Release Notes for Cisco Wireless Controllers and Lightweight Access Points, Cisco Wireless Release 8.3.150.0

First Published: 2019-03-16

Last Modified: 2019-04-18

About the Release Notes

This release notes document describes what is new or changed in this release, instructions to upgrade to this release, and open and resolved caveats for this release. Unless otherwise noted, in this document, Cisco Wireless Controllers are referred to as *controllers*, and Cisco lightweight access points are referred to as *access points* or *APs*.

Content Hub

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

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

Do provide feedback about your experience with the Content Hub.

Revision History

Table 1: Revision History

Modification Date	Modification Details
April 18, 2019	Resolved Caveats—Added table **Cisco Security Advisories Caveats**.

Cisco Wireless Controller and Access Point Platforms

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 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 Controllers on VMware ESXi and Kernel-based virtual machine (KVM) systems.

Note Kernel-based virtual machine (KVM) is supported in Cisco Wireless Release 8.1 and later releases. 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 5508 WLC, Cisco 5520 WLC, Cisco Wireless Services Module 2 (Cisco WiSM2), Cisco Flex 7510 WLC, Cisco 8510 WLC, and Cisco 8540 WLC.

Note AP Stateful switchover (SSO) is not supported on Cisco 2504 WLCs.

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

Supported Access Point Platforms

The following access point platforms are supported in this release:

- Cisco Aironet 1040 Series Access Points
- Cisco Aironet 1140 Series Access Points
- Cisco Aironet 1260 Series Access Points
- Cisco Aironet 1600 Series Access Points
- Cisco Aironet 1700 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 600 Series OfficeExtend Access Points
- Cisco Aironet 700 Series Access Points
- Cisco Aironet 700W Series Access Points
- Cisco AP802 Integrated Access Point
- Cisco AP803 Integrated Access Point
- Cisco ASA 5506W-AP702
- Cisco Aironet 1530 Series Access Points
- Cisco Aironet 1550 Series Access Points
- Cisco Aironet 1560 Series Access Points
- Cisco Aironet 1570 Series Access Points
- Cisco Industrial Wireless 3700 Series Access Points

Note The Cisco 1040 Series, 1140 Series, and 1260 Series access points have feature parity with Cisco Wireless Release 8.0. Features introduced in Cisco Wireless Release 8.1 and later are not supported on these access points.

Note Before you associate Cisco Aironet 1830 Series and 1850 Series APs with Cisco vWLC running Cisco 8.3.112.0 release software, you must upgrade the APs to Cisco 8.3.112.0 release.

Note Cisco AP802 and AP803 are integrated access points on the Cisco 800 Series Integrated Services Routers (ISRs). For more information about the stock-keeping units (SKUs) for the AP802s and AP803s Cisco ISRs, see http://www.cisco.com/c/en/us/products/routers/800-series-routers/brochure-listing.html. Before you use a Cisco AP802 series lightweight access point with Cisco Wireless Release 8.4, you must upgrade the software in the Cisco 800 Series ISRs to Cisco IOS 15.1(4)M or later releases.

Note 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.

What's New in Release 8.3.150.0

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.

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

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

- Before you upgrade to this release, we recommend that you remove the **config network web-auth port** *443* configuration, if present.

  Follow these steps to remove this configuration:

  1. Check if the configuration is present by entering this command:

  grep include "config network web-auth port 443" "show run-config startup-commands"

  2. If there are any matches, then remove this configuration by entering this command:

  config network web-auth port 0

  3. Save the configuration by entering this command:

  save config

  You can now go ahead with the upgrade procedure. For more information about why you are required to do this configuration, see CSCvi13589.

- We recommend that you install Release 1.9.0.0 of Cisco Wireless LAN 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/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, see https://www.cisco.com/c/en/us/td/docs/wireless/controller/release/notes/fus_rn_OL-31390-01.html.

  Note If you are using a Cisco 2500 Series controller, you must install Release 1.9.0.0 or higher of Cisco Wireless LAN Controller FUS. This is not required if you are using other controller hardware models.

  Note The FUS image installation process reboots the Cisco WLC several times and reboots the runtime image. The entire process takes approximately 30 minutes. We recommend that you install the FUS image in a planned outage window.

- Release 8.3 supports additional configuration options for 802.11r FT enable and disable. The additional configuration option is not valid for older releases. If you downgrade from Release 8.3.x 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 8.3.150.0 to a 7.x release, the trap configuration is lost and must be reconfigured.
- If you downgrade from Release 8.3.150.0 to Release 8.1, the Cisco Aironet 1850 Series AP, whose mode prior to the downgrade was Sensor 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 8.3.150.0 or a later release, ensure that the following is done:
  - Enable IPv4 and DHCPv4 on the network—Load a new Cisco WLC software image on all Cisco WLCs plus Supplementary AP Bundle images on the Cisco 2504 WLC, 5508 WLC, and WiSM2 or perform a predownload of AP images on the required Cisco WLCs.
  - Reboot Cisco WLC immediately or at the preset time.
  - Ensure that all Cisco APs are associated with Cisco WLC.
  - Disable IPv4 and DHCPv4 on the network.
- After downloading new software to the Cisco APs, it is possible that a Cisco AP may get stuck in an "upgrading image" state. In such a case of a stranded Cisco AP, it may be necessary to forcefully reboot the Cisco WLC to download a new image or to reboot the Cisco WLC after the download of the new image. You can forcefully reboot the Cisco WLC by entering the **reset system forced** command.
- It is not possible to download some of the older configurations from the Cisco WLC because of the Multicast and IP address validations. See the "Restrictions on Configuring Multicast Mode" section in the configuration guide for detailed information about platform support for Global Multicast and Multicast Mode.
- If you upgrade from Release 8.0.110.0 to a later release, the **config redundancy mobilitymac** *mac-addr* command's setting is removed. You must manually reconfigure the mobility MAC address after the upgrade.
- If you are upgrading from Release 8.0.140.0 or 8.0.15x.0 to a later release and also have the multiple country code feature configured, the feature configuration is corrupted after the upgrade. For more information, see CSCve41740.
- If you have ACL configurations in a Cisco WLC, and downgrade from a 7.4 or later release to a 7.3 or earlier release, you might experience XML errors on rebooting the Cisco WLC. However, these errors do not have any impact on any of the functionalities or configurations.
- 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 FlexConnect APs (known as H-REAP APs in the 7.0.x releases) that are associated with a Cisco WLC that has all the 7.0.x software releases prior to Release 7.0.240.0, upgrade to Release 8.3.150.0, the APs lose the enabled VLAN support configuration. The VLAN mappings revert to the default values of the VLAN of the associated interface. The workaround is to upgrade from Release 7.0.240.0 and later 7.0.x releases to Release 8.3.150.0.

Note In case of FlexConnect VLAN mapping deployment, we recommend that the deployment be done using FlexConnect groups. This allows you to recover VLAN mapping after an AP rejoins the Cisco WLC without having to manually reassign the VLAN mappings.

- 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.
- After you upgrade to Release 7.4, networks that were not affected by the existing preauthentication access control lists might not work because the rules are now enforced. That is, networks with clients configured with static DNS servers might not work unless the static server is defined in the preauthentication ACL.
- On the Cisco Flex 7500 Series WLCs, if FIPS is enabled, the reduced boot options are displayed only after a bootloader upgrade.

Note Bootloader upgrade is not required if FIPS is disabled.

- If you have to downgrade 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 saved on the backup server, or to reconfigure the Cisco WLC.
- It is not possible to directly upgrade to Release 8.3.150.0 release from a release that is earlier than Release 7.0.98.0.
- You can upgrade or downgrade the Cisco WLC software only between certain releases. In some instances, you must first install an intermediate release prior to upgrading to Release 8.3.150.0. The following table shows the upgrade path that you must follow before downloading Release 8.3.150.0.

Note If you upgrade directly to 7.6.x or a later release from a release that is earlier than 7.5, the predownload functionality on Cisco Aironet 2600 and 3600 APs fails. The predownload functionality failure is only a one-time failure. After the upgrade to 7.6.x or a later release, the new image is loaded on the said Cisco APs, and the predownload functionality works as expected.

For detailed release recommendations, see the *Guidelines for Cisco Wireless Software Release Migration Bulletin* at: https://www.cisco.com/c/en/us/products/collateral/wireless/8500-series-wireless-controllers/bulletin-c25-738147.html

Table 3: Upgrade Path to Cisco Wireless Software Release 8.3.150.0

Current Software Release	Upgrade Path to 8.3.150.0 Software
8.0.x	You can upgrade directly to Release 8.3.150.0.
8.2.x	You can upgrade directly to Release 8.3.150.0. See the "Changes in Images and Installation Procedure for Cisco 2504 WLC, Cisco 5508 WLC, and Cisco WiSM2" section in the 8.3 release notes about special upgrade instructions for Cisco 2504 WLC, 5508 WLC, and WiSM2.
8.3.x	You can upgrade directly to Release 8.3.150.0.

- When you upgrade the Cisco WLC to an intermediate software release, you must wait until all of the access points that are associated with the 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 access point.
- You can upgrade to a new release of the Cisco WLC software or downgrade to an earlier release even if Federal Information Processing Standard (FIPS) is enabled.
- When you upgrade to the latest software release, the software on the access points associated with the Cisco WLC is also automatically upgraded. When an access point is loading software, each of its LEDs blinks in succession.
- We recommend that you access the Cisco WLC GUI using Microsoft Internet Explorer 10 or a later version or Mozilla Firefox 32 or a later version.

Note Microsoft Internet Explorer 8 might fail to connect over HTTPS because of compatibility issues. In such cases, you can explicitly enable SSLv3 by entering the **config network secureweb sslv3 enable** command.

- Cisco WLCs support standard SNMP MIB files. MIBs can be downloaded from the Software Center on Cisco.com.
- The Cisco WLC software is factory installed on your Cisco WLC and is automatically downloaded to the access points after a release upgrade and whenever an access point joins a Cisco WLC. We recommend that you install the latest software version available for maximum operational benefit.
- Ensure that you have a TFTP, 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 Release 8.3.150.0. Some TFTP servers that support files of this size are tftpd32 and the TFTP server within the Prime Infrastructure. If you attempt to download the 8.3.150.0 Cisco WLC software 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 5500 Series WLC differ from the menu options for the other Cisco WLC platforms.

  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:
```

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 pertaining to your Cisco WLC platform for more details on running the bootup script and 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 menu to boot from the backup image. Then, upgrade with a known working image and reboot the 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**}

  Here:

  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 for the **config network ap-discovery nat-ip-only** command. To disable AP link latency, use the **config ap link-latency disable all** command.

- You can configure 802.1p tagging by using the **config qos dot1p-tag** {**bronze** | **silver** | **gold** | **platinum**} command. For Release 7.2.103.0 and later releases, if you tag 802.1p packets, the tagging has an impact on only wired packets. Wireless packets are impacted only by the maximum priority level set for QoS.

- You can reduce the network downtime using the following options:

  - You can predownload the AP image.

- For FlexConnect access points, use the FlexConnect AP upgrade feature to reduce traffic between the Cisco WLC and the AP (main site and the branch). For more information about the FlexConnect AP upgrade feature, see the *Cisco Wireless Controller Configuration Guide*.

- Do not power down the Cisco WLC or any access point during the upgrade process; otherwise, you might corrupt the software image. Upgrading a Cisco WLC with a large number of access points can take as long as 30 minutes, depending on the size of your network. However, with the increased number of concurrent access point upgrades supported, the upgrade time should be significantly reduced. The access points must remain powered, and the Cisco WLC must not be reset during this time.
- To downgrade from Release 8.3.150.0 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 the Cisco WLC, reboot the Cisco WLC for the changes to take effect:
  - Enable or disable link aggregation (LAG)
  - Enable a feature that is dependent on certificates (such as HTTPS and web authentication)
  - Add a new license or modify an existing license
  - 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
  - Make changes to TCP MSS settings

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

Due to an increase in the size of the Release 8.3.150.0 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:
  - AP802

- Cisco Aironet 1530 Series AP
- Cisco Aironet 1550 Series AP (with 64-MB memory)
- Cisco Aironet 1550 Series AP (with 128-MB memory)
- Cisco Aironet 1570 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 Release 8.3.150.0 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
Cisco 2504 WLC	AIR-CT2500-K9-8-3-150-0.aes	AIR-CT2500-AP_BUNDLE-K9-8-3-150-0.aes
Cisco 5508 WLC	AIR-CT5500-K9-8-3-150-0.aes AIR-CT5500-LDPE-K9-8-3-150-0.aes	AIR-CT5500-AP_BUNDLE-K9-8-3-150-0.aes AIR-CT5500-LDPE-AP_BUNDLE-K9-8-3-150-0.aes
Cisco WiSM2	AIR-WISM2-K9-8-3-150-0.aes	AIR-WISM2-AP_BUNDLE-K9-8-3-150-0.aes

Note AP_BUNDLE or FUS installation files from Release 8.3 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 to Cisco WLC Software Release 8.3.150.0 (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 Release 8.3.150.0 software:

a) Browse to https://software.cisco.com/download/home.
b) Choose **Wireless** from the center selection window.
c) Click **Wireless LAN Controllers**. The following options are displayed. Depending on your Cisco WLC platform, select either of these options:

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

d) Select the Cisco WLC model number or name.
The **Download Software** page is displayed.

e) The software releases are labeled as follows 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.

f) Click the filename (filename.aes).

Note In Release 8.3.102.0, 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, to upgrade to Release8.3.150.0, 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, Cisco Aironet 1530 Series AP, Cisco Aironet 1550 Series AP (with 64-MB memory), Cisco Aironet 1550 Series AP (with 128-MB memory), and/or Cisco Aironet 1570 Series APs. For more information, see the "Changes in Images and Installation Procedure for Cisco 2504 WLC, Cisco 5508 WLC, and Cisco WiSM2" section.

g) Click **Download**.
h) Read the Cisco End User Software License Agreement and click **Agree**.
i) Save the file to your hard drive.
j) Repeat steps a through *i* 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 802.11a/n and 802.11b/g/n networks.

Note For busy networks, Cisco WLCs on high utilization, and small Cisco WLC platforms, we recommend that you disable the 802.11a/n and 802.11b/g/n 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** text box, 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** text field, and 6 seconds for the Timeout text field should work correctly without any adjustment. However, you can change these values, if desired. To do so, enter the maximum number of times that the TFTP server attempts to

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

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

Step 11 In the **File Name** text box, 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** text box, enter the username with which to log on to the FTP server.
b) In the **Server Login Password** text box, enter the password with which to log on to the FTP server.
c) In the **Server Port Number** text box, 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 appears indicating the status of the download.

Note In Release 8.3.102.0, 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, to upgrade to Release8.3.150.0, 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, Cisco Aironet 1530 Series AP, Cisco Aironet 1550 Series AP (with 64-MB memory), Cisco Aironet 1550 Series AP (with 128-MB memory), and/or Cisco Aironet 1570 Series 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 on the Catalyst switch, check the port channel and re-enable the port channel if necessary.

Step 18 If you have disabled the 802.11a/n and 802.11b/g/n networks, re-enable them.

Step 19 To verify that the 8.3.150.0 Cisco WLC software is installed on your Cisco WLC, click **Monitor** on the Cisco WLC GUI 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 in Release 8.3.15x.0

This section describes the interoperability of Cisco WLC Software, Release 8.3.15x.0 with other client devices.

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

Test Bed Configuration for Interoperability

Hardware/Software Parameter	Hardware/Software Configuration Type
Release	8.3.15x.0
Cisco WLC	Cisco 55xx Series Wireless Controller
Access points	AIR-CAP3802E-B-K9, AIR-AP1852E-B-K9, AIR-CAP3602E-A-K9

Radio	802.11ac, 802.11a, 802.11g, 802.11n (2.4 GHz / 5.0 GHz)
Security	Open, PSK (WPA-TKIP-WPA2-AES), 802.1X (WPA-TKIP-WPA2-AES) (EAP-FAST, EAP-TLS)
RADIUS	ISE 2.2, ISE 2.3
Types of tests	Connectivity, traffic (ICMP), and roaming between two APs

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

Table 8: Laptop

Client Name	Version Details
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
Intel 9260	20.20.2.2
Broadcom 4360	6.30.163.2005
Dell 1520/Broadcom 43224HMS	5.60.48.18
Dell 1530 (Broadcom BCM4359)	5.100.235.12
Dell 1560	6.30.223.262
Dell 1540	6.30.223.215
Samsung Chromebook	55.0.2883.103
HP Chromebook	55.0.2883.103
MacBook Pro	OSX 10.11.6
MacBook Air old	OSX 10.11.5
MacBook Air new	OSX 10.12.2
Macbook Pro with Retina Display	OSX 10.12
Macbook New 2015	OSX 10.12.4

Table 9: Tablets

Client Name	Version Details
Apple iPad2	iOS 10
Apple iPad 3	iOS 10
Apple iPad mini with Retina display	iOS 10
Apple iPad Air	iOS 10
Apple iPad Air 2	iOS 11
Apple iPad Pro	iOS 11.0.3
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

Table 10: Mobile Devices

Client Name	Version Details
Apple iPhone 4s	iOS 10.2.1
Apple iPhone 5	iOS 10.2.1
Apple iPhone 5c	iOS 10.3.1
Apple iPhone 5s	iOS 10.2.1
Apple iPhone 6	iOS 10.3.1
Apple iPhone 6 Plus	iOS 10.3.1
Apple iPhone 6s	iOS 10.2.1

Client Name	Version Details
Apple iPhone 7	iOS 11.2.5
Apple iPhone X	iOS 11.1.2
Cisco 7925G-EX	CP7925G-1.4.8.4.LOADS
Cisco 7926G	CP7925G-1.4.5.3.LOADS
Cisco 8821	sip8821.11-0-3ES2-1
Cisco 8861	Sip88xx.10-2-1-16
Cisco-9971	sip9971.9-4-1-9
Google Nexus 5	Android 6.0.1
Google Nexus 5X	Android 8.0.0
Google Pixel	Android 7.1.1
HTC One	Android 5.0
LG G4	Android 5.1
Nokia Lumia 1520	Windows Phone 8.10.14219.341
OnePlus One	Android 4.3
OnePlus Three	Android 6.0.1
Samsung Galaxy Mega SM900	Android 4.4.2
Samsung Galaxy Nexus GTI9200	Android 4.4.2
Samsung Galaxy S III	Android 4.3
Samsung Galaxy S4	Android 5.0.1
Samsung Galaxy S4 T-I9500	Android 5.0.1
Samsung Galaxy S5	Android 4.4.2
Samsung Galaxy S5-SM-G900A	Android 4.4.2
Samsung Galaxy S6	Android 7.0
Samsung Galaxy S7	Android 7.0
Sony Xperia Z Ultra	Android 4.4.2
Vocera Badge	B3000 and B3000N
Xiaomi Mi 4c	Android 5.1
Xiaomi Mi 4i	Android 6.0.1

Table 11: Printers

Client Name	Version Details
HP Color LaserJet Pro M452nw	2.4.0.125

Features Not Supported on Cisco WLC Platforms

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

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

Key Features Not Supported on Cisco 2504 WLCs

- Autoinstall
- Cisco WLC integration with Lync SDN API
- Application Visibility and Control (AVC) for FlexConnect local switched access points
- Application Visibility and Control (AVC) for FlexConnect centrally switched access points

  Note However, AVC for local mode APs is supported. If you are using a Cisco 2500 Series controller and you intend to use the Application Visibility and Control (AVC) and NetFlow protocol features, you must install Release 1.9.0.0 of Cisco Wireless LAN Controller FUS. This is not required if you are using other controller hardware models.

- 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.

Note Directly connected APs are supported only in the local mode.

Key Features Not Supported on WiSM2 and Cisco 5508 WLCs

- Spanning Tree Protocol (STP)
- Port Mirroring
- VPN Termination (such as IPsec and L2TP)
- VPN Passthrough Option

  Note You can replicate this functionality on a Cisco 5500 Series WLC by creating an open WLAN using an ACL.

- Configuration of 802.3 bridging, AppleTalk, and Point-to-Point Protocol over Ethernet (PPPoE)
- Fragmented pings on any interface
- Right-to-Use Licensing
- Cisco 5508 WLC cannot function as mobility controller (MC). However, Cisco 5508 WLC can function as guest anchor in a New Mobility environment.
- Cisco Smart Software Licensing

Key Features Not Supported on Cisco Flex 7510 WLCs

- Static AP-manager interface

  Note For Cisco Flex 7500 Series WLCs, it is not necessary to configure an AP-manager interface. The management interface acts as an AP-manager interface by default, and the access points can join on this interface.

- IPv6 and Dual Stack client visibility

  Note IPv6 client bridging and Router Advertisement Guard are supported.

- Internal DHCP server

- Access points in local mode

Note An AP associated with the Cisco WLC in the local mode should be converted to the FlexConnect mode or monitor mode, either manually or by enabling the autoconvert feature. On the Cisco Flex 7500 WLC CLI, enable the autoconvert feature by entering the config ap autoconvert enable command.

- Mesh (use Flex + Bridge mode for mesh-enabled FlexConnect deployments)
- Spanning Tree Protocol (STP)
- Cisco Flex 7500 Series WLC cannot be configured as a guest anchor Cisco WLC. However, it can be configured as a foreign Cisco WLC to tunnel guest traffic to a guest anchor Cisco WLC in a DMZ.
- Multicast

Note FlexConnect local-switched multicast traffic is bridged transparently for both wired and wireless on the same VLAN. FlexConnect access points do not limit traffic based on Internet Group Management Protocol (IGMP) or MLD snooping.

- PMIPv6
- Cisco Smart Software Licensing
- EoGRE

Key Features Not Supported on Cisco 5520, 8510, and 8540 WLCs

- Internal DHCP Server
- Mobility controller functionality in converged access mode

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

- Spanning Tree Protocol (STP)
- Port Mirroring
- VPN Termination (such as IPsec and L2TP)
- VPN Passthrough Option

Note You can replicate this functionality by creating an open WLAN using an ACL.

- Configuration of 802.3 bridging, AppleTalk, and Point-to-Point Protocol over Ethernet (PPPoE)
- Fragmented pings on any interface

- Cisco 5520, 8510, and 8540 WLCs cannot function as mobility controller (MC). However, they can function as guest anchor in a New Mobility environment.

Key Features Not Supported on Cisco Virtual WLCs

- Internal DHCP server
- TrustSec SXP
- Access points in local mode
- Mobility/Guest Anchor
- Wired Guest
- Multicast

Note FlexConnect local-switched multicast traffic is bridged transparently for both wired and wireless on the same VLAN. FlexConnect access points do not limit traffic based on IGMP or MLD snooping.

- FlexConnect central switching in large-scale deployments

Note
- FlexConnect central switching is supported in only small-scale deployments, wherein the total traffic on Cisco WLC ports is not more than 500 Mbps.
- FlexConnect local switching is supported.

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

Features Not Supported on Access Point Platforms

Key Features Not Supported on Cisco Aironet 1520 and 1550 APs (with 64 MB memory)

- PPPoE
- PMIPv6
- EoGRE

See the amount of memory in a Cisco Aironet 1550 AP by entering this command in Cisco WLC CLI:

show mesh ap summary

Key Features Not Supported on Cisco Aironet 1560, 1810 OEAP, 1810W, 1815, 1830, 1850, 2800, and 3800 Series APs

Table 12: Key Features Not Supported on Cisco Aironet 1560, 1810 OEAP, 1810W, 1815, 1830, 1850, 2800 and 3800 Series APs

Operational Modes	• Spectrum Expert Connect • Autonomous Bridge and Workgroup Bridge (WGB) mode • Mesh mode • Flex plus Mesh • 802.1x supplicant for AP authentication on the wired port • Link aggregation (LAG) behind NAT/PAT environment
Protocols	• 802.11u • Full Cisco Compatible Extensions (CCX) support • Rogue Location Discovery Protocol (RLDP) • Native IPv6 • Internet Group Management Protocol (IGMP) v3

Security	• TrustSec SXP • 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	• Per Client AAA (QoS Override) • Bidirectional rate-limiting • Split Tunneling • EoGRE • PPPoE • Multicast to Unicast (MC2UC) • Traffic Specification (TSpec) • Cisco Compatible Extensions (CCX) • Call Admission Control (CAC) • DHCP Option 60 • NAT/PAT support • VSA/Realm Match Authentication • Link aggregation (LAG) • MAC Authentication Flex Local Authentication • SIP snooping with FlexConnect in local switching mode

Key Features Not Supported on Cisco Aironet 1810 OEAP and 1810W Series APs

Table 13: Key Features Not Supported on Cisco Aironet 1810 OEAP and 1810W Series APs

Operational Modes	• Monitor Mode • Mobility Express

Key Features Not Supported on Cisco Aironet 1830 and 1850 Series and 1815i APs

Table 14: Key Features Not Supported on Cisco Aironet 1830 and 1850 Series and 1815i APs

Operational Modes	• Monitor Mode

Key Features Not Supported on 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
- Access point join priority (mesh access points have a fixed priority)
- Location-based services

Caveats

Open Caveats

Table 15: Open Caveats

Caveat ID Number	Description
CSCuw22659	Memory leak with QoS/AVC - PPM_FILTER_API, PPCP_PPM
CSCux23710	The observed behavior of Cisco IW3702 AP LED status is inconsistent in the CCO user guide
CSCux28505	Cisco 8510 WLC stopped working with high traffic during boot
CSCuy66962	Roaming fails with WLC not sending "Sent 1x initiate message"
CSCuz11374	Cisco WLC selects an incorrect DHCP relay even though it is configured on an interface
CSCuz18799	Cisco 3802 AP sends VHT SGI frames to STA that does not support SGI
CSCuz27736	Cisco 3800 AP on Flex-AP deauthenticates after FT roam (Freq- 3-4%)
CSCuz29774	Cisco 1852 APs lose connectivity to the ME controller when AVC is enabled
CSCuz33090	Cisco 3802 AP - antennas supported is always 4 in VHT Capabilities IE
CSCuz65017	Cisco 3800 AP not updating HT Op Mode bits in presence of legacy AP
CSCuz68479	Cisco 3800 AP: not reassembling wireless fragmented frames
CSCuz78490	DHCP: Usage indicator will not show 100% usage even if all IP's are in use

Caveat ID Number	Description
CSCva07048	WLC DP stopped working wqe stuck
CSCva07307	Voice tagged frames drop at AP radio after upgrade to 8.2 and later release
CSCva16449	Cisco 1552 APs not showing temperature on Cisco WLC on 8.2 release
CSCva25999	Rate limit not followed as per QoS Role defined for Guest user
CSCva29463	Cisco 3800 AP: WLAN client fails >=1500 bytes ICMP traffic in standalone mode
CSCva29554	FlexConnect AAA overridden ACL is not plumbed in the Cisco WLC
CSCva51719	QoS profile and priority mismatch in 1850 as primary AP in Cisco Mobility Express setup
CSCva53980	Issue in CleanAir when client serving band is 5 GHz
CSCva55165	IPv6 MLD from PMIPv6 client show client MAC on Layer 3 and Layer 2 switch
CSCva65380	Multicast mobility mode config enable with IP is not getting preserved
CSCva71002	WLC GUI client filter fails with spaces used in the client name
CSCva72044	Cisco 1572 mesh AP with no distance command implementation
CSCvb19483	Cisco 1852 ME unable to download login-banner
CSCvb72389	CWA: Redirect traffic from client goes through CAPWAP tunnel instead of VxLan
CSCvb89227	For last AP connection failure reason: messages not getting properly on join statistics
CSCvc03888	Cisco 5520 and 8540 controller on 8.4: T'put Performace Degradation for 102(small) pkt size
CSCvc25658	Cisco 2800,3800 padding from small CAPWAP fragments transmitted over the air to clients
CSCvc50667	New Mobility tunnel needs to be plumbed with DTLS version 1.0
CSCvc80047	Cisco AP reloads unexpectedly- dpaa_get_pool_id_from_ios_pool_ptr
CSCvc94490	URL filtering traffic is not getting blocked inside EOGRE tunnel
CSCvd31160	Cisco WLC shows cleared NAC clients with quarantine IP addresses
CSCve81183	Cisco 2800, 3800 APs - Rx hang in 8.2.154.17 release
CSCvf27533	Cisco 2800, 3800 AP in a constant reboot loop when wIPS sub-mode is enabled
CSCvf74377	AP3800 Sniffer mode: 802.11 acks, RTS, CTS, QoS Null packets do not get captured
CSCvf89335	Cisco 3700 AP stopped working with memory allocation failure CAPWAP

Caveat ID Number	Description
CSCvg44450	Cisco 2800,3800,1560 AP cannot forward packets downstream; 'Failed to get ARP entry for WLC'
CSCvg82156	Cisco 2802E AP: Radio1 reloads unexpectedly
CSCvg87547	AP: Client disconnected due to idle timeout wrongly kicking in when client is going to power save
CSCvg91770	Cisco 1810W AP stops to send data frame intermittently
CSCvg98078	AP with Flex AVC visibility Tx frames with sequence jumps causing client to not process packets
CSCvh21953	Cisco Aironet 1560, 1800, 2800 and 3800 Series Access Point Denial of Service Vulnerability
CSCvh30447	MAP changes its statically assigned non-backhaul channel after it rejoins RAP
CSCvh54235	Cisco 3800 AP FW stopped working on Radio 0
CSCvh67548	Cisco 1600AP sending de-auth frame with reason code 7 to Random MAC Address XX:XX:00:00:00:00
CSCvh67549	Cisco 8540 WLC Data Plane reloads unexpectedly on __udp_input
CSCvh81391	Cisco 2800, 3800 AP add CAPWAP ap-primed-join-timeout logic
CSCvh87451	Cisco 1832 AP Rx not working with AP not responding to probe requests
CSCvh89438	Cisco 8510 WLC SNMP Traps for duplicate IP reported with IP address inversely
CSCvh91290	Cisco Wave 2 APs need to send XID broadcast on client association for FlexConnect local switching
CSCvh97977	WLC Local Policy - Client Local Profiling assigns wrong Interface to Client
CSCvh98496	Fan failure errors seen after upgrade to 8.3.133.10 release
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
CSCvi02980	Cisco Controller becomes inaccessible with client rate limiting
CSCvi03824	Cisco Wave 2 APs reloads unexpectedly due to watchdog reset(capwapd) when AVC debug is enabled
CSCvi07609	Cisco 5520 WLC experiences fatal dataplane reloads unexpectedly at broffu_fp_dapi_cmd.c:4588
CSCvi09095	Radio Reset Tx jammed seen on both 8.3 and 8.5 releases
CSCvi09424	Layer 3 Roam fails back to L2 Anchor with MAC Filtering MAB

Caveat ID Number	Description
CSCvi10888	Cisco AP intermittently stops transmitting Beacon for 12 and 85 seconds
CSCvi42632	AP generating 'hostapd' core files, does not respond to EAPOL
CSCvi49114	Cisco 3700 AP: memory allocation issue on Cisco Wave 1 AP
CSCvi49590	Bad phase calibration values in Triggerfish EEPROM
CSCvi51372	Client unable to reach RUN state on anchor WLC with 802.1x + ISE NAC
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
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
CSCvi77457	Cisco 5520 WLC experiences fatal dataplane crash at broffu_fp_dapi_cmd.c:4588 -- Invalid Timer Wheel
CSCvi84734	Cisco 702w AP: client intermittently cannot connect- decrypt errors
CSCvi85464	AP specific configuration lost post ap reload - wlan-acl mappings and policies lost
CSCvi91017	The FlexConnect groups are missing in backup configuration file
CSCvi98357	Cisco AP1815I : reloads unexpectedly due to 'watchdog reset(sync_log)'
CSCvi98368	AP 1815I stops working due to kernel panic in radio driver, PC is at ieee80211_node_unauthorize+0x48
CSCvi98415	AP 1815I stopped working due to kernel panic during radio reset in 8.3.140.0
CSCvj04401	Client remains stuck in DHCP-REQD state on Anchor side unless ISE NAC is disabled on the anchor side
CSCvj27642	8540 WLC running version 8.3.135.0 reloads unexpectedly due to pmalloc detected memory corruption
CSCvj29270	Flex AP's WLAN-VLAN mapping mismatch in multiple controller scenarios
CSCvj32964	WGB is only allowing 8 MAC addresses pass traffic using 3802 AP [as CAPWAP AP and 3702 AP as WGB]
CSCvj36853	AP name corruption after upgrade
CSCvj41040	Cisco 1800 APs in Cisco FlexConnect mode, fail FT roam
CSCvj48316	AP3700: process "QoS stats process" causes unexpected reloads
CSCvj48364	Cisco Controller is generating client traps without a session-id
CSCvj62672	Cisco controller sending wrong NAS ID when AAA override is enabled

Caveat ID Number	Description
CSCvj72136	Cisco 2800, 3800 APs loose its ability to reach the default gateway
CSCvj77078	Cisco controller unexpectedly reboots on Dot1x_NW_MsgTask_1
CSCvk24360	Cisco controller's power supply status is incorrect when there is no power supply
CSCvk41068	Advance IPMI is not set and causing fan noise
CSCvk65908	Cisco 5520 controller reloads unexpectedly with taskname emWeb when checking "show tech-support"
CSCvk70860	WLC AVC Profile application rate limit causes all traffic drop
CSCvk79597	Frequent DFS detection
CSCvm00214	Cisco WiSM2 memory leak due to hotspot_anqp
CSCvm18273	Handling of Cisco 702W AP reloads due to memory limitation from 8.5release and other memleak fixes
CSCvm34641	Cisco controller is sending packets out to Gateway with DF =1 when inside header is set DF =0 -EoGRE
CSCvm48446	Unexpected reload in "Dot1x_NW_MsgTask_*"
CSCvm53457	Cisco AP reloads unexpectedly with Memory ALLOC Failed - LWAPP DHCP REAP process is bloated
CSCvm58235	Cisco 2802E AP with DART connector - custom RF profile not always applied properly to XOR
CSCvm65360	Cisco controller redirects to internal webauth login page after successful external webauth login
CSCvm80592	Cisco 2800 AP reloads unexpectedly with ERROR TAMD device 'ap-tam' heartbeat failure
CSCvn03560	Decrypt errors seen on Cisco 702 AP
CSCvn62176	Cisco 3802 series APs unable to associate clients when using UNII-1 Channels
CSCvn74026	1832 AP stops to send data frame intermittently even after upgrading to fixed version 8.3.143.4
CSCvo20540	Wave 2 AP rejecting association request on 5-GHz if it does not include 36Mbps

Resolved Caveats

Table 16: Resolved Caveats

Caveat ID Number	Description
CSCvf28459	Write of the Private File nvram:/lwapp_ap.cfg Failed on compare RCA needed (try = 1)
CSCvh56836	SFTP mode is not working
CSCvh65876	Cisco Wireless LAN Controller Software GUI Privilege Escalation Vulnerability
CSCvh82606	LSC configurations are not persistent after certificate installation followed by system reboot
CSCvi02106	CDP-4-DUPLEX_MISMATCH log is seen when 2800/3800 & 1560 APs are connected to a Cisco Switch
CSCvi80205	[AP1552] ETSI domain Compliance and Throughput testing
CSCvi97023	Cisco Wireless LAN Controller Cross-Site Scripting Vulnerability
CSCvj18900	TLS1.0 remains active on 85MR3
CSCvj70790	Cisco Aironet 1800, 2800, and 3800 Series AP ARP Request Handling DoS Vulnerability
CSCvj79479	Cisco 8500 Wireless LAN Controller web interface unvalidated web page redirect vulnerability
CSCvj95336	Cisco Wireless LAN Controller Software Information Disclosure Vulnerability
CSCvk15043	Wave 1 APs - AP radio FW image install failure in the bootup loop
CSCvk15068	Cisco Wave 1 APs recovery logic for failure on primary image
CSCvk26732	New Flash recovery logic
CSCvk39545	Cisco Wireless LAN Controller Software Information Disclosure Vulnerability
CSCvm15469	Evaluation of click-ap for CVE-2018-5391 (FragmentSmack)
CSCvm33617	Configuration file should not be modified due to low flash memory
CSCvn45914	[AP802] ETSI domain Compliance and Throughput testing
CSCvn80172	CIAM Alert: Multiple Vulnerabilities in curl

Table 17: Cisco Security Advisories Caveats

Caveat ID Number	Description
CSCvb35683	Cisco Wireless LAN Controller Software GUI Configuration Denial of Service Vulnerabilities

Caveat ID Number	Description
CSCvd64417	Cisco Wireless LAN Controller Software GUI Configuration Denial of Service Vulnerabilities
CSCve58704	Cisco Wireless LAN Controller Software GUI Configuration Denial of Service Vulnerabilities
CSCve68131	Cisco Wireless LAN Controller Software GUI Configuration Denial of Service Vulnerabilities
CSCve82306	Cisco Wireless LAN Controller Software GUI Configuration Denial of Service Vulnerabilities
CSCve88013	Cisco Wireless LAN Controller Software GUI Configuration Denial of Service Vulnerabilities
CSCve90361	Cisco Wireless LAN Controller Software GUI Configuration Denial of Service Vulnerabilities
CSCve90365	Cisco Wireless LAN Controller Software GUI Configuration Denial of Service Vulnerabilities
CSCve91536	Cisco Wireless LAN Controller Software GUI Configuration Denial of Service Vulnerabilities
CSCve91601	Cisco Wireless LAN Controller Software GUI Configuration Denial of Service Vulnerabilities
CSCve92619	Cisco Wireless LAN Controller Software GUI Configuration Denial of Service Vulnerabilities
CSCve93039	Cisco Wireless LAN Controller Software GUI Configuration Denial of Service Vulnerabilities
CSCve93215	Cisco Wireless LAN Controller Software GUI Configuration Denial of Service Vulnerabilities
CSCve93547	Cisco Wireless LAN Controller Software GUI Configuration Denial of Service Vulnerabilities
CSCve94030	Cisco Wireless LAN Controller Software GUI Configuration Denial of Service Vulnerabilities
CSCve94052	Cisco Wireless LAN Controller Software GUI Configuration Denial of Service Vulnerabilities
CSCve94683	Cisco Wireless LAN Controller Software GUI Configuration Denial of Service Vulnerabilities
CSCve94821	Cisco Wireless LAN Controller Software GUI Configuration Denial of Service Vulnerabilities
CSCve94942	Cisco Wireless LAN Controller Software GUI Configuration Denial of Service Vulnerabilities

Caveat ID Number	Description
CSCve95046	Cisco Wireless LAN Controller Software GUI Configuration Denial of Service Vulnerabilities
CSCve95104	Cisco Wireless LAN Controller Software GUI Configuration Denial of Service Vulnerabilities
CSCve95848	Cisco Wireless LAN Controller Software GUI Configuration Denial of Service Vulnerabilities
CSCve95866	Cisco Wireless LAN Controller Software GUI Configuration Denial of Service Vulnerabilities
CSCve95898	Cisco Wireless LAN Controller Software GUI Configuration Denial of Service Vulnerabilities
CSCve95987	Cisco Wireless LAN Controller Software GUI Configuration Denial of Service Vulnerabilities
CSCve96534	Cisco Wireless LAN Controller Software GUI Configuration Denial of Service Vulnerabilities
CSCve96615	Cisco Wireless LAN Controller Software GUI Configuration Denial of Service Vulnerabilities
CSCve96858	Cisco Wireless LAN Controller Software GUI Configuration Denial of Service Vulnerabilities
CSCve96879	Cisco Wireless LAN Controller Software GUI Configuration Denial of Service Vulnerabilities
CSCve97734	Cisco Wireless LAN Controller Software GUI Configuration Denial of Service Vulnerabilities
CSCve97771	Cisco Wireless LAN Controller Software GUI Configuration Denial of Service Vulnerabilities
CSCve98357	Cisco Wireless LAN Controller Software GUI Configuration Denial of Service Vulnerabilities
CSCve98393	Cisco Wireless LAN Controller Software GUI Configuration Denial of Service Vulnerabilities
CSCve98434	Cisco Wireless LAN Controller Software GUI Configuration Denial of Service Vulnerabilities
CSCve99020	Cisco Wireless LAN Controller Software GUI Configuration Denial of Service Vulnerabilities
CSCve99072	Cisco Wireless LAN Controller Software GUI Configuration Denial of Service Vulnerabilities
CSCve99744	Cisco Wireless LAN Controller Software GUI Configuration Denial of Service Vulnerabilities

Caveat ID Number	Description
CSCvf01690	Cisco Wireless LAN Controller Software GUI Configuration Denial of Service Vulnerabilities
CSCvf02412	Cisco Wireless LAN Controller Software GUI Configuration Denial of Service Vulnerabilities
CSCvf08015	Cisco Wireless LAN Controller Software GUI Configuration Denial of Service Vulnerabilities
CSCvf15789	Cisco Wireless LAN Controller Software GUI Configuration Denial of Service Vulnerabilities
CSCvf16237	Cisco Wireless LAN Controller Software GUI Configuration Denial of Service Vulnerabilities
CSCvf16322	Cisco Wireless LAN Controller Software GUI Configuration Denial of Service Vulnerabilities
CSCvf16358	Cisco Wireless LAN Controller Software GUI Configuration Denial of Service Vulnerabilities
CSCvf27133	Cisco Wireless LAN Controller Software GUI Configuration Denial of Service Vulnerabilities
CSCvf27342	Cisco Wireless LAN Controller Software GUI Configuration Denial of Service Vulnerabilities
CSCvf42722	Cisco Wireless LAN Controller Software GUI Configuration Denial of Service Vulnerabilities
CSCvf47085	Cisco Wireless LAN Controller Software GUI Configuration Denial of Service Vulnerabilities
CSCvf47220	Cisco Wireless LAN Controller Software GUI Configuration Denial of Service Vulnerabilities
CSCvf47430	Cisco Wireless LAN Controller Software GUI Configuration Denial of Service Vulnerabilities
CSCvf47934	Cisco Wireless LAN Controller Software GUI Configuration Denial of Service Vulnerabilities
CSCvf54469	Cisco Wireless LAN Controller Software GUI Configuration Denial of Service Vulnerabilities
CSCvf57639	Cisco Wireless LAN Controller Software GUI Configuration Denial of Service Vulnerabilities
CSCvf58849	Cisco Wireless LAN Controller Software GUI Configuration Denial of Service Vulnerabilities
CSCvf59210	Cisco Wireless LAN Controller Software GUI Configuration Denial of Service Vulnerabilities

Caveat ID Number	Description
CSCvf59796	Cisco Wireless LAN Controller Software GUI Configuration Denial of Service Vulnerabilities
CSCvf59799	Cisco Wireless LAN Controller Software GUI Configuration Denial of Service Vulnerabilities
CSCvh91032	Cisco Wireless LAN Controller IAPP Message Handling Denial of Service Vulnerability
CSCvh96364	Cisco Wireless LAN Controller IAPP Message Handling Denial of Service Vulnerability
CSCvi89027	Cisco Wireless LAN Controller IAPP Message Handling Denial of Service Vulnerability
CSCvj06910	Cisco Wireless LAN Controller Cross Site Request Forgery Vulnerability
CSCvj07995	Cisco Wireless LAN Controller Locally Significant Certificate Denial of Service Vulnerability
CSCvk42764	Cisco Aironet Series Access Point Development Shell Access Vulnerability
CSCvk66471	Cisco Aironet Series Access Point Command Injection Vulnerability
CSCvk79421	Cisco Wireless LAN Controller SSH Unauthorized Access Vulnerability

Cisco Mobility Express Solution Release Notes

Overview

Note The Cisco Mobility Express wireless network solution is available starting from Cisco Wireless Release 8.1.122.0.

The Cisco Mobility Express wireless network solution provides a wireless controller functionality bundled into the Cisco Aironet 1560, 1815, 1830, 1850, 2800, and 3800 Series access points.

In the Cisco Mobility Express wireless network solution, one AP, which runs the Cisco Mobility Express wireless controller, is designated as the primary AP. Other access points, referred to as Subordinate APs, associate to this primary AP.

The primary AP operates as a wireless controller, to manage and control the subordinate APs. It also operates as an AP to serve clients. The subordinate APs behave as normal lightweight APs to serve clients.

For more information about the solution, including the setup and configuration, see the *Cisco Mobility Express User Guide for Release 8.3*, at http://www.cisco.com/c/en/us/td/docs/wireless/access_point/mob_exp/83/user_guide/b_ME_User_Guide_83.html

Supported Cisco Aironet Access Points

APs Supported as Primary (Support Integrated Wireless Controller Capability)	APs Supported as Subordinate
Cisco Aironet 1560 Series Cisco Aironet 1815i Access Point Cisco Aironet 1830 Series Cisco Aironet 1850 Series Cisco Aironet 2800 Series Cisco Aironet 3800 Series	In addition to the following, all the APs that are supported as primary APs are also supported as subordinate APs: Cisco Aironet 700i Series Cisco Aironet 700w Series Cisco Aironet 1600 Series Cisco Aironet 1700 Series Cisco Aironet 1810W Series Cisco Aironet 2600 Series Cisco Aironet 2700 Series Cisco Aironet 3500 Series Cisco Aironet 3600 Series Cisco Aironet 3700 Series

Cisco Mobility Express Features

There are no new features and functionalities introduced in this release.

The following are existing features, with continued support in the current release:

Note Even if the Cisco AP is 802.3ad (LACP)-compliant, link aggregation groups (LAG) are not supported on the AP while it has a Cisco Mobility Express software image.

- Support for the following access points:
  - Cisco Aironet 1560 Series
  - Cisco Aironet 1815 Series
  - Cisco Aironet 2800 Series
  - Cisco Aironet 3800 Series
- Simple Network Management Protocol (SNMP) Version 3 polling; configurable through the GUI.
- Support for the Flexible Radio Assignment (FRA) functionality for the radio in slot 0 on Cisco Aironet 3800 Series access points. FRA automatically detects when a high number of devices are connected to a network, and changes the dual radios in an access point from 2.4GHz/5GHz to 5GHz/5GHz to serve more clients.
- Improvements in software update and access point image management with direct download from Cisco.com.

- Integration with Cisco CMX Cloud for both guest services and presence analytics. This is enabled by the integrated cloud connector on the Cisco Mobility Express controller for seamless integration and easier provisioning.
- Localization to Japanese and Korean for the Cisco Mobility Express controller GUI.
- Setting up and managing an internal DHCP server through the GUI.
- Importing a customized guest login page.
- Forced failover to a specified AP as primary.
- Scalability:
  - Up to 25 APs
  - Up to 16 WLANs
  - Up to 100 rogue APs
  - Up to 1000 rogue clients
- License—Does not require any licenses (Cisco Right-To-Use License or Swift) for APs.
- Operation— The primary AP can concurrently function as controller (to manage APs) and as an AP (to serve clients).
- GUI and CLI-based initial configuration wizards.
- Up to three Network Time Protocol (NTP) servers, with support for FQDN names.
- Simple Network Management Protocol (SNMP) Version 3 polling, configurable through the CLI.
- IEEE 802.11r with support for Over-the-Air Fast BSS transition method, Over-the-DS Fast BSS transition method, and Fast Transition PSK authentication. Fast BSS transition methods are supported via CLI only.
- CCKM, supported via CLI only.
- Client ping test
- Changing the country code on the controller and APs on the network, via the controller GUI.
- Syslog messaging towards external server.
- Software image download using TFTP and HTTP.
- Priming at distribution site.
- Default Service Set Identifier (SSID), set from factory. Available for initial provisioning only.
- Management through the web interface Monitoring Dashboard.
- Cisco Wireless Controller Best Practices.
- Quality of Service (QoS).
- Multicast with default settings.
- Application Visibility and Control (AVC)—Limited HTTP, with only Application Visibility and not Control. Deep Packet inspection with 1,500+ signatures.

- WLAN access control lists (ACLs).
- Roaming—Layer 2 roaming without mobility groups.
- IPv6—For client bridging only.
- High Density Experience (HDX)—Supported when managing APs that support HDX.
- Radio Resource Management (RRM)—Supported within AP group only.
- WPA2 Security.
- WLAN-VLAN mapping.
- Guest WLAN login with Web Authorization.
- Local EAP Authentication (local RADIUS server).
- Local profile.
- Network Time Protocol (NTP) Server.
- Cisco Discovery Protocol (CDP) and Link Layer Discovery Protocol (LLDP).
- Clean Air.
- Simple Network Management Protocol—SNMPv1, by default, and SNMPv2c.
- Management—SSH, Telnet, Admin users.
- Reset to factory defaults.
- Serviceability—Core file and core options, Logging and syslog.
- Cisco Prime Infrastructure.
- BYOD—Onboarding only.
- UX regulatory domain.
- Authentication, Authorization, Accounting (AAA) Override.
- IEEE 802.11k
- IEEE 802.11r
- Supported—Over-the-Air Fast BSS transition method
- Not Supported—Over-the-DS Fast BSS transition and Fast Transition PSK authentication
- Passive Client
- Voice with Call Admission Control (CAC), with Traffic Specification (TSpec)
- Fast SSID Changing
- Terminal Access Controller Access Control System (TACACS)
- Management over wireless
- High Availability and Redundancy—Built-in redundancy mechanism to self-select a primary AP and to select a new AP as primary in case of a failure. Supported using VRRP.

- Software upgrade with preimage download
- Migration to controller-based deployment.

Compatibility with Other Cisco Wireless Solutions

See the Cisco Wireless Solutions Software Compatibility Matrix, at: http://www.cisco.com/c/en/us/td/docs/wireless/compatibility/matrix/compatibility-matrix.html

Software Release Information

The following table lists the Cisco Mobility Express software for Cisco Wireless 8.3.150.0.

Access Points Supported As Primary	Software to be Used only for Conversion from Unified Wireless Network Lightweight AP Software To Cisco Mobility Express Software	AP Software Image Bundle, to be Used for Software Update, or Supported Access Point Images, or Both
1560	AIR-AP1560-K9-8-3-150-0.tar	AIR-AP1560-K9-ME-8-3-150-0.zip
1815	AIR-AP1815-K9-8-3-150-0.tar	AIR-AP1815-K9-ME-8-3-150-0.zip
1830	AIR-AP1830-K9-8-3-150-0.tar	AIR-AP1830-K9-ME-8-3-150-0.zip
1850	AIR-AP1850-K9-8-3-150-0.tar	AIR-AP1850-K9-ME-8-3-150-0.zip
2800	AIR-AP2800-K9-8-3-150-0.tar	AIR-AP2800-K9-ME-8-3-150-0.zip
3800	AIR-AP3800-K9-8-3-150-0.tar	AIR-AP3800-K9-ME-8-3-150-0.zip

Installing Mobility Express Software

See the “Getting Started” section in the *Mobility Express User Guide* at https://www.cisco.com/c/en/us/td/docs/wireless/access_point/mob_exp/83/user_guide/b_ME_User_Guide_83.html

Caveats

The open caveats applicable to the Cisco Mobility Express solution are listed under the Open Caveats section. All caveats associated with the Cisco Mobility Express solution have *Cisco Mobility Express* specified in the headline.

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