Release Notes for Cisco Wireless Controllers and Lightweight Access Points, Cisco Wireless Release 8.5.140.0

First Published: 2018-11-29

Last Modified: 2021-02-12

Release Notes for Cisco Wireless Controllers and Lightweight Access Points, Cisco Wireless Release 8.5.140.0

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*.

Revison History

Table 1: Revision History

Modification Date	Modification Details
February 01, 2019	Added: **Guidelines and Limitations** section—Included a procedure to continue using Cisco Smart Licence after the boot image upgrade.
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.

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 8.5.140.0

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 Changed in Release 8.5.140.0

This section provides information about the changes and enhancements that are introduced in this release.

–E Domain Support for Kingdom of Morocco

The –E domain access points are supported when the controller country is set to Morocco (MA).

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 8.5.140.0

Current Software Release	Upgrade Path to 8.5.140.0 Software
8.0.x.x	You can upgrade directly to Release 8.5.140.0 **Note** This is applicable only to Cisco 5508 Wireless Controller and Cisco WiSM2.
8.2.16x.0 and later	You can upgrade directly to Release 8.5.140.0 **Note** Release 8.2.16x.0 is affected by CSCvf12068. This issue is addressed by upgrading to 8.5.140.0.
8.3.x.0	You can upgrade directly to Release 8.5.140.0
8.4.100.0	You can upgrade directly to Release 8.5.140.0

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 8.5.140.0.

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

- We recommend you to perform the following procedure if you have the Cisco Smart License enabled and the Controller is registered on Cisco Smart Account.

  Perform this procedure before upgrading the Cisco Controller's boot image.

  1. Deregister the Cisco Controller running the old build from the Cisco Smart Software Manager (CSSM).
  2. Upgrade the Cisco Controller with new boot image.
  3. Reregister the upgraded Cisco Controller with new build on CiscoSmartSoftware Manager (CSSM).

- When the Cisco controller is downgraded from 8.5.140.0 to 8.3.x release, it is possible that the OSU SSID profile name information may be lost and only the OSU SSID name is retained. Reconfigure the controller with the desired profile name to have the HotSpot 2.0 in action after downgrading the controller to 8.3.x release is complete.
- 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 have 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 before 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. 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 differs 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 many 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-K9-8-5-140-0.aes	AIR-CT2500-AP_BUNDLE-K9-8-5-140-0.aes
Cisco 5508 WLC	AIR-CT5500-K9-8-5-140-0.aes AIR-CT5500-LDPE-K9-8-5-140-0.aes	AIR-CT5500-AP_BUNDLE-K9-8-5-140-0.aes AIR-CT5500-LDPE-AP_BUNDLE-K9-8-5-140-0.aes
Cisco WiSM2	AIR-WISM2-K9-8-5-140-0.aes	AIR-WISM2-AP_BUNDLE-K9-8-5-140-0.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.x.x
Cisco WLC	Cisco 5520 Wireless Controller
Access Points	AIR-AP2802I-B-K9, AIR-AP1852E-B-K9, AIR-AP1810W-B-K9, AIR-AP3802I-B-K9

Hardware or Software Parameter	Hardware or Software Configuration Type
Radio	802.11ac, 802.11a, 802.11g, 802.11n (2.4 GHz or 5 GHz)
Security	Open, PSK (WPA-TKIP-WPA2-AES), 802.1X (WPA-TKIP-WPA2-AES) (EAP-FAST, EAP-TLS)
RADIUS	Cisco ACS 5.3, Cisco ISE 2.2, Cisco ISE 2.3
Types of tests	Connectivity, traffic (ICMP), and roaming between two APs

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

Table 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
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

Client Type and Name	Version
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
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

Client Type and Name	Version
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
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
CSCut85555	APF_HA-3-SYNC_RETRANSMIT_FAIL Messages in show msglog

Caveat ID Number	Description
CSCvb26809	WLC should use port MAC for non LAG and box MAC for LAG
CSCve82488	Cisco Wave 2 APs in FlexConnect mode stop redirecting CWA clients after WLAN change
CSCvf57867	Only single IMM / CIMC IP addr configured for both controller active and standby
CSCvf65133	Dynamic interface template fails to apply on Cisco WLC with DHCP Option 82 setting
CSCvg10746	Cisco 1815i and 1542 APs: Per-user BW contract not working for upstream
CSCvg61933	GUI is not accepting the valid IPv4 netmask (255.255.255.255) while updating SNMP community
CSCvg83836	Clients cannot pass traffic with Cisco 1810w MAB FlexConnect local switching RLAN
CSCvh24354	ME: 1800 AP disconnects the client during EAP negotiation by reason: MN_REASSOC_TIMEOUT
CSCvh58148	Cisco Wave 2 APs uses invalid CAPWAP-Data keep-alive source port
CSCvh72867	Radio reset with transmitter seems to have stopped
CSCvi77141	HA_send_usmDbSpamSetRadSlotBand, ErrType:Apply Config failed on Standby
CSCvi82746	WLC reloads unexpectedly with Task Name SISF BT Process
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
CSCvj69298	Cisco 7510, 8500 WLCs: Data Plane reloads unexpectedly due to RPE/Double bit errors
CSCvj72076	Cisco 1800 AP drops a lot of packets
CSCvj79841	Cisco 3802 AP unexpected reboot on 8.2.167.1
CSCvj83372	Cisco 1852 AP showing irregular data usage
CSCvk42225	Max client reached on AP. Sending association response failure with reason code 17
CSCvm33978	Apple iPad devices are getting profiled as Apple device
CSCvm92486	Cisco controller unable to clear stale client entries on anchor controller 8.5.135
CSCvn07126	Cisco FlexConnect - Cisco 2802 APs lowers the priority UP on QoS on the downlink transmit

Resolved Caveats

Table 14: Resolved Caveats

Caveat ID Number	Description
CSCuq00445	Add CLI/GUI option to disable Weak SSL cipher suites for NMSP
CSCur14475	Request syslog, SNMP to show users making config changes
CSCuw22659	Memory leak with QoS/AVC - PPM_FILTER_API, PPCP_PPM
CSCvc62540	Smart Licensing next communication attempt pre-dates the controller time after reboot
CSCvc80047	Unexpected AP reloads - dpaa_get_pool_id_from_ios_pool_ptr
CSCvd67485	Cisco 3700 AP Tx stop Radio reset due to false radio Tx inprog count
CSCve14291	CAP1830: 'show version' shows old software version as 'AP running image' and longer up time
CSCve31869	Enable dual DFS filtering for 1560
CSCve84257	[8.5] show inventory displaying incorrect output for Cisco 802 AP
CSCvf05741	Reason for channel change is shown as none and noise/energy/interfere as 0 for the dual band radio
CSCvf19400	Mobility statistics is getting updated wrongly for L3 roam
CSCvf32557	FlexConnect local switching standalone mode EoGRE client connecting as simple client
CSCvf75888	Unsupported Cisco 801s APs can still join the controller
CSCvf83983	client filter not working for Monitor clients page
CSCvf89335	Cisco 3700 AP stopped working with memory allocation failure CAPWAP
CSCvf91292	ME: For external webauth/CMX, the WLC landing page is displayed
CSCvf99887	MAP Gigabit port being learnt in Mesh management VLAN instead of client VLAN
CSCvg06111	WLC 'in sync' with NTP while authentication is ignored with invalid keys
CSCvg09787	8.6:GUI filtering is broken if change channel on XOR and back while this issue is not on 802.11a
CSCvg16095	Incorrect values of RSSI, SNR are being reported to WSA
CSCvg23810	PMTU change to 1500 from a lesser value is not reflected in AP
CSCvg27613	DHCP Proxy is enabled and DHCP Server info is removed from the Dynamic Interface, disables the WLAN
CSCvg34769	ME UI: Top 10 access point dashlet shows APs with 0 as stats

Caveat ID Number	Description
CSCvg43654	Cisco Wave 2 APs in FlexConect mode do not forward DHCP NAK to wireless client
CSCvg50680	AP3800 still advertises RSN IE after WLAN is changed to OPEN
CSCvg76166	Channel utilization changes to 0% on Marvell chipset based Cisco Wave 1 APs
CSCvg78210	AP syslog config does not change level from AP syslog to informational it remains in emergencies
CSCvg80634	WLC msglogs flooded with DNS-3-GETADDRINFO_SUCCESS every 10mins with DNS for NTP
CSCvg87933	AP1815w consumes PoE+ 802.3at instead of using 8-9 watts with PoE disabled
CSCvg94718	Standby WLC reloads unexpectedly on spamApTask
CSCvh19234	Stale DTLS connection entry is present in the standby WLC
CSCvh21605	ME - wired clients drop-off shortly after being started from show client ap remote-lan
CSCvh22988	Cisco controller reloads unexpectedly with task name emweb while accessing GUI
CSCvh58467	Kernel Panic with PC at skb_release_data+0xe0/0x230
CSCvh62827	Wireless client cannot communicate each other with dynamic VLAN
CSCvh67548	Cisco 1600AP sending de-auth frame with reason code 7 to Random MAC Address XX:XX:00:00:00:00
CSCvh77575	ATF monitor mode config for AP group is not reflecting on GUI
CSCvh86834	802.11w client association data traffic drops after 802.11r roaming with PMF enabled or optional
CSCvh96956	Cisco Wave 2 APs fails to translate downstream CAPWAP DSCP to correct 802.11e UP value
CSCvi00898	Valid client on Rogue AP does not work other than Mac delimiter as 'No delimeter'
CSCvi01147	LSC certificate keysize not retained after upload/download config
CSCvi04556	SSO failover causes mobilty tunnels go down
CSCvi06841	'show flexconnect status' gives no o/p if AP is in pure IPv6 network
CSCvi09153	Cisco Wave 1 APs radio reset due FST14 FW: cmd=0x31 seq=6 due to mcast stuck in radio
CSCvi13589	Locally generated webadmin certificate shows as 3rd party after upgrade on 8.3 code
CSCvi25724	Cisco IOS APs unexpectedly reloads due to bad CPQ on 8.5 release code
CSCvi27226	Cisco 3802 AP: Radio core - receive path hang - RX-RING-STUCK

Caveat ID Number	Description
CSCvi30627	Config missing after WLC failover
CSCvi30993	Lost neighbor AP field on WLC GUI - NEIGHBOR AND ROGUE APS
CSCvi32951	Cisco Wave 2 APs go offchannel if scan deferral value is greater than 255 msec
CSCvi42919	Cisco 702w AP - Radio resets with ath_ACIF_radio_dead message
CSCvi45149	No RSSI/SNR info displayed with show client detail
CSCvi48427	'Enable DHCP Option 82 - VPN select' setting is lost after WLC reload
CSCvi49126	RSN IE validation fails in M2 (802.11r session timeout) after reassociation causing deauth code 17
CSCvi51536	Access Point is not sending TCP fragments over the air
CSCvi51858	WLC not sending proper VSA list at acct-stop when client moves to another SSID
CSCvi53734	AP 3800 : ME mode: AP reloads unexpectedly due to capwapd after the upgrade
CSCvi57213	Cisco 1832 AP unexpectedly reloads with 'PC is at __napi_complete+0x28/0x60'
CSCvi65222	802.11 arp-cache does not work if BVI VLAN and client VLAN are different
CSCvi67565	TrustSec: AP picks wrong SXP Node ID
CSCvi72334	L2 roams fails for EOGRE client
CSCvi73013	Cisco Wave 1 AP deauthenticating client due to idle timeout
CSCvi73402	Cisco 1810W AP not giving IPs to cell phones using WPA/TKIP protocol
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
CSCvi78286	WLC Dashboard does not display the correct values for client throughput
CSCvi78819	HA : config service statistics not synced after failover
CSCvi80205	ETSI domain Compliance and Throughput testing
CSCvi82147	Failed to set Country Codes when WLC has redundant country codes CA2, KR, PH2, US2, USL, USX
CSCvi84511	Cisco 3800 AP with Wired1 (aux) LAN enabled - CDP-4-DUPLEX_MISMATCH messages constantly logged
CSCvi84734	Cisco 702w AP: client intermittently cannot connect- decrypt errors
CSCvi84843	Client filter matches WLAN SSID, not WLAN Profile or WLAN ID

Caveat ID Number	Description
CSCvi84849	Cisco 1852 series APs unexpectedly reloads due to Kernel Panic
CSCvi85464	AP specific configuration lost post ap reload - wlan-acl mappings and policies lost
CSCvi85834	New Mobility CAPWAP control keepalive should not plumb keys when receiving unencrypted responses
CSCvi86267	Mesh I-Domain: Supports 2.4-GHz only, hence default backhaul should be set to 2.4-GHz only
CSCvi86834	Mesh Ethernet bridging - wired client associated to MAP fails to pass traffic over tagged VLAN
CSCvi90766	Cisco AP with regulatory domain Morocco cannot join the Cisco WLC
CSCvi91017	The FlexConnect groups are missing in backup configuration file
CSCvi92170	Cisco 1800 series 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
CSCvi97282	Assigning a NetFlow monitor to the WLAN will internally enable AVC on WLC
CSCvj01739	Cisco WiSM2 unexpectedly reloads on task name sshpmLscTask after initial config
CSCvj03161	Cisco Wave 1 APs not reporting known interference with disabled WSSI module
CSCvj06837	Cisco Wave 1 MAP: Mesh security failures after roaming between 2 parents
CSCvj07805	Wrong syntax NVGEN'd for "sniffer" CLI, after the CSCvd01486 commit
CSCvj07930	Cisco 3802, 2802 AP with DART connectors has a Tx power value of 0
CSCvj08387	WLC reloads unexpectedly while working on spamApTask6
CSCvj11251	Cisco 2802 AP not sending re-association response to Cisco 8821 phone
CSCvj11270	Watchdog reset out of memory on Cisco 3800 AP running 8.3.133.0 code
CSCvj11397	Cisco 3504 Controller - OpenDNS registration failure - Return 77
CSCvj13920	WLC system reloads unexpectedly due to task name RRM-MGR-2_4-GRP
CSCvj17181	Creating a webauth CSR certificate on the WLC GUI does not allow spaces
CSCvj23235	WLC: Need to change active fall-back of AAA probing w/probes of 'dead' RADIUS server
CSCvj23814	IPsec tunnels not coming up with GCM ciphers
CSCvj25768	Bridge mode Cisco Wave 2 Mesh APs bridging issues

Caveat ID Number	Description
CSCvj26203	8.8: Config static IPv4 but still using DHCP IPv6/after AP joins WLC, still sends discovery requests
CSCvj28658	Cisco 1810wAP kernel panic leads to unexpected reload on PC at ieee80211_node_authorize+0x90/0xb8
CSCvj32964	WGB is only allowing 8 MAC addresses pass traffic using 3802 AP [as CAPWAP AP and 3702 AP as WGB]
CSCvj33894	Add 'show advanced hyperlocation summary' to 'show run-config' and 'show tech'
CSCvj35883	Allow Cisco 2800, 3800 APs to be able to convert to sensor mode
CSCvj36491	Corrupted phase calibration programmed in Triggerfish EEPROM
CSCvj36923	Cisco AP name mismatch with controller on join
CSCvj37393	Cisco Wav 2 APs not sending probe response when SSID is not broadcasted
CSCvj38456	WLC is losing its EoGRE configuration after reboot
CSCvj39633	CWA WLANs configured in 8.8 is shown as open+macfilter after downgrade to 8.5
CSCvj41040	Cisco 1800 APs in Cisco FlexConnect mode, fail FT roam
CSCvj41817	IOS AP 3702 fails to upgrade from 8.3.141.0 to 8.5MR3 with 3802 as ME
CSCvj44800	Client entries getting deleted from standby controller post AP FT - client sync failing in HA
CSCvj47445	Cisco WLC sending CAPWAP discovery response when it has no available licenses
CSCvj47452	NTP MD5 key cannot be retrieved, by which time sync is failed- upgrade downgrade test 8.2 to 8.5
CSCvj47460	Cisco WiSM2 reloads unexpectedly on SNMP task
CSCvj48364	Cisco Controller is generating client traps without a session-id
CSCvj48448	Need to remove Optimized Roaming option from Moblity Express from releases earlier than 8.8
CSCvj50100	8.8 ME Free memory decreasing on ME setups over the time
CSCvj50170	Client coming back within 10 seconds of cleanup time is stopping the DHCP timer on the WLC
CSCvj53743	Cisco 1572IC AP: Channels and Maximum Power Settings settings spreadsheet incorrect values for V02
CSCvj56030	Make WSA Agent restartable from watchdog
CSCvj56689	8.5 MR3: AP1850 stopped working due to OOM

Caveat ID Number	Description
CSCvj60609	Cisco vWLC web authentication not working
CSCvj61140	Having Sensor-Driven tests configured cause 3802I AP to intermittent unexpected reload
CSCvj62672	WLC sending wrong NAS ID when AAA override is enabled
CSCvj65449	AIR-AP1562D-E-K9 with regulatory domain Kazakhstan does not join the WLC
CSCvj69146	CME reloads unexpectedly in a loop due to PMALLOC_DOUBLE_FREE (capwap_ac_sm.c)
CSCvj70604	Cisco mesh APs Best-Effort Tx queue stuck
CSCvj70790	Cisco Aironet 1800, 2800, and 3800 Series AP ARP Request Handling DoS Vulnerability
CSCvj71905	Change in MIB collection behaviour
CSCvj72136	Cisco 2800, 3800 APs loose its ability to reach the default gateway
CSCvj72766	UX AP:Primed UX AP reset to UX when SNTP server is configured
CSCvj72890	Cisco 5520 WLC reloads unexpectedly when RADIUS server returns invalid value in Airespace-ACL-Name
CSCvj73077	Cisco 1810W APs may have power denied from older PoE 802.3af switches
CSCvj76009	Cisco 3800, 2800 APs: multiple WSA Agent process running, that might be the cause of OOM trigger
CSCvj76378	Local policy is not applied when foreign WLC is running 8.3.141.0
CSCvj77078	WLC unexpectedly reboots on Dot1x_NW_MsgTask_1
CSCvj79108	WSA-8.5- NAC restarted with signal 6 after few minutes of WSA enabled in scale setup
CSCvj79479	Cisco 8500 Wireless LAN Controller web interface unvalidated web page redirect vulnerability
CSCvj79831	AP Tx/Rx accounting information only reaches 2147483647 as max value
CSCvj80388	Flex-ACL on Wave 2 AP's denying host instead of subnet
CSCvj81101	Cisco 2800, 3800 VAPs/TBTT timers are not enabled properly
CSCvj86238	Cisco controller stops working as emWeb spikes to 100% CPU usage after executing 'show run-config'
CSCvj91645	Clients not getting exported to anchor on New Mobility
CSCvj92959	Day0 config push from app to WLC is considered as Dynamic IP instead of static IP

Caveat ID Number	Description
CSCvj94659	Unable to update TACACS+ DNS parameters on configuring IPv6 DNS server under global settings
CSCvj94919	Cisco 702w AP running VLAN ID is NA after AP reboot
CSCvj95464	Ethernet Bridging: Low throughput
CSCvj95744	Cisco 3700 AP -Downstream ping test fails for WGB wired client with FlexConnect local switching
CSCvj95984	Cisco 3800, 4800 APs seems to be hung in PoE negotiation, unable to be reloaded from console either
CSCvj96316	Cisco 2800, 3800 APs in Local mode leaks some MAC addresses from clients into the Local switch port
CSCvj97129	Neighbor packet Tx failure on Cisco 1542, 1562, and 1815 APs
CSCvj97430	Mobility Express AP - Loop detected that causes AP reboot
CSCvk00884	The WLC is replying with the wrong value for the following OID: bsnAPIfProfileParamAssignment
CSCvk02153	Wave 1 AP WLAN Client Stats cldcClientDataRetries counter is zero
CSCvk03686	EoGRE client count is not getting cleared in Standby on switching SSID
CSCvk05396	vEWLC:3802I reloads with capwapvpndecap/cw_mcast_reasm :: CapwapReassembler - bad mem_used
CSCvk05965	Cisco WLC in HA SSO: standby controller is in a reboot loop
CSCvk06178	Uplink BPDUs are not bridged
CSCvk06974	1815AP logs flooded with TLV-DEC-ERR: cannot process TLV for TLV_DMS_CLIENT_REQUEST_PAYLOAD
CSCvk09513	AP is not downloading the WLC 85Mr3 image rather it says image is already in the backup
CSCvk15043	Wave 1 APs - AP radio FW image install failure in the bootup loop
CSCvk15068	IOS APs, recovery logic for failure on primary image
CSCvk15165	Cisco Controller reloads unexpectedly after modifying SNMP trap controls via GUI
CSCvk18752	Cisco 1815AP: Incorrect VCI string of DHCP option 60
CSCvk19286	Policy mapped with WLAN and AP group lost during upload download config file
CSCvk20801	MAC OUI database not getting updated
CSCvk22312	Hotspot 2.0 OSU SSID is picking profile name

Caveat ID Number	Description
CSCvk23508	No legacy rates; default to lowest CCK/OFDM rate
CSCvk23577	Client is unable to connect due to the 'Failed to create a timer' error
CSCvk24360	WLC power supply status is incorrect when there is no power supply
CSCvk25593	Cisco 1542, 1815I APs - Ethernet interface flapping when connected to 100Mbit switchports
CSCvk26519	Cisco 1562 MAP stops sending Block ACK once the Cisco 1572 RAP moves to another controller
CSCvk26563	Cisco 1810W AP running 8.2.170.4 code: 5G radio FW resets @0x009A4F9F
CSCvk27093	NAS-ID in WLAN cannot be changed in the startup-command after you saved once
CSCvk35047	Cisco WLC stops working when LAG mode is enabled on the AP
CSCvk36887	Some clients cannot associate because their entry is not getting deleted at the WLC.
CSCvk38453	AP does not initiate the CAPWAP discovery process, it gets stuck during the PNP discovery process
CSCvk38950	DNAC UI is not showing international character name SSID
CSCvk39432	IPv6 Frag:Changing PMTU on router to IPv6 minimum(1280) is not changing AP PMTU to 1280 for Wave2 AP
CSCvk39948	WLC is not returning the expected prompt when logging in via SSH
CSCvk41068	Advance IPMI is not set and causing fan noise
CSCvk41512	APX800 sniffer mode not sending frames with AMSDU 1500 Bytes to destination
CSCvk42592	Disabling 'Out of box' in RF Profiles throws SNMP error
CSCvk43936	2800/3800 AP with LAG enabled would bridge BPDU packets
CSCvk44831	LSC certificate: Cisco Wave 2 APs not taking configured LSC cert keysize
CSCvk44959	Cisco controller reloads unexpectedly on Taskname 'emWeb'
CSCvk46817	AIR-AP2802I not sending beacons with both radios in 5GHz
CSCvk51634	Wave 2 Flex Efficient Upgrade fails as primary AP sends empty image_str to WLC
CSCvk53743	8.5_New mobility:UI throws wrong error message while adding used public IP
CSCvk53963	DNS-ACL - Cisco 1815 ME switchdriver reloads unexpectedly running 8.8.2.18 code
CSCvk55651	Cisco 1852 AP failure of association due to set CAPWAP tunnel failed
CSCvk59498	Cisco 3702 AP: High CPU utilization under NCI Rx. Unable to join the controller

Caveat ID Number	Description
CSCvk59536	Unable to upgrade to 8.8+ ME from 8.7
CSCvk61078	VLAN priority tag inside the EoGRE packet set to non-zero when 802.1p set to none in LOCAL mode
CSCvk62055	Cisco Wave 2 APs Preimage download fails after 64 retries with poor WAN link
CSCvk62355	CAP2800 on ME image 8.6.101.0, 8.7.106.0 reloads unexpectedly in ewsContexSendRedirect200->ewaDate
CSCvk62680	Cisco WiSM2 not releasing licenses after reboot
CSCvk63215	Cisco 1852 series APs Kernel Panic due to NSS memory corruption
CSCvk63459	Cisco 3802, 4800 AP drops packets larger than 1426 (inner IP) with VxLAN
CSCvk63784	8.5MR4 - Error string is not getting updated in last error field in 'show network assurance summary'
CSCvk64829	Observing CMX Certificate error and WSA certificate related XML message on Mobility Express
CSCvk65908	Cisco 5520 controller reloads unexpectedly with taskname emWeb when checking "show tech-support"
CSCvk66354	8.5MR4 - GUI issues with Assurance statistics
CSCvk66762	8.5MR4: Error sending/receiving register device request/rsp ACT2 could not be registered in TAM
CSCvk71715	8.8 WLC: Client events gets dropped during continuous assoc and auth events
CSCvk72075	WLC is sending incorrect counter value for the broadcast and multicast throgh SNMP
CSCvk73639	Cisco controller to support OUI based Client Profiling
CSCvk76043	Unable to Associate clients with PSK/dot1x security in Flexconnect Standalone Mode.
CSCvm00214	Cisco WiSM2 memory leak due to hotspot_anqp
CSCvm02935	Ethernet bridging with VLAN Transparent enabled does not work with non-native VLAN
CSCvm03831	Cisco 5500 Series controller on 8.5.137.35 code reloads unexpectedly with SNMPTask
CSCvm04245	Cisco 1810W AP reports low power after requesting and receiving 14.2W after upgrading to 8.5.131.0
CSCvm05695	AAA override for native VLAN with flexlocal switching not applied to client on Cisco 1562 AP
CSCvm07201	Cisco 3700AP +HALO: NULL in rrmClientMonitorNeighborUpdate after WSSI disabled+WIPS submode

Caveat ID Number	Description
CSCvm10716	Cisco WLC or ME is not sending WLAN post-auth ACL to AP if AAA accept receive w/o any ACL
CSCvm11060	WLC: After soft-roam of client, client is not able to see new Apple TV from associated AP-Grp VLAN
CSCvm14183	In GUI unexpected Error Message while disable AVC with Flow Monitor configuration
CSCvm15331	Adding Cisco 802 APs PIDs to support new ETSI regulation
CSCvm15469	Evaluation of click-ap for CVE-2018-5391 (FragmentSmack)
CSCvm15625	DCA channel assignment on XOR radio is broken while static 5G assignment
CSCvm18273	Cisco 702W AP: Runs out of memory and reloads
CSCvm19309	Cisco 8510 controller IMM configuration is not taking effect
CSCvm23672	Sometimes Cisco Wave 2 AP does not send IAPP update after client address change
CSCvm25082	EoGRE clients ARP Response inside CAPWAP gets corrupted
CSCvm33617	Configuration file should not be modified due to low flash memory
CSCvm34641	Cisco controller is sending packets out to Gateway with DF =1 when inside header is set DF =0 -EoGRE
CSCvm41626	Assoc/Disso stat trap on GUI enables enhanced Assoc/Disso stat trap but does not generate stat traps
CSCvm46810	Cisco controller reloads unexpectedly in Dot1x_NW_MsgTask_7 due to validateWpaKeyStateSTART
CSCvm51362	Cisco controller reloads unexpectedly due to data plane crash
CSCvm51648	Cisco WLC open auth guest clients unable to pass traffic and PEM state struck in STATICIP_NOL3SEC
CSCvm60915	Cisco 3800 AP stops passing traffic under client load in MU-MIMO deployment
CSCvm62619	Cisco controller reloads unexpectedly with task emweb after 'debug flexconnect' command is typed
CSCvm65360	Cisco controller redirects to internal webauth login page after successful external webauth login
CSCvm71487	Cisco 2800, 3800 APs: dropping the Neighbor Advertisement for Global IPv6 address
CSCvm73919	Ciso 1832 AP: kernel panic due to "WLAN driver causing looping in the code"
CSCvm78368	Leak in I/O memory - middle buffers - due to LWAPP IPv6
CSCvm84941	Cisco 1600, 1700 APs: memory leak due to packets accumulation

Caveat ID Number	Description
CSCvm87777	New mobility: Control path remain down in 2500 WLC if AirOS WLC mgmt address is higher than NGWC
CSCvm90337	Cisco 18xx APs unexpectedly reload due to 'radio failure (radio recovery failed)'
CSCvn03560	Decrypt errors seen on Cisco 702 AP
CSCvn11713	Cisco AP702w Beacon Stuck

Related Documentation

Wireless Products Comparison

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

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

- Product Approval Status:

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

- Wireless LAN Compliance Lookup:

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

Cisco Wireless Controller

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

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

For all controller software related documentation, see:

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

Cisco Mobility Express

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

Cisco Aironet Access Points for Cisco IOS Releases

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

Open Source Used in Controller and Access Point Software

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

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

Cisco Prime Infrastructure

Cisco Prime Infrastructure Documentation

Cisco 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.

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.