apple IPad	iOS 9.3.1
Apple iPad3	iOS 10
Apple iPad mini	iOS 9.3.5
Apple iPad mini 2	iOS 10.3.1
Apple iPad mini 4	iOS 10
Apple iPad Air	iOS 10.1.1
Apple iPad Air 2	iOS 10.2.1
Apple iPad Pro	iOS 11.0.3
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
Zebra ET50PE	Android 5.1.1
Mobile Phones	
Apple iPhone 4S	iOS 10.2.1

Client Type and Name	Version
Apple iPhone 5	iOS 10.3.1
Apple iPhone 5s	iOS 10.2.1
Apple iPhone 5c	iOS 10.3.1
Apple iPhone 6	iOS 11.3
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 5.0.2
Motorola MotoX 2nd Gen	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 925	Windows 8.1 Mobile
Nokia Lumia 1520	Windows 10 Mobile
Google Nexus 5	Android 6.0.1
Google Nexus 6	Android 5.1.1
Google Nexus 7	Android 6.0
Google Nexus 9	Android 6.0.1
Google Pixel	Android 7.1.1
Samsung Galaxy Note3	Android 5.0
Samsung Galaxy Note4 edge	Android 6.0.1
Samsung Galaxy S4	Android 5.0.1
Samsung Galaxy S6	Android 7.0
Samsung Galaxy S7	Android 7.0
Samsung Galaxy S8	Android 7.0
Samsung Galaxy Nexus GTI9200	Android 4.4.2
Samsung SM-P600	Android 4.4.2
LG G4	Android 5.1
LG D855	Android 5.0
Xiaomi Mi 4c	Android 5.1.1

Client Type and Name	Version
Zebra ET1	Android 2.3.4
Zebra TC510K	Android 6.0.1
Zebra TC8000	Android 4.4.3

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 10: 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 11: 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 12: 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 13: 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
CSCve14291	CAP1830: "show version" shows old software version as "AP running image" and longer up time
CSCvf65133	Dynamic interface template fails to apply on Cisco WLC with DHCP Option 82 setting
CSCvg06111	WLC "in sync" with NTP while authentication is ignored with invalid keys
CSCvg27613	DHCP Proxy is enabled and DHCP Server info is removed from the Dynamic Interface, disables the WLAN
CSCvg43654	Cisco Wave 2 APs in FlexConect mode do not forward DHCP NAK to wireless client
CSCvg61933	GUI is not accepting the valid IPv4 netmask (255.255.255.255) while updating SNMP community
CSCvg67509	Cisco 1810W AP reloads unexpectedly over a kernel panic

Caveat ID Number	Description
CSCvg73484	Client fabric stats showing -ve values - Number of Fabric Clients Registered.. -8
CSCvg94718	Standby WLC reloads unexpectedly on spamApTask
CSCvh58148	AP COS uses invalid CAPWAP-Data keep-alive source port
CSCvh58467	Kernel Panic with PC at skb_release_data+0xe0/0x230
CSCvh72867	Radio reset with transmitter seems to have stopped
CSCvh86834	802.11w client association data traffic drops after 802.11r roaming with PMF enabled or optional
CSCvi25724	IOS APs crashing due to bad CPQ on 8.5
CSCvi30993	Lost neighbor AP field on WLC GUI - NEIGHBOR AND ROGUE APS
CSCvi49126	802.11r session timeout after reassociation causing deauth code 17
CSCvi51858	WLC not sending proper VSA list at acct-stop when client moves to another SSID
CSCvi67565	TrustSec: AP picks wrong SXP Node ID
CSCvi73402	Cisco 1810W AP not giving IPs to cell phones using WPA/TKIP protocol
CSCvi74243	Cisco 2800 AP reloads unexpectedly on _ZN6IntArg5parseEPKcS1_biPji+0x0/0x320 for SIP call
CSCvi74683	AIR-CT3504 mGig showing FCS errors incrementing
CSCvi77757	Cisco AP does not copy DSCP to TID marking correctly for Wi-Fi calling packets with AVC profile
CSCvi78819	HA : config service statistics not synced after failover
CSCvi84849	Cisco 1852 series APs unexpectedly reloads due to Kernel Panic
CSCvi90766	CAP with regulatory domain Morocco cannot join the Cisco WLC
CSCvi92170	Cisco 1815w APs falsely shows 100% channel utilization on 5GHz
CSCvi96066	Cisco Wave2 APs on 8.5MR3:2.4GHz backhaul map will not connect to RAP/Wave2 AP client low throughput
CSCvi96718	Cisco ME (Mobility Express) unexpectedly reloads on DHCP spamSendConfigSync
CSCvj01739	Cisco WiSM2 unexpectedly reloads on task name sshpmLscTask after initial config
CSCvj06451	Cisco 8510WLC on 8.5.x unexpectedly reloads at apfProbeThread -pmalloc detected memory corruption
CSCvj07930	CAP 3802, 2802 AP with DART connectors has a Tx power value of 0
CSCvj10154	Target assert after client association with PMF WLAN

Caveat ID Number	Description
CSCvj11397	WLC 3504 - OpenDNS registration failure - Return 77
CSCvj12234	ME-1560 boot up failed after day-0 config, errmsg "failed execution Repeat wlFwGetHwSpecs"
CSCvj13958	2802 AP sending beacon on wrong channels intermittently on 5GHz
CSCvj23814	IPsec tunnels not coming up with GCM ciphers
CSCvj25194	Clean up debug lisp map-server output for AP onboarding
CSCvj32199	SSH/Management Access of Primary WLC not possible when HA failover occurs in 8.5.120.0
CSCvj34879	AP reporting MD5 mismatch on poller script after running all flash bug fixes
CSCvj35883	Allow 2800/3800 to be able to convert to sensor mode.
CSCvj37990	Multiple VLANs not working with broadcast on WGB
CSCvj38456	WLC is losing its EoGRE configuration after reboot
CSCvj57770	CDP-4-DUPLEX_MISMATCH log is seen on the switch port connected to Mobility Express AP2802
CSCvj61084	Cisco WLC Standby unexpectedly reloads due to memory corruption in cpf_handle_rx_msg
CSCvj61140	Having Sensor-Driven tests configured cause 3802I AP to intermittent unexpected reload
CSCvj65449	AIR-AP1562D-E-K9 with regulatory domain Kazakhstan does not join the WLC
CSCvj69298	Cisco WLC Data Plane reloads unexpectedly due to buffers Red/Black Zone crash
CSCvj73077	Cisco 1810, 1815, 1832 APs may have power denied from older POE 802.3af switches
CSCvj73176	Multicast traffic deccrypt mismatch with Draeger device.
CSCvj96316	Cisco 2800, 3800 APs in Local mode leaks some MAC addresses from clients into the Local switch port
CSCvk44249	WLC 5508 - foreign mapping is missing on a WLAN when restoring a backup

Resolved Caveats

Table 14: Resolved Caveats

Caveat ID Number	Description
Resolved Caveats for 8.5.135.0	
CSCvh66937	International Characters conversion issue

Caveat ID Number	Description
CSCvi97023	Cisco Wireless LAN Controller Cross-Site Scripting Vulnerability
CSCvj39970	WSA-8.8 NAC restarted in Cisco 8540 WLC scale setup
CSCvj95336	Cisco Wireless LAN Controller Software Information Disclosure Vulnerability
CSCvk05965	Cisco 8540 WLC in HA SSO: Standby is continuously rebooting
CSCvk20484	IPC timeout and tracebacks reported on Cisco 8540 HA pair running 8.5.131.0 (8.5MR3)
CSCvk25644	WLC HA standby reboots reaching Maintenance mode due to missing NaServCaCert_p12.pem on Active
CSCvk26732	New Flash recovery logic
Resolved Caveats for 8.5.131.0	
CSCva26469	Cisco 2800, 3800 APs - More Packet Loss for Multicast traffic
CSCvb44979	Cisco WLC Local EAP with Cisco Unified Wireless IP Phone 7925 IP Phone Handshake Failure
CSCvc66728	WLC: Traceback pattern #2 on 8.2MR5 in apfProcessAssocReq
CSCvc78347	Cisco 1832 AP expectedly reloads in ZN6IntArg5parseEPKcS1_biPji+0x0/0x320 for SIP call
CSCve64652	Cisco Access Point 802.11r Fast Transition Denial of Service Vulnerability
CSCve79470	Cisco Wave 2 APs sends RADIUS message directly even if Local Authentication is disabled
CSCvf10786	CAP 2800, 3800 sniffer mode logs wrong PHY and data rates for 802.11ac
CSCvf10811	Sniffer mode APs should log more layer 1 information
CSCvf11072	ME: SUBNET_MISMATCH_IP_ADD_ON_MSCB mismatches while registering IP address x.x.x.x
CSCvf17078	Cisco 3702 AP reloads unexpectedly on Dot11_eogre_cfg
CSCvf31881	Cisco 2800 AP detects Intel Dual Band Wireless-AC 8260 as rogue client/AP
CSCvf52731	New Mobility member status shows as Unknown when editing mobility member IP address
CSCvf61977	Cisco AP3802I-B AP reloads unexpectedly on watchdog reset(wcpd)
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

Caveat ID Number	Description
CSCvf66723	Cisco Wireless LAN Controller Directory Traversal Vulnerability
CSCvf74377	AP3800 Sniffer mode: 802.11 acks, RTS, CTS, QoS Null packets do not get captured
CSCvf74406	AP3800 Sniffer mode: AP doesnot fill BAR Request Type, BAR Control, SSC, FCS in BAR and BA packets
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
CSCvg18543	Cisco 3700AP Tx jammed and radio reloads unexpectedly
CSCvg19012	OEAP 1815 performs "Start Network Diagnostics" test could hit different kinds of errors
CSCvg19242	Cisco 1700/2700/3700 log wrong PHY in sniffer mode for 802.11ac
CSCvg21910	Deleting one SSID will affect another SSID created on the same radio interface
CSCvg24833	Cisco 1530 AP in WGB mode reloads unexpectedly on associating with root
CSCvg28378	AP: cmd timeout AP radio reloads unexpectedly in 8.6 due to Rx hang
CSCvg29325	FTP download fails on Cisco WLC when using untagged interfaces on different ports
CSCvg32087	Cisco 5520 WLC reloads unexpectedly on Task Name: nmspTxServerTask
CSCvg34502	Cisco 1542 AP not joining WLC with Costa Rica (CR) Country
CSCvg35115	Cisco 3802 running 8.3.130 shows radio core without the crash file
CSCvg38548	Walk index discrepency between 8.6 and 8.4. Needs to be corrected as per 8.4
CSCvg40339	Cisco 2800 AP in sniffer mode is missing huge amount of data packets
CSCvg40792	Client global IPv6 not correctly mapped to MAC address under certain conditions
CSCvg44078	WLC unable to timeout clients; stale client entries on anchor controller
CSCvg44450	Cisco 2800,3800,1560 AP cannot forward packets downstream; 'Failed to get ARP entry for WLC'
CSCvg45986	WGB forwards downstream Broadcast within un-configured VLAN to native VLAN
CSCvg46125	Cisco WLC reloads unexpectedly multiple times
CSCvg46708	Cisco 5508 WLC reloading due to memory leak in Anon Pages emweb
CSCvg54772	Buff Leak messages on ap console again when ap changes channel

Caveat ID Number	Description
CSCvg56184	IOS APs in sniffer mode shows incorrect TID in captured traffic
CSCvg59338	NMSP drops observed in high density deployments
CSCvg60758	Cisco Wave 2 APs drops TCP retransmit from server
CSCvg61878	COS AP does not send k9w8 in LLDP Packets leading to false classification
CSCvg62359	Cisco 2800, 3800 APs: Click scheduler 0 stuck at Sched/FSys:1/0 Epoch
CSCvg64750	HA osapi_file.c:1030 Failed to open the file, %OSAPI-3-SOCK_SEND_FAILED: [SA]osapi_support
CSCvg64993	WLC mDns secure printer service response missing TXT record with mDNS snooping enabled
CSCvg70420	Cisco 2800, 3800 APs unexpectedly reloads while changing fields on OEAP page
CSCvg73797	Cisco 2800, 3800 AP: Command timeout at 0x8000 in FW
CSCvg74107	WLC reloads unexpectedly in Dot1x_NW_MsgTask - dynamic VLANs from AAA
CSCvg75189	Cisco 1800 AP: Radio failure and firmware freeze
CSCvg76168	5GHz radio interface on 1532 APs remains down due to DFS even when not all channels are in the blocked list.
CSCvg77711	System reloads at random on running mesh commands
CSCvg78101	Local EAP profiles changed not retained after it is applied
CSCvg82066	Cisco 1815I AP Reload due to Kernel Panic
CSCvg82156	Cisco 2802E AP: Radio1 reloads unexpectedly
CSCvg86324	WLC reloads unexpectedly with SNMP operation with Flex ACL
CSCvg87401	Cisco 1542 AP reloads unexpectedly when in Flex + Mesh mode
CSCvg94522	TxFSM stuck on Radio 0 with new signature
CSCvg94780	Cisco WLC reloads unexpectedly on 8.5.105.0 release
CSCvg96160	WLC: Crashed after 1-day on 8.7 Alpha bring-up and ~7-users on tail-end of lunch rush at Cafe-11
CSCvg96183	Proxy ARP always enabled in Beacon IE for Flex mode AP irrespective of ARP cache config
CSCvg96533	Cisco 3800, 2800 APs FIQ/NMI reset see on .98 image and .102
CSCvg96852	Cisco 1815W SnifferMode AP beacons allows clients to join and blackhole traffic
CSCvg96864	8.5MR1 - 8.5.107.110 - AP3702 Radio core with reason "Bad acq dtx"

Caveat ID Number	Description
CSCvg97013	Cisco 8540 WLC reloads unexpectedly on Task Name: emWeb on 8.5.110.0
CSCvg98078	AP with Flex AVC visibility Tx frames with sequence jumps causing client to not process packets
CSCvg98098	AP1852: 5-GHz radio firmware crash @0x00981CED and @0x0099010D
CSCvg98807	8.5MR1: AP702 reloads unexpectedly due to illegal access to a low address
CSCvh01114	Autonomous AP should honor COS value and maps it to UP value accordingly
CSCvh03119	Traceback with SNMPTask %OSAPI-5-MUTEX_UNLOCK_FAILED invalid(NULL) pointer passed. errcode = UNKNOWN
CSCvh07545	AP2800/3800 Kernel Panic due to processing of RX frames before driver is initialized
CSCvh14509	Queue full issue observed with NmspNormalTxQ, breached 1 time. having Capacity 65535
CSCvh14989	Client in RUN state on anchor with 0.0.0.0 IP address
CSCvh15342	Apple client fails to pass traffic when after fast roaming because of sending EAPOL start in 4way HS
CSCvh15852	WLC GUI/SSH not accessible - emweb consuming 100% cpu
CSCvh16413	WLC system reloads unexpectedly with apfRogueTask_0
CSCvh16970	Cisco WLC does not apply ACL Template from PI correctly
CSCvh19127	Cisco 1815I AP no response from wired side
CSCvh20238	Cisco 2800, 3800 APs joining the WLC in flex-mode fail to update FlexACL in group policies
CSCvh21486	WLC reloads unexpectedly due to Task apfMsConnectionTask when MBUF debug is enabled
CSCvh21953	Cisco Aironet 1560, 1800, 2800 and 3800 Series Access Point Denial of Service Vulnerability
CSCvh22023	AP: reloads unexpectedly due to FIQ/NMI in memcpy running 8.7.1.92 release
CSCvh23473	AP1572 shows incorrect regulatory power level for Qatar domain
CSCvh23785	AireOS WLC: Multiple wireless clients failing the broadcast Key refresh (M5).
CSCvh25039	SNMP causes unexpected reloads
CSCvh25368	WLC memory leak on CDP
CSCvh27557	Cisco 1562 AP limited to 54 Mbps in 2.4-GHz backhaul
CSCvh27570	cLSiIdrClusterAffectedChannels OID returning unexpected values

Caveat ID Number	Description
CSCvh28229	Incorrect count for cLApWlanStatsOnlineUserNum when SSID is changed
CSCvh30228	Profile Longevity: Cisco 1832I AP reloads unexpectedly with kernel panic on load 8.5.114.9 (8.5 MR2)
CSCvh30447	MAP changes its statically assigned non-backhaul channel after it rejoins RAP
CSCvh30872	Decrypt errors on Cisco 1532 AP
CSCvh32590	AP:1852 - Observed a radio core on loading the image, 5G @0x0099B20C,
CSCvh32630	FT Auth Response is corrupted when PMF is enabled
CSCvh32971	Management Via Wireless Not Working
CSCvh33064	Config logging traceinfo setting not restored correctly
CSCvh47521	Cisco IOS AP shows Decrypt failed messages on driver debug
CSCvh48916	Cisco 1815I pwr should consume power draw mentioned in the datasheet.
CSCvh49820	WLAN disabled after any change due to PSK lost
CSCvh50166	Cisco 2802e model without dart connector being considered as RRF candidate and assigned 5 GHz role
CSCvh51835	WGB client not getting IP address from the VLAN returned as AAA override
CSCvh51873	WLC reloads unexpectedly on Task Name: emWeb due to DATACORRUPTION-DATAINCONSISTENCY
CSCvh54235	Cisco 3800 AP FW stopped working on Radio 0
CSCvh55157	WLC reuses Acct-Session-Id when Client changes WLANs
CSCvh56064	Profile: 2802I AP reloads unexpectedly due to kernel panic with load 8.5.114.15
CSCvh58266	WLC reloads unexpectedly on Task Name: ccxL2RoamTask 0x162ad5d l2roamGetRrmNeighborList+77
CSCvh58486	WLC reloads unexpectedly on Task Name: emWeb osapiMsgQueueDetailClear+42/usmDbMsgQueueDetailClear+27
CSCvh59834	ME : Cannot change the role of XOR radio from Auto to Manual on AP2802E without DART
CSCvh60627	Cisco 3504 WLC reloads unexpectedly with taskname 'osapiReaper'
CSCvh60970	WLC reloads unexpectedly on Task Name:emWeb osapiMutexDumpAllLocked+890 after timezone setting of AP
CSCvh61355	WLC need remove WGB behind wired client after WGB changes to worst uplink

Caveat ID Number	Description
CSCvh61939	Cisco 1562 MAP is not forwarding BPDUs sent by the RAP when using ethernet bridging
CSCvh63417	d0: *** sensord died (src/dspm_main.c:1662/0) - slot 0 ***
CSCvh65876	Cisco Wireless LAN Controller Software GUI Privilege Escalation Vulnerability
CSCvh66002	AP sniffer doen't capture traffic when enabled for the first time on a channel
CSCvh66793	AP 1815W - continuously logs: missing case for op class XXX in ieee80211_mbo_operating_class_to_chan
CSCvh66816	Cisco 1815w AP: WCPD reloads unexpectedly on RlanportControl element
CSCvh67549	Cisco 8540 Data Plane reloads unexpectedly on __udp_input
CSCvh67590	WLC delay packets due to high DP packet buffers in use
CSCvh72613	AP reloads unexpectedly when running 'show controller d1 atf cfs client'
CSCvh73146	Cisco Controller reloads unexpectedly due to clientTroubleShootingTask 8.3.133.0
CSCvh73674	Cisco 1562 MAP not sending Air Quality reports to WLC
CSCvh73821	Cisco WLC reloads unexpectedly on sh run-config
CSCvh74663	IOS AP unexpectedly reloads during show capwap client config using SSH
CSCvh75618	85MR2 - Starting NA Connector...message flood on WLC console
CSCvh77719	External MDNS resolution fails with WLC 'link local bridging' enabled
CSCvh78149	Cisco 1815 AP idle clients are not removed after 24 hrs
CSCvh78884	Cisco AP reloads unexpectedly on NBAR timer tick task
CSCvh79344	WLC is returning values for 'cLSiIdrDeviceSignature' OID with a length greater than 32 bytes
CSCvh81391	Cisco 2800, 3800 AP add CAPWAP ap-primed-join-timeout logic
CSCvh82606	LSC configurations are not persistent after certificate installation followed by system reboot
CSCvh83197	Cisco 1560 AP will create a loop when faling over to wireless and wired connection comes back
CSCvh83328	WLC reloads unexpectedly in loop while trying to download old config from TFTP
CSCvh85082	Cisco 1562-I AP failed to decode discovery response and crash
CSCvh85830	WLC Blocks Client MAC Authentication for wrong WLAN Profile
CSCvh89438	Cisco 8510 WLC SNMP Traps for duplicate IP reported with IP address inversely

Caveat ID Number	Description
CSCvh91290	AP-COS needs to send XID broadcast on client association for FlexConnect local switching
CSCvh92524	Cisco WLC reloads unexpectedly with EoGRE rule add CLI
CSCvh94458	Cisco Wave 1 APs Last reload reason shows Invalid image opcode
CSCvh96132	8.5.110.0 too many channel changes on XOR 5GHz
CSCvh97636	3800/2800/1832 Flex APs stop redirecting CWA clients after WLAN change
CSCvh98439	WLC stopped working while executing "config client deauthenticate <mac>" command
CSCvh98496	Fan failure errors seen after upgrade to 8.3.133.10
CSCvh99287	OEAP drops wired client traffic after N+1 failover
CSCvi01675	New Mobility with 3650MA and 5520 Achor - Guest users cannot reach DG on 8.3.x
CSCvi01918	Cisco 3702 AP: RRM stall - RF neighbor list empty on both WLC and AP on 5GHz
CSCvi03114	Cisco 1852 Series APs reloads unexpectedly due to Kernel Panic
CSCvi06165	IPsec tunnel is not coming up after disabling or changing the profile using PSK
CSCvi06528	VLAN priority tag inside the EoGRE packet set to non-zero when 802.1p set to none
CSCvi07460	WLC is incorrectly returning '5' for snmpwalk on bsnMobileStationApMode OID
CSCvi07565	Cisco 3800AP: Client EAP auth not working with wireless devices which sends certificate in fragments
CSCvi07609	Cisco 5520 WLC experiences fatal dataplane crash at broffu_fp_dapi_cmd.c:4588
CSCvi09095	Radio Reset Tx Jammed on 8.5.120.0 after upgrade
CSCvi09424	Layer 3 Roam fails back to L2 Anchor with MAC Filtering MAB
CSCvi11287	Cisco 2800 AP consistently reboots around 1 second after joining to the WLC
CSCvi11609	DNS snooping not working for URL ACL after upgrade to 8.5
CSCvi12046	FlexConnect AP WLAN-VLAN Mapped incorrectly on AP2800
CSCvi13706	MAP will map ethernet bridging wired devices to the wrong VLAN
CSCvi17380	TxFSM stuck on Radio 0 with TCQVerify patch.
CSCvi17786	EoGRE client doesn't receive IP and stays in DHCP_REQ
CSCvi19811	NBAR support for WiFi calling in 8.5
CSCvi21680	Change Cisco 1810w max CDP power to old value 24.4w

Caveat ID Number	Description
CSCvi22594	DNAC: Adding new WLC successful or existing devices show that inventory poll fails with SNMP issue
CSCvi25420	COS AP always send RTS at 6 data rate when data rate is supported
CSCvi25532	Standby 8540 WLC-reloads unexpectedly with rmgrMain due to IPC timeout
CSCvi30899	WLC 8.5 - AP fails to join the WLC when QA country code is used (-E AP)
CSCvi31343	WLC HA pair continues to reload unexpectedly due to system crash at on broffu_SocketReceive
CSCvi33984	HA pair does not sync VLAN support configuration for Cisco Mesh APs
CSCvi34440	Secondary Cisco 3504 WLC reloads unexpectedly in a loop
CSCvi38017	Standby WLC goes into a reboot loop after the software upgrade
CSCvi39854	ME - HEAP Memory Leak when internal DHCP scopes are used
CSCvi42526	Mesh 1562AP: AP will not go into bridge mode for I domain
CSCvi42632	AP generating 'hostapd' core files, does not respond to EAPOL
CSCvi42743	ME: Image upgrade got stuck, Slave AP Status showing as "Initiated"
CSCvi43963	AP1562D to AP1562D bridge does not transmit fragmented traffic on 8.5.120.0
CSCvi45088	AP2800/3800: adjust NDP pkt transmission power level
CSCvi49059	[FALL WLC BUNDLE] NO CVE Cisco Wireless LAN Controller Privilege Escalation Vulnerability
CSCvi49114	Cisco 3700 AP: memory allocation issue on IOS AP
CSCvi49590	Bad phase calibration values in Triggerfish EEPROM
CSCvi50929	Cisco 3504 WLC reloads unexpectedly on 8.6.101 release
CSCvi51372	Client unable to reach RUN state on anchor WLC with 802.1x + ISE NAC
CSCvi52529	WLC: OsapiBsnTimer increase memory causing a crash, no crash file generated
CSCvi53601	New Mobility Anchor Controller unexpectedly reboots with Task Name: mcListen
CSCvi54067	COS AP won't clear client statistics after device removed from client's database
CSCvi56046	Cisco 1560 RAP after reboot will lose the VLAN support configuration.
CSCvi56738	IW3702 on auto-bridge mode not preserving channel width more than 20MHz
CSCvi57043	WLC: WLC hang suddenly without crash file, osapiReaper accessing file that does not exist

Caveat ID Number	Description
CSCvi57169	SDA-Wireless AAA Override VNID ID is lost when roaming from one AP Group to another
CSCvi57232	CAP1815w -specific VLAN override RLAN fails, SSID FlexConnect VLAN takes precedence after AP reboot
CSCvi59432	Creation Time of Local Net User set to Jan 1 00:00:00 1970
CSCvi61401	WLC remote access failing after upgrade
CSCvi63043	Hyperlocation disabled, but WLC overfloods log with hyperlocation messages
CSCvi70783	Wireless Service Assurance WSA DNA Assurance certficate is not upated on WLC
CSCvi81204	Cisco 2800, 3800 APs MTU issue with Fabric enable network
CSCvi90205	Cisco WiSM2 upgrade issues with 8.5.124.34 - EXT2-fs: Magic mismatch
CSCvi96690	Cisco 2800 AP detects Intel Dual Band Wireless-AC 8260 as rogue client/AP
CSCvi98154	ME: SSH stopped working for WLC.
CSCvi98357	Cisco AP1815I : reloads unexpectedly due to 'watchdog reset(sync_log)'
CSCvi98514	MAP ethernet port comes up as TRUNK and Allowed VLAN 4095
CSCvj01120	Cisco OEAP have DHCP server feature enabled by default even after disabling
CSCvj03021	After upgrade the AP VLAN Trunking config changed to Disabled state
CSCvj04401	Client remain stuck in DHCP-REQD state on Anchor side unless ISE NAC is disabled on the anchor side
CSCvj07190	Cisco 2800 AP not joining WLC if 'Enable NAT Address' feature is enabled
CSCvj18004	8.5MR3 Interim AP cannot join with NAT address on management interface of controller
CSCvj25842	Cisco 1815I AP: Kernel panic: PC is at vfs_read+0x14/0x134
CSCvj29270	Flex AP's WLAN-VLAN mapping mismatch in multiple WLC scenarios
CSCvj30550	Cisco WLC reloads unexpectedly when configuring PSK Provisioning key
CSCvj36633	AP 3700: AP fail to boot after upgrade from 8.5 to 8.8
CSCvj36853	AP name corruption after upgrade
CSCvj39005	[SDA] Wireless Clients losing L2VNID override when performing Switchover on Cisco 5520 WLC
CSCvj41853	Incorrect Tx power on AP3802P-Q
CSCvj54432	Cisco WLC unexpectedly reloads on task Dot1x_NW_MsgTask_2

Caveat ID Number	Description
CSCvj70569	Incorrect Tx power on AP2800/3800/4800 on power on till we configure Tx power using Cisco WLC

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.