Release Notes for Cisco Wireless Controllers and Lightweight Access Points, Cisco Wireless Release 8.3.130, 8.3.132.0, and 8.3.133.0

First Published: 2017-09-26

Last Modified: 2018-08-30

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
August 23, 2018	Open Caveat—Added CSCvk44249
January 29, 2018	Key Features Not Supported in Cisco Virtual WLC section—Modified information about FlexConnect central switching.
October 30, 2017	Resolved Caveat—Added CSCvg50082
October 27, 2017	What's New In Release 8.3.132.0 section—Added Important Upgrade Information
October 22, 2017	Resolved Caveats—Added CSCvf47808, CSCvg10793, CSCvg18366, CSCvg29019, and CSCvg42682

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 8.3.133.0

Release 8.3.133.0 is a repost of Release 8.3.132.0 to address the caveat listed in the table below. There are no other updates in this release, all resolved and open caveats in addition to the one resolved bug applies to this release.

Table 2: Resolved Caveats in Release 8.3.133.0

Caveat ID Number	Description
CSCvg50082	Prevent unexpected Cisco WLC reload related to CSCvf87731

What's New in Release 8.3.132.0

Release 8.3.132.0 is a repost of Release 8.3.130.0 to address the caveats listed in the table below. There are no other updates in this release, all resolved and open caveats in addition to the five resolved bugs apply to this release.

Table 3: Resolved Caveats in Release 8.3.132.0

Caveat ID Number	Description
CSCvf47808	Cisco Wave 1 APs: Key Reinstallation attacks against WPA protocol
CSCvg10793	Cisco Wave 2 APs: Key Reinstallation attacks against WPA protocol
CSCvg18366	hostapd deleting client entry when client goes to FWD state in WCPD
CSCvg29019	AP18xx : Bypassed scan in returning to DFS channel after blacklist timeout
CSCvg42682	Cisco Wave 1 APs: Additional fix for Key Reinstallation attacks against WPA protocol

Important Upgrade Information

The releases 8.3.130.0 (deferred release) and 8.3.132.0 are affected by the caveat: CSCvf87731. This could cause the Cisco WLC to unexpectedly reload, triggered by a timing issue during the processing of multiple

join requests from the same AP. This issue could be more prevalent in scenarios of networks with packet drops or reordering.

Therefore, we recommend that you do not upgrade to Release 8.3.132.0, but instead upgrade to a newer release to be made available by October 30, 2017.

What's New in Release 8.3.130.0

Multi-user MIMO Enhancements for Aironet 2800 and Aironet 3800 Series APs

In this release, the Multi-user MIMO (MU-MIMO) feature on the Cisco 2800 and 3800 APs is enhanced to provide improved stability and higher performance gain. It enables concurrent transmission in the downstream direction to multiple clients, however, the client device must support this feature.

There are no new features in this release. This release addresses critical issues with the controller software. For more information, see the "Caveats" section.

Software Release Types and Recommendations

Table 4: 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:

https://www.cisco.com/c/en/us/products/collateral/wireless/8500-series-wireless-controllers/bulletin-c25-738147.html

Upgrading the Cisco WLC Software Release

Guidelines and Limitations

- 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 8.3.13x.0 to a 7.x release, the trap configuration is lost and must be reconfigured.
- If you downgrade from Release 8.3.13x.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 8.3.133.0 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 8.3.13x.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 8.3.13x.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 8.3.133.0 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 8.3.133.0. The following table shows the upgrade path that you must follow before downloading Release 8.3.133.0.

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:

http://www.cisco.com/c/en/us/products/collateral/wireless/8500-series-wireless-controllers/bulletin-c25-730741.html

Table 5: Upgrade Path to Cisco WLC Software Release 8.3.133.0

Current Software Release	Upgrade Path to 8.3.133.0 Software
8.0.x	You can upgrade directly to 8.3.133.0.
8.2.x	You can upgrade directly to 8.3.133.0. For more information about special upgrade instructions for Cisco 2504 WLC, 5508 WLC, and WiSM2, see the "Changes in Images and Installation Procedure for Cisco 2504 WLC, Cisco 5508 WLC, and Cisco WiSM2" section.
8.3.x	You can upgrade directly to 8.3.133.0.

- 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 8.3.133.0. 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 8.3.133.0 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 5500 Series 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 8.3.133.0 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 WLC, Cisco 5508 WLC, and Cisco WiSM2

Due to an increase in the size of the Release 8.3.133.0 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 8.3.133.0 for the applicable Cisco WLC platforms:

Table 6: 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-K9-8-3-133-0.aes	AIR-CT2500-AP_BUNDLE-K9-8-3-133-0.aes
Cisco 5508 WLC	AIR-CT5500-K9-8-3-133-0.aes AIR-CT5500-LDPE-K9-8-3-133-0.aes	AIR-CT5500-AP_BUNDLE-K9-8-3-133-0.aes AIR-CT5500-LDPE-AP_BUNDLE-K9-8-3-133-0.aes
Cisco WiSM2	AIR-WISM2-K9-8-3-133-0.aes	AIR-WISM2-AP_BUNDLE-K9-8-3-133-0.aes

[1] 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 8.3.133.0 (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 8.3.133.0 software:

a) Browse to https://software.cisco.com/download/navigator.html.
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 Release8.3.133.0, 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 about special upgrade instructions for Cisco 2504 WLC, 5508 WLC, and WiSM2, 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 Release8.3.133.0, 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 about special upgrade instructions for Cisco 2504 WLC, 5508 WLC, and WiSM2, see the "Changes in Images and Installation Procedure for Cisco 2504 WLC, Cisco 5508 WLC, and Cisco WiSM2" section.

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 8.3.133.0 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.

Interoperability With Other Clients in Release 8.3.13x.0

This section describes the interoperability of Cisco WLC Software, Release 8.3.13x.0 with other client devices.

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

Table 7: Test Bed Configuration for Interoperability

Hardware/Software Parameter	Hardware/Software Configuration Type
Release	8.3.13x.0
Cisco WLC	Cisco 55xx Series Wireless Controller
Access points	AIR-CAP3802E-B-K9, AIR-AP1852E-B-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)
RADIUS	ISE 2.2
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
Acer Aspire E15 E5-573-3870	11.0.0.492
Dell Inspiron 13-5368	18.40.0.12
Dell Latitude	18.33.3.2
Dell Latitude	15.18.0.1
Dell Latitude E5430	18.33.6.2
Dell Latitude E5430	15.1.1.1
Dell Latitude E5430	15.17.0.1
Dell Latitude E5450	19.10.1.2
Dell Latitude E5540	17.13.2.2
Dell Latitude E6420	15.16.0.2
Dell Latitude E6430	15.11.0.7
Dell Latitude E6430	17.15.0.5
Dell Latitude E6430	15.9.2.1
Dell Latitude E7450	6.30.223.262
Dell Latitude E7450	6.30.223.245
Dell Latitude E7450	19.10.1.2
Dell XPS	18.40.0.9
Dell XPS 139350	1.555.0.0
Dell XPS 13 9350	1.566.0.0
Fujitsu LifeBook E556	19.20.0.6
Lenovo ThinkPad Yoga 460	19.1.0.4
Lenovo ThinkPad Yoga 460	19.1.0.4
MacBook	OS X Beta (16A202w)
MacBook (Retina, 12-inch, Early 2015)	OS X El Capitan (10.11.5)
MacBook Air	OS X 10.9.5 (13F34)

Client Name	Version Details
MacBook Air (11-inch, Early 2015)	macOS Sierra (10.12.2)
MacBook Air (11-inch, Early 2015)	OS X El Capitan (10.11.6)
MacBook Air (11-inch, Early 2015)	macOS Sierra (10.12.2)
MacBook Air (11-inch, Mid 2013)	OS X Yosemite (10.10.5)
MacBook Air (11-inch, Mid 2013)	macOS Sierra (10.12.3)
Macbook Pro	MacOs 10.12.4
MacBook Pro (Retina, 13-inch, Early 2015)	OS X Yosemite (10.10.5)
MacBook Pro (Retina, 13-inch, Late 2013)	macOS Sierra (10.12.2)
Macbook Pro 13 inch(mid 2009)	OSX 10.8.5
Toshiba Satellite NB15t-A	16.1.5.2
Windows Surface Pro 4	15.68.9040.67

Table 9: Tablets

Client Name	Version Details
Amazon Kindle Fire Hd 8	Fire OS 5.4.0.0
Apple iPad	9.3.1(13E238)
Apple iPad	8.3(12F69)
Apple iPad 2	9.3.1 (13E238)
Apple iPad Air	10.1.1(14B100)
Apple iPad Air	9.3.1
Apple iPad Air 2	10
Apple iPad Air 2	8.4.1(12H143)
Apple iPad Air 2	9.3.1(13E238
Apple iPad Air 2	9.2(13C75)
Apple iPad Mini	9.3.5(13G36)
Apple iPad Mini 2	10.3.1
Apple iPad Mini 2	9.3.1
Apple iPad Mini 4	10.0(14A5261v)

Client Name	Version Details
Apple iPad Pro 12.9"	10.0(14A5345a)
Apple iPad Pro 12.9"	10.3.1
Samsung Galaxy Tab Pro 10.1	4.4.2

Table 10: Mobile Devices

Client Name	Version Details
Apple iPhone 4S	iOS 9.3.2(13F69)
Apple iPhone 4S	iOS 8.0 (12A4265u)
Apple iPhone 5	iOS 8.1(12B411)
Apple iPhone 5	iOS 10.2.1(14D27)
Apple iPhone 5c	iOS 10.2.1(14D27)
Apple iPhone 5c	iOS 9.3.1(13E238)
Apple iPhone 5c	iOS 9.3.2(13F69)
Apple iPhone 5S	iOS 9.3.2(13F69)
Apple iPhone 6 Plus	iOS 10.3(14E5260b)
Apple iPhone 6 Plus	iOS 10.2.1
Apple iPhone 7	iOS 10.2.1(14D27)
Apple iPhone SE	iOS 9.3.3(13G34)
Apple iPhone SE	iOS 9.3.3(13G34)
Apple iPod Touch	iOS 8.4.1(12H318)
Cisco 7925G-EX	CP7925G-1.4.8.4.LOADS
Cisco 7926G	1.4.8.4.LOADS
Cisco 8821	11.0.3SR4.3
Cisco 8861	12.0.1.11
Cisco 8865	12.0.1.11
Cisco DX650	10.2.5.215
Cisco DX70	• Android—10.2.5.215 • CE—9.1.4

Client Name	Version Details
Cisco DX80	• Android—10.2.5.215 • CE—9.1.4
Galaxy Nexus	Android 4.0.2
Galaxy Note4 Edge	Android 5.0.1
Google Nexus 5X	Android 6.0.1
Google Nexus 5X	Android 6.0.1
Google Pixel C	Android 7.1.1
LG G4	Android 5.1
MC40N0	Android 4.4.4
MC70	Android 05.01.0476
MC9090-C030	Android 5.1.478 (Build 15706.3.5.2)
MC92	Android 4.4.4
Motorola MC 75A	OS 5.2.23137 (Build 23137.5.3.9)
Motorola MC 75A	OS 5.2.23137 (Build 23137.5.3.9)
Moto X 2nd Generation	Android 5.0
Nokia Lumia 1520	Windows Phone 8.10.14219.341
Nokia Lumia 925.5	Windows Phone 1.10.1.17
OnePlus One	Android 4.3
OnePlus Three	Android 6.0.1
Samsung Galaxy Mega GT-i9200	Android 4.4.2
Samsung S3	Android 4.3
Samsung S4	Android 4.2.2
Samsung S4	Android 5.0.1
Samsung S5	Android 4.4.2
Samsung S6	Android 6.0.1
Samsung S6	Android 5.1.1
Samsung S7	Android 6.0.1

Client Name	Version Details
Samsung S8	Android 7.0
Sony Xperia Z Uktra	Android 4.3
Xiaomi Mi 4i	Android 5.0.2 LRX22G
Xiaomi Mi 4w	Android 4.4.2
Xiaomi Mi Note 2	Android 4.4.4 KTU84P

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 11: 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 12: 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 13: 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 14: Open Caveats for Release 8.3.13x.0

Caveat ID Number	Description
CSCvd93634	Cisco 2700 series AP radio resets reason code 37 RADIO_RC_IDB_RESET
CSCve56562	Cisco 1800 AP running 8.3MR2: IP Phone disassociates while making voice calls
CSCve59671	Cisco WLC and ME: RADIUS fail-over does not work when retransmit timeout is not set to default value
CSCve78449	Cisco 3700 AP: radio d1 reset: Tx jammed
CSCvf05776	Target assert XXXXXXXX WAITING FOR STOP EVENT on Cisco 1810 AP
CSCvf08272	Black-list timer is showing as "blacklist due to be cleared" but still black-list timer remaining
CSCvf22867	The Wireless LAN Controller stopped working while fetching the WLAN LDAP entry
CSCvf25062	Cisco 3802AP on 8.3.124.17 release [cmd mismatch] wifi0: Host Cmd:0x9201 F/W Cmd:0x8001 Last:0x801d
CSCvf33154	Wireless to Wireless multicast failure on Cisco 2800, 3800 APs with WPA-PSK-TKIP
CSCvf38379	Bad 68xx NICs in Cisco 8540, 5520 WLCs - "System could not find 68xx Nic Card"
CSCvf41510	Cisco WLC reloads unexpectedly due to SXP CORE when a new download was initiated

Caveat ID Number	Description
CSCvf44061	SNMP get or walk on device for bsnAPBridgingSupport returns ENABLE for Cisco 2800, 3800 APs
CSCvf44583	Cisco 2800, 3800 APs transmitting at MCS/802.11n rates to clients with WMM disabled
CSCvf47545	WiSM2 is not forwarding wireless originating RTP traffic downstream if CAC is enabled
CSCvf47830	In a Anchor or foreign guest Network the L3 security fails
CSCvf53126	Cisco 3700 AP reloads unexpectedly on Pid 104: Process "LWAPP Rogue Monitoring process"
CSCvf54541	LWAPP-3-INVALID_AID2 being generated on HA standby controller and sent to syslog server
CSCvf55570	Clients unable to connect when CCKM and FT802.1X are enabled together
CSCvf55741	Cisco 1532 AP cannot use static IP address when configured as mesh AP (MAP)
CSCvf56212	EAPOL Retransmit Issue _ Stuck on M1 after client ack
CSCvf56313	Apple clients when moving from PSK to CWA SSID are not able to connect
CSCvf56556	Guest User role cannot be called properly on the Cisco 2504 WLC platform
CSCvf57360	Cisco Wave2 AP clients constantly deleted with active voice traffic and optimized roaming enabled
CSCvf57588	Cisco Wireless LAN Controller - standby WLC reloads unexpectedly at HA Config Sync Task
CSCvf58977	RTU license count taking over Smart Account count
CSCvf59416	2800,3800 APs adds padding bytes for Assoc req to WLC if assoc request is small packet size -50bytes
CSCvf59685	Cisco 3602i/e AP reloads unexpectedly while failover occurs
CSCvf59701	3800 AP high 802.11a channel and transmit utilization and traffic forward delay with 30+ clients
CSCvf60045	Cisco WLC reloads unexpectedly on "config bleBeaconwhiteList add HomeDepot"
CSCvf62836	Cisco WLC rejecting association with reason Caller id 18 and 20
CSCvf62876	Cisco AP not sending auth-resp to client
CSCvf66859	Cisco 3800 AP beacon stuck due WCP seen in Cisco release 8.3.124.40
CSCvf66863	Clients on PSK+CWA enabled WLAN get redirect loop/10 second re-auth delay with Cisco 3800 AP
CSCvf71026	8.3.124.46 : CAP702I-A - LWAPP KAM-AP process crashed

Caveat ID Number	Description
CSCvf71136	Infra IPv6 AP drops off from the WLC every 4 to 12 hours
CSCvf76274	Cisco APs can no longer join the WLC; CAPWAP-3-DTLS_DB_ERR
CSCvk44249	WLC 5508 - foreign mapping is missing on a WLAN when restoring a backup

Resolved Caveats

Table 15: Release Caveats for Release 8.3.13x.0

Caveat ID Number	Description
CSCuc78713	dWEP client cannot receive broadcast after broadcast key rotation
CSCuh45072	WLC HA TACACS+ authentication authorization sent to different AAA server
CSCuy29182	Peer Upload:No progress status, no error, normal Upload error misleading
CSCuy61155	802.11b inconsistent probe response - band select enabled - 2.4GHz
CSCuy75333	Cisco 2504 WLC config restoration fails due to multicast mode command
CSCuz59858	Cisco 3500AP (SC1), client association failure - R2H Buffer full
CSCuz60117	Foreign WLC allows "local" anchor and guest anchor WLC on same WLAN
CSCuz97296	Cisco 3500AP: Client pak stuck during Payload Encryption
CSCva27419	Channel changed trap with Unknown Radio Type on dual band radio
CSCva37010	Invalid staid XXX received
CSCva50180	AIR-CAP1602I-E-K9 stopped working
CSCva69083	Controller drops NMSP packet from MSE
CSCva87833	Cisco WLC reloads unexpectedly due to Mesh tree update
CSCvb14702	Client does not join if it sends two association packets at the same time
CSCvb57793	AP does not fragment EAP cert correctly
CSCvb71347	WLC multicast config not coherent for code upload or download
CSCvb86237	Cisco 8510 WLC stopped working Task Name: TempStatus
CSCvb90235	Cisco3700 WGB inconsistently facing joining issues because of no probe response by 3600-11ac root AP
CSCvc06547	AP re-transmits packet even though client sends ACK
CSCvc07674	WLC sends ciscoLwappApAssociated trap twice when Cisco 2800 AP joins

Caveat ID Number	Description
CSCvc17678	83MR1: wrong "enable global mDNS snooping" message when clicking apply in AP config edit page
CSCvc18786	WLC stops working during multiple login sessions either with local user or with TACACS+
CSCvc19987	Fresh WLANs not getting broadcast in Cisco 3802 AP
CSCvc24104	Rx-SOP threshold failed to set with Cisco 1852, 1700, 1815, 1830 APs
CSCvc24917	Defect of msglog corresponding to 'AP Message Timeout: Max retransmissions reached on AP ...'
CSCvc28035	clDLApBootTable shows blank when WLC has Cisco 2800I AP connected
CSCvc30828	AP does not allow world mode to be set via GUI on 15.3(3)JD
CSCvc34930	Receiving DELETE_MOBILE, deleting client entry, but not sending any deauth to client
CSCvc35183	CISCO-LWAPP-CLOUD-SERVICES-MIB: Parse errors like bad month and undefined objects
CSCvc37641	Cisco 700 AP does not provide SSH access in wIPS submode for FlexConnect
CSCvc50775	Webauth redirection stop working when AP manager is configured on a dynamic interface
CSCvc51637	802.1x CCKM roams fail on WGB at GTK key rotation
CSCvc51666	Cisco Wave 1 AP transmits on disabled rate 24Mb
CSCvc55430	WLC HA redundancy management interface not reachable for a short time after failover
CSCvc56757	WGB HSR 802.11v neighbor report validation fails when Infrastructure MFP is enabled
CSCvc61795	IP call setup fail after L3 handover happens during call among 1832
CSCvc71012	Error in retrieving number of mDNS policies when given command "show mdns policy service-group"
CSCvc71537	Cisco WLC profiles Cisco Unified Wireless IP Phone 7925G incorrectly
CSCvc72724	Cisco 8510: WLC AP SSO stopped working on portalProcessLogout
CSCvc84637	Cisco 1810w sending invalid AC_NAME when WLC hostname is 31 bytes long
CSCvc85158	AP Group configurations are not retained during upload and download of configurations
CSCvc93377	Tracebacks and MFP queue logs filling up the msglog on WLC
CSCvc94704	Cisco WLC reloads unexpectedly due to task dtlArpTask

Caveat ID Number	Description
CSCvc96076	Cisco WiSM2 HA - standby stopped working with task name spamApTask2 in ideal state
CSCvd09507	Rogue rule substring-ssid turns invalid on WLC when user configured SSID is included in PI template
CSCvd16346	WLC memory corruption occurs when TACACS+ responds with unknown attributes
CSCvd16380	Cisco 3800 AP detecting DFS false triggers
CSCvd23185	WGB wired clients not seen by WLC
CSCvd23301	WLC GUI trapflags for client association with statistics does not display correct configuration
CSCvd23902	Cisco 1532AP: root bridge drops packets from non-root bridge in non-native VLAN
CSCvd26885	Unit of probe suppression hysteresis should be 'dB'
CSCvd28374	Cisco 802AP incorrect base radio MAC assigned not ending with zero results in only one BSSID support
CSCvd30486	Cisco 2800, 3800 APs - radio incorrectly shown as disabled due to PoE
CSCvd31705	AP: Offchannel cleanup in IRQ context can trigger an indefinite loop if sensorD owns the radio
CSCvd35885	Cisco ME2800 reloads unexpectedly with Task Name : capwapSocketTask
CSCvd36190	Cisco 5520 WLC stopped working with taskname haSSOServiceTask6
CSCvd37522	show run-config commands: incorrect index numbers for RADIUS Accounting Servers
CSCvd42669	Cisco 2500 WLC stopped working
CSCvd44909	Client traffic dropped in Anchor foreign AireOS setup with new-mobility if foreign client behind NAT
CSCvd45744	Customer reports that AP reboots after 4 hours while doing site survey
CSCvd56588	In 2800 and 3800 series APs, incorrect RSSI values are displayed when client associates to XOR radio
CSCvd61468	Custom mDNS profile is not saved on the WLAN config after the reboot
CSCvd62184	Cisco 3600 AP: Radio reset with reason reqsema on 8.3MR2
CSCvd62568	XML validation is failing for the AVC profile
CSCvd64819	Cisco Wave 2 AP drops downstream DHCP; kills wcpd (reason: OOM); kernel panic
CSCvd67730	Client fails PSK SSID authentication after primary AP reboot (EAPOL M3 not sent on 4-way handshake)

Caveat ID Number	Description
CSCvd68141	WLC 5520/8540/VM stopped working at task nmspRxServerTask
CSCvd72131	Cisco 7500 WLC in flex-mode stopped working after the SNMPTask Reaper reset
CSCvd74297	Cisco 3800, 2800 APs: Extended core dump CLI is not persistent
CSCvd78452	APs joining the WLC in flex-mode fails to use the flex ACLs in the group policies
CSCvd78495	Failed to get ARP entry due to PHY driver not loaded
CSCvd79511	RADIUS admin mode goes for Disable state in LTB setup
CSCvd80240	FlexConnect AP sends associate response with wrong HT capabilities
CSCvd80508	LAN ports of the 1810W AP are stuck on Admin-Down after modifying RLAN settings
CSCvd86566	Client with incorrect NAI realm gets Access-Accept from RADIUS server
CSCvd90377	WLC is applying wrong ACL to clients when doing CWA
CSCvd94004	Cisco 2800, 3800 APs detecting DFS False triggers
CSCve02210	SNMP OID that is used to monitor WLAN status for FT is returning wrong results
CSCve02585	Webauth login page is not showing up after enabling TLS1.2 on WLC
CSCve02612	HA-Config sync fails on standby when flex AP configurations are modified
CSCve02679	VMs with Bridged Mode NIC on wireless client fails to get IP address
CSCve02689	Silent reboot is observed after the memory usage goes up to 85%
CSCve05507	Retransmit configuration is not reflected when new 1800, 2800, and 3800 series APs join the WLC
CSCve06890	Randomly, Wave 1 APs cannot send NDP Tx on all channels and cant be found as neighbors on nearby APs
CSCve13779	AP2802 Rogue Detection config changed back to "Enabled" after AP reboot
CSCve20123	Corrupt voice packets are observed when a client with an active call does an inter-AP roam
CSCve22001	ME Default value of WLAN parameters is changed after configuration is restored
CSCve24687	Channelization issue occurs when Cisco 3802 AP reverts to channel 36 for 75% of APs at a site
CSCve26935	Cisco 2800, 3800 AP displays low throughput for IPv4 TCP with Windows 10 Creator
CSCve26965	AP2800/3800 Last Reload Reason incorrectly showing as Reload Cmd for AP BootScript
CSCve33506	Client EAP-TLS handshake does not succeed with AP-COS APs

Caveat ID Number	Description
CSCve35431	Downstream QoS 802.11 UP marking does not work for Flex AVC profile
CSCve37579	Cisco 3800 AP stops working due to WIPS kernel panic
CSCve37770	Cisco 5508 WLC stops working when AP's radio CLI command is executed
CSCve42311	Cisco 3800 AP experiences kernel panic due to double free in wireless driver during radio coredump
CSCve45744	Cisco 1850 AP stops working due to memory leak in slab SUnreclaim
CSCve49741	Cisco WLC fails to send SFTP and FTP when using untagged interfaces on different ports
CSCve51301	Cisco 1850, 1830 AP: Stops beaconing
CSCve52807	Standby WiSM2 running 8.5.x reloads unexpectedly with task name 'rsyncmgrIpcqTask'
CSCve61049	Radio resets in Cisco 2700 AP
CSCve63497	Cisco WLC stops working with Task Name emWeb when timer changes
CSCve63755	Cisco WLC running 8.4.100.0: Cisco APs fail to join the WLC if it has LSC enabled on it
CSCve63800	Prime Infrastructure does not show all WLANs when querying MIB bsnAPGroupsVlanMappingSsid
CSCve66007	Cisco 8540 WLC stops working with Task Name emWeb
CSCve66630	Clients cannot connect to Cisco 3800 AP when configuring TKIP only WLAN and PSK with central auth
CSCve68039	Some APs cannot join the WLC because the WLC misrecognizes the number of APs
CSCve68787	Cisco AP is not transmitting out the de-auth frame over the air that was received from the WLC
CSCve75022	Cisco WLC does not apply QoS tag upstream from foreign to anchor
CSCve76202	WLC IPv4 CPU ACL is applied as IPv6 CPU ACL during backup recovery or SSO failover
CSCve81183	Cisco 2800, 3800 - Rx hang in 8.2.154.17 release
CSCve86609	Dynamic interface default gateway must not be configured to "0.0.0.0" in CLI
CSCve89496	AP stops servicing clients
CSCve89758	vWLC code download fails with HTTP mode
CSCve90085	Active WLC in HA pair reloads unexpectedly with task apfRogueTask_0

Caveat ID Number	Description
CSCve92259	Cisco 3800, 2800: APs start beaconing during CAC period if AP boots up in DFS channel
CSCve96310	Cisco WLC installs certificate without a password. However, WebAuthentication fails.
CSCve96480	IOS AP stopped working when it is changed from sensor mode.
CSCve98892	DNS lookup for RADIUS/TACACS+ fails because it is queried before the physical port is up
CSCve99696	CPU ACLs are missing after the WLC reload.
CSCvf02705	The IP-SGT binding is removed from SXP peer after a WLC redundancy switchover
CSCvf03024	The power constraint value is advertised as 3, though it is configured as 0
CSCvf03782	WLC stopped working on emWeb with "ewaFormSubmit_file_upload" in stack
CSCvf04027	Cisco FlexConnect AP failed to parse tlvDecodeApFlexGroupName - flexgroup with spaces
CSCvf05046	Cisoc 1800,2800,3800 APs: correction in unit of antenna gain in show controller output
CSCvf07775	Cisco 2800,3800 AP - Kernel panic FIQ or NMI - Panic in click
CSCvf09441	PMIPv6 MAG is not initialized in the backend
CSCvf09458	Cisco 2800/3800 series XOR radios are not moving to 5GHz or Monitor mode
CSCvf09581	Samsung S8 device cannot stay associated with 802.11v enabled on Wave 2 APs
CSCvf12571	Cisco 2800,3800- CAPWAP tunnel does not restart automatically after configuring primary-base WLCName
CSCvf12728	Cisco 7510 WLC stopped working in SNMP task with no traceback
CSCvf15991	Client data traffic drops when AAA override and link-local-bridging are enabled due to timing issue
CSCvf16629	The OUI string updates properly in Cisco 5508 WLC but disappears after a reboot
CSCvf17085	The radio of Cisco 3800 series AP stopped working after an image reload
CSCvf17488	Cisco WLC reloads unexpectedly with task name: mmMaListen on 8.4.100.0
CSCvf22342	Cisco 3800, 2800 AP running 8.2.154.64 release: TxFSM Stuck
CSCvf23182	Radio parameters become blank after setting channel width to 40-above
CSCvf24515	Inline cleanup for local auth clients on the controller when it gets HREAP_APAUTH_CLIENT_DEL
CSCvf25015	AP on8.2.154.62 reloads unexpectedly on ENTROPY-0-ENTROPY_ERROR:unable to collect sufficient entropy

Caveat ID Number	Description
CSCvf27491	Cisco WLC does not reflect the failure to connect to NA server using wrong RBAC token
CSCvf30451	FRA Last run is showing incorrect time on standby WLC
CSCvf30881	After changing the AP CAPWAP v4 to v6, AP name is changing to default MAC name
CSCvf31894	Backout changes - CSCvc78546 that leads to CSCve20123
CSCvf32021	WLC not marking TID in CAPWAP for TSPEC/TCLASS client after roam it is marked
CSCvf33081	WLC running 8.3.121.0 is not accepting IPs for NetFlow exporter when ending between .224 - .255
CSCvf34744	Correct fix for CSCvc78546 (Zero 801.11e QoS for downstream voice when CAC disabled)
CSCvf38154	Cisco 2800, 3800 APs- Dual DFS Fix that avoids False DFS triggers in HD environment
CSCvf39106	WLC IPv4 CPU ACL mapping is removed after redundancy switchover
CSCvf40306	8.3MR3: COF calculation not getting propagated after FRA run
CSCvf41405	WLC: Need to correct changing MDIE behavior in case of adaptive WLAN
CSCvf41485	WLC reloads unexpectedly when entering 'show run-config' command
CSCvf41726	8.3MR3 "show advanced fra" showing COF/Suggested Mode as None
CSCvf41909	XOR radio is not set to lowest Tx power after moving to 5-GHz band by FRA
CSCvf44254	Call station ID type: ap-mac-ssid-ap-group, returns AP base radio MAC address instead of AP mac addr
CSCvf44285	8.3 does not allow use of spaces in FlexConnect group names, no APs showed on GUI for existing names
CSCvf44497	Cisco 2800, 3800 Flex- If there is no RSN IE, yet the AP is advertising both HT and VHT IEs
CSCvf46715	Cisco 3800 AP running 8.3.124.31: Kernel panic seen on alpha
CSCvf47017	Cisco 2800, 3800 AP - not able to boot and get stuck "BootROM: Image checksum verification FAILED"
CSCvf47808	Cisco Wave 1 APs: Key Reinstallation attacks against WPA protocol
CSCvf48180	Beacon stuck on 2.4GHz band radio
CSCvf50747	When traffic is not initiated by the WLC, the WLC does not check ARP table
CSCvf52008	WLC's GUI hanged and unexpectedly rebooted

Caveat ID Number	Description
CSCvf52723	IOS AP FlexConnect local switching - client cannot pass traffic when using 802.1X + NAC
CSCvf56076	Cal data stored for channels 40, 149 and 153 are incorrect
CSCvf56281	Cisco 3802 AP - Apple Broken Antenna Detection Feature - CLI
CSCvf59621	Cisco 3800, 2800 AP running 8.3.124.40 release: TxFSM Stuck
CSCvf59751	Unable to move FlexConnect APs to custom FlexConnect group
CSCvf62670	AP1850/1830 : Stop Rx without beacon drop in noisy environment
CSCvf63726	Cisco Wave 2 APs - Apple Broken Antenna Detection Feature WCP console error message flood
CSCvf68629	Antenna monitoring is enabled/disabled by ap-name it can not be config'd enabled by group/global
CSCvg10793	Cisco Wave2 APs: Key Reinstallation attacks against WPA protocol
CSCvg18366	hostapd deleting client entry when client goes to FWD state in WCPD
CSCvg29019	AP18xx : Bypassed scan in returning to DFS channel after a blocked-list timeout
CSCvg42682	Cisco Wave 1 APs: Additional fix for Key Reinstallation attacks against WPA protocol
CSCvg50082	Prevent unexpected Cisco WLC reload related to CSCvf87731

Cisco Mobility Express Solution Release Notes

Overview

Note The Cisco Mobility Express wireless network solution is available starting from Cisco Wireless Release 8.3.133.0.

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 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

The following new features and functionalities have been introduced in this release:

- Support for the following access points:
  - Cisco Aironet 1560 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.

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.

- 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 8.3.133.0.

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-K9-8-3-133-0.tar	AIR-AP1560-K9-ME-8-3-133-0.zip
1830	AIR-AP1830-K9-8-3-133-0.tar	AIR-AP1830-K9-ME-8-3-133-0.zip
1850	AIR-AP1850-K9-8-3-133-0.tar	AIR-AP1850-K9-ME-8-3-133-0.zip
2800	AIR-AP2800-K9-8-3-133-0.tar	AIR-AP2800-K9-ME-8-3-133-0.zip
3800	AIR-AP3800-K9-8-3-133-0.tar	AIR-AP3800-K9-ME-8-3-133-0.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