Release Notes for Cisco Wireless Controllers and Lightweight Access Points, Cisco Wireless Release 8.3.140.0, 8.3.141.0, and 8.3.143.0

First Published: 2018-02-16

Last Modified: 2019-01-30

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
January 30, 2019	Added a note about issues related to Cisco Wave 1 AP flash and the solution to address them in the Upgrading Cisco Wireless Release section.
October 30, 2018	Open Caveats—Added CSCvh65876, CSCvi97023, CSCvj95336, CSCvh21953 Resolved Caveats—Added CSCvf66680, CSCvf66696, CSCve64652, CSCvf66723
August 23, 2018	Open Caveat—Added CSCvk44249
July 24, 2018	Added the CIMC Utility Upgrade for 5520 and 8540 Controllers section.
July 17, 2018	Added: Resolved Caveat— CSCvj70569

Modification Date	Modification Details
June 07, 2018	Included Release 8.3.143.0 • Updated Resolved caveats
May 23, 2018	Added information related to CSCvi13589.
April 03, 2018	• Included Release 8.3.141.0 • Updated: Resolved Caveats—CSCvi14641, CSCvi11287
March 20, 2018	Updated the What's New in this Release section.
March 09, 2018	Added: Open Caveats—CSCvi14641, CSCvi32951, CSCvi11287, CSCvi07609, CSCvi01675, CSCvi09424
March 07, 2018	Added: Resolved Caveat—CSCve83024
February 19, 2018	Added: Resolved Caveats—CSCvf76274 and CSCve35938

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 8.3.143.0

Release 8.3.143.0 is a repost of Release 8.3.141.0 to address the caveats listed in the table below. There are no other updates in this release, all open and resolved caveats in addition to the following resolved bugs apply to this release.

Table 2: Resolved Caveats in Release 8.3.143.0

Caveat ID Number	Description
CSCvg39082	Crash after TCP session timeout
CSCvg94522	TxFSM stuck on Radio 0 with new signature
CSCvi02072	Cisco Wave 2 APs: ETSI 5G adaptive Wi-Fi compliance fix
CSCvi17380	TxFSM stuck on Radio 0 with TCQVerify patch
CSCvj36633	Cisco 3700 AP: AP fail to boot after upgrade from 8.5 to 8.8
CSCvj41853	Incorrect Tx power on AP3802P-Q

ETSI New Regulatory Compliance Information

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

For more information, see https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-7/b_upcoming_software_changes_to_meet_the_new_european_requirements_for_5ghz_lan_equipment.html

What's New in Release 8.3.141.0

Release 8.3.141.0 is a repost of Release 8.3.140.0 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 two resolved bugs apply to this release.

Table 3: Resolved Caveats in Release 8.3.141.0

Caveat ID Number	Description
CSCvi11287	Cisco 2800 AP consistently reboots around 1 second after joining to the WLC
CSCvi14641	Cisco 2802, 3802 APs cannot connect with 100Mbps LAN speed

What's New in Release 8.3.140.0

Federal Information Processing Standard (FIPS) Support

In this release, there is an update to the existing FIPS feature function. As per this update, when the Cisco WLC is in FIPS mode or when the Cisco Prime Infrastructure (PI) is used for SNMP management, SNMP trap logger, and as a syslog server with IPSec, you must add the Cisco PI IP address in the Cisco WLC before adding the Cisco WLC IP address in the PI configuration.

You can add the Cisco PI IP address using the following CLI.

config snmp pi-ip-address *ip-address* **{add | delete}**

Note You can add up to three Cisco PI IP addresses in the Cisco WLC configuration.

For more information, see Preparing Cisco WLC in FIPS Mode for Management in Cisco Prime Infrastructure procedure in the *Cisco Wireless Controller Configuration Guide*.

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:

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 8.3.143.0 to a 7.x release, the trap configuration is lost and must be reconfigured.
- If you downgrade from Release 8.3.143.0 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 8.3.143.0 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 8.3.143.0, 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 8.3.143.0.

  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 8.3.143.0 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 8.3.143.0. The following table shows the upgrade path that you must follow before downloading Release 8.3.143.0.

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 5: Upgrade Path to Cisco Wireless Software Release 8.3.143.0

Current Software Release	Upgrade Path to 8.3.143.0 Software
8.0.x	You can upgrade directly to Release 8.3.143.0.
8.2.x	You can upgrade directly to Release 8.3.143.0. 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 8.3.143.0.

- 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 8.3.143.0. 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 8.3.143.0 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 8.3.143.0 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 8.3.143.0 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 8.3.143.0 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
Cisco 2504 WLC	AIR-CT2500-K9-8-3-143-0.aes	AIR-CT2500-AP_BUNDLE-K9-8-3-143-0.aes
Cisco 5508 WLC	AIR-CT5500-K9-8-3-143-0.aes AIR-CT5500-LDPE-K9-8-3-143-0.aes	AIR-CT5500-AP_BUNDLE-K9-8-3-143-0.aes AIR-CT5500-LDPE-AP_BUNDLE-K9-8-3-143-0.aes
Cisco WiSM2	AIR-WISM2-K9-8-3-143-0.aes	AIR-WISM2-AP_BUNDLE-K9-8-3-143-0.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 8.3.143.0 (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 8.3.143.0 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 Release8.3.143.0, 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 Release8.3.143.0, 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 8.3.143.0 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 7: 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 8: 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 9: 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 8.3.14x.0

This section describes the interoperability of Cisco WLC Software, Release 8.3.14x.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	8.3.14x.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 10: 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

Client Name	Version Details
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 11: 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

Client Name	Version Details
Toshiba Thrive AT105	Android 4.0.4

Table 12: 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
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

Client Name	Version Details
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 13: 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 14: 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
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 15: 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 16: 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 17: Open Caveats

Caveat ID Number	Description
CSCva58429	Cisco 1532i AP: low throughput (FlexConnect Local switching + EoGRE)
CSCva86093	'ap-manager' should not be accepted as dynamic interface name
CSCvc29232	Unable to convert Cisco 1815 AP as Mobility Express
CSCvc36044	When 2800, 3800 AP is in Sniffer mode, the non-dual-band is showing "NA" instead of "Sniffer".
CSCvc62540	Smart Licensing "Next Communication Attempt" pre-dates the Controller time after Reboot
CSCvd79510	Wrong error message displayed when applying Local switching with Local Auth in WLC
CSCvd79745	Clients are failing authentication when using Layer 2 and Web-Auth on MAC failure on the same WLAN
CSCve93338	Cisco 1552 AP with 64 MB - radio reloads unexpectedly
CSCvf05741	Reason for channel change is shown as none and noise/energy/interfere as 0 for the dual band radio
CSCvf10786	CAP 2800, 3800 sniffer mode logs wrong PHY and data rates for 802.11ac
CSCvf56556	Guest User role cannot be called properly on the Cisco 2504 WLC platform
CSCvf65133	Dynamic interface template fails to apply on Cisco WLC with DHCP Option 82 setting
CSCvf66801	WLC setting the df bit to on on SNMP get response
CSCvf83251	WLC debug client, flooding logs with " iapp ipv6" logs
CSCvf84806	FIQ/NMI Reset AP2800 PC __pci_bus_size_bridges+0x274/0x768 LR warn_slowpath_common+0x58/0x94
CSCvf91228	WLC unable to timeout clients; stale client entries
CSCvf97662	AP801/AP802 not support DTLS data encryption but it is configurable
CSCvg43654	Cisco Wave 2 APs in FlexConect mode do not forward DHCP NAK to wireless client

Caveat ID Number	Description
CSCvg48786	Cisco 1815T AP LAN3 not coming up when a client is directly connected
CSCvg75189	Cisco 1800 AP: Radio failure and firmware freeze
CSCvg94522	TxFSM stuck on Radio 0 with new signature
CSCvg94718	Standby WLC reloads unexpectedly on spamApTask
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
CSCvh28229	Incorrect count for cLApWlanStatsOnlineUserNum when SSID is changed
CSCvh30872	Decrypt errors on 1532 AP
CSCvh55157	WLC reuses Acct-Session-Id when Client changes WLANs
CSCvh65876	Cisco Wireless LAN Controller Software GUI Privilege Escalation Vulnerability
CSCvh67549	Cisco 8540 WLC Data Plane reloads unexpectedly on __udp_input
CSCvh67590	WLC delay packets due to high DP packet buffers in use
CSCvi01675	New Mobility with 3650MA and 5520 Achor - Guest users cannot reach DG on 8.3.x
CSCvi02106	Repeated CDP-4-DUPLEX_MISMATCH is observed when Cisco Wave 2 APs are connected to a Cisco switch
CSCvi03824	ME 1850 AP reloads unexpectedly due to watchdog reset(capwapd) when AVC debug is enabled
CSCvi07609	Cisco 5520 WLC experiences fatal dataplane crash at broffu_fp_dapi_cmd.c:4588
CSCvi09153	Cisco Wave 1 APs radio reset due FST14 FW: cmd=0x31 seq=6 due to mcast stuck in radio
CSCvi09424	Layer 3 Roam fails back to L2 Anchor with MAC Filtering MAB
CSCvi32951	Cisco Wave 2 APs ignore scanning defer and goes offchannel
CSCvi42632	AP generating 'hostapd' core files, does not respond to EAPOL
CSCvi48503	Standby WLC constinuously reboots with "Reason: XMLs were not trasferred from Active to Standby"
CSCvi51372	Client unable to reach RUN state on anchor WLC with 802.1x + ISE NAC
CSCvi61401	WLC remote access failing after upgrade
CSCvi73013	Cisco Wave 1 AP deauthenticating client due to idle timeout

Caveat ID Number	Description
CSCvi77457	Cisco 5520 WLC experiences fatal dataplane crash at broffu_fp_dapi_cmd.c:4588 -- Invalid Timer Wheel
CSCvi97023	Cisco Wireless LAN Controller Cross-Site Scripting Vulnerability
CSCvj04401	Client remains stuck in DHCP-REQD state on Anchor side unless ISE NAC is disabled on the anchor side
CSCvj41040	Cisco 1800 APs, in Cisco FlexConnect mode, fail FT roam
CSCvj95336	Cisco Wireless LAN Controller Software Information Disclosure Vulnerability
CSCvk44249	WLC 5508 - foreign mapping is missing on a WLAN when restoring a backup

Resolved Caveats

Table 18: Resolved Caveats

Caveat ID Number	Description
Resolved Caveats in Release 8.3.143.0	
CSCvg94522	TxFSM stuck on Radio 0 with new signature
CSCvi02072	Cisco Wave 2 APs: ETSI 5G adaptive Wi-Fi compliance fix
CSCvi17380	TxFSM stuck on Radio 0 with TCQVerify patch
CSCvj36633	Cisco 3700 AP: AP fail to boot after upgrade from 8.5 to 8.8
CSCvj41853	Incorrect Tx power on AP3802P-Q
CSCvj70569	Cisco 2800, 3800,4800 APs: Incorrect Tx power on power on till we configure Tx power using Cisco WLC
Release Caveats for Release 8.3.141.0 and 8.3.140.0	
CSCuz85056	Modifying IP mode from DHCP to Static does not change for a scenario
CSCva27809	Cisco 1850 reboots when joining the Cisco WLC from standalone mode(VAP start failure)
CSCva98597	Emweb task stuck at 100% CPU usage
CSCvb72084	8.2.121.11/8.2.124.15 : Unexpected reload: fatal condition at broffu_fp_dapi_cmd.c
CSCvc07521	AP3800 sends A-MSDU larger than client can handle

Caveat ID Number	Description
CSCvc15777	Cisco 1800, 2800, 3800 APs Tx ARP request with IP address 10.128.128.128
CSCvc78347	Cisco 1832 AP stops working in WLAN when voice traffic transmitted through
CSCvc86951	Cisco 1850 AP beacon missing or corrupted during downstream traffic test
CSCvc89971	Cisco WLC msglog shows AP is being contained on slot 1
CSCvc98310	Cisco 1830AP: 2.4-GHz radio stopped working at @0x009915D7
CSCvd20251	Data Plane stopped working on Cisco 5508 WLC running 8.0.140.0
CSCvd28645	AP sending RTS at 6 data rate when data rate 6 is disabled
CSCvd34105	EoGRE or Mobility Express clients reauth when associated AP moves from standalone to connected mode
CSCvd54154	All Cisco 1850 APs connected to master AP unexpectedly reloads in a loop due to watchdog reset
CSCvd54750	Cisco 7500 WLC on 8.4.2.15 reloads unexpectedly in ideal state with TaskName:spamApTask7
CSCve00464	Cisco 1852 APs detect high noise level on 5-GHz radio for every channel except the serving one
CSCve09179	Cisco 3800 AP sending deauthentication to connected clients when CAPWAP flaps
CSCve10751	Clients cannot assocate with AP after changing from DFS to non-DFS channels during CAC
CSCve15860	CAPWAP data(client)traffic arriving before first Keepalive, keepalive was getting dropped
CSCve18213	Foreign WLC leaks IPv6 and IPv4 multicast client traffic out of EoIP tunnel
CSCve35938	Dual DFS detection implementation on Cisco 2700, 3700 APs
CSCve49772	Multiple APs running 8.5 release reload unexpectedly due to Assertion failure
CSCve57121	Cisco 3800 AP is not passing traffic

Caveat ID Number	Description
CSCve61049	Radio resets in Cisco 2700 AP
CSCve64066	AP is not joining the controller when for first time IP is changed from DHCP to static
CSCve64652	Cisco Access Point 802.11r Fast Transition Denial of Service Vulnerability
CSCve70752	SNMP issue: Tx power level returns null causing Cisco PI, WLC sync to not update AP information
CSCve75022	Cisco WLC does not apply QoS tag upstream from foreign to anchor
CSCve79470	Cisco Wave 2 APs sends RADIUS message directly even if Local Authentication is disabled
CSCve81183	Cisco 2800, 3800 APs - Rx hang in 8.2.154.17 release
CSCve81269	Clients failed to get connected to the Cisco AP in Flex mode with message as AID already in use
CSCve83024	WLC power supply issues not showing up on 360 page
CSCve96870	WCPD out of memory; AP-COS reloads, or fails to send auth or DHCP response to client
CSCvf04412	Cisco 2800/3800 AP acting as ME stopped working due to watchdog reset (OOM) after 23 days of up time
CSCvf05427	Cisco 2800/3800 AP cannot use the RX-SOP
CSCvf07776	Cisco 2800, 3800 AP - FIQ stopped working due to firmware core dump loop
CSCvf10157	Cisco WiSM2 stopped working with emWeb in 8.5.1.183 build
CSCvf12582	Cisco 8.2 release: AP failing NDP Rx causing FRA to misbehave
CSCvf16302	Flash on lightweight IOS APs gets corrupted
CSCvf23079	CAPWAP_HA-3-AP_TEMP_DB_ADD_ERR in standby WLC when changing CAPWAP mode continuously
CSCvf31881	Cisco 2800 AP detects Intel Dual Band Wireless-AC 8260 as rogue client/AP
CSCvf44583	Cisco 2800, 3800 APs transmitting at MCS/802.11n rates to clients with WMM disabled

Caveat ID Number	Description
CSCvf51131	DHCPv6 stateless not working
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
CSCvf66680	Cisco WLC Control And Provisioning of Wireless Access Points Information Disclosure
CSCvf66696	Cisco WLC Control & Provisioning of Wireless Access Points Protocol Denial of Service Vulnerability
CSCvf66723	Cisco Wireless LAN Controller Directory Traversal Vulnerability
CSCvf68648	Dataplane reloads unexpectedly when using EoGRE tunnel
CSCvf71789	Client traffic to local resources go through when the client is in WebAuth reqd state
CSCvf75275	WLC local EAP-TLS authentication with Cisco Unified Wireless IP Phone 7925 handshake failure
CSCvf76274	Cisco APs can no longer join the WLC; CAPWAP-3-DTLS_DB_ERR
CSCvf80409	AP1815 not sending all traffic after period under load
CSCvf81919	Cisco 3800 AP stops working: selipc causing double free
CSCvf82117	WLC fails to send complete IPv6 client information to Prime Infrastructure
CSCvf83391	Cisco 8.3 Release: AP reloads unexpectedly at TAMD ap-tam process
CSCvf83404	VLAN override on RLAN with FlexConnect Local Switching does not work
CSCvf84540	Cisco 3700 AP: radio d1 reset: Tx jammed, probably beacon was not really sent by Hw
CSCvf84715	AP loses config and NAND disk error messages are seen on console
CSCvf85016	Cisco 1142 AP running 8.0 release facing ping loss
CSCvf86148	Cisco 3800 AP reloads unexpectedly while running 8.3.124.40 code

Caveat ID Number	Description
CSCvf93914	AP 3702 5GHz radio constantly flapping
CSCvf95036	Cisco 1850 radio firmware reloads unexpectedly at 0x009A4859
CSCvf96532	WLC anchor commands are missing from the backup
CSCvg00507	Cisco 3700 AP reloads unexpectedly- PID 104: Process "LWAPP Rogue Monitoring process"
CSCvg04467	Client SSID switch: the RADIUS IPv6 traffic does not go out of WLC port
CSCvg07438	AP3800: Low throughput due to packet drops in AP in both fragmented and non-fragmented packets
CSCvg08001	Cisco WiSM 2 reloads unexpectedly on task name spamApTask3 8.2.151.0
CSCvg18366	hostapd deleting client entry when client goes to FWD state in WCPD
CSCvg20743	The client RSSI/SNR is shown as unavailable when connected to 2800/3800 APs.
CSCvg21263	CIAM Alert: GNU dnsmasq DNS Reply Heap Buffer Overflow Vulnerability
CSCvg24597	WLC management VLAN zero in kernel causing reachability issues
CSCvg24833	Cisco 1530 AP in WGB mode reloads unexpectedly on associating with root
CSCvg24954	AID audit should persistent even after reboot
CSCvg25199	Copy cores commands returns syntax error if AP hostname contains (
CSCvg25773	Cisco 7510 WLC on 8.2.151.0 reloads unexpectedly with TaskName:spamApTask7
CSCvg27361	Adding "switchport voice vlan x" causes wired phone not to pull an IP address.
CSCvg27599	Cisco WLC reloads unexpectedly sometime when client switches between FT enabled SSID and CCKM SSIDs
CSCvg28378	AP: cmd timeout AP radio reloads unexpectedly in 8.6 due to Rx hang

Caveat ID Number	Description
CSCvg29907	AP 3800/2800 8.5.107.61 AP sending wrong BSSID in the Request,Identity packet
CSCvg32087	Cisco 5520 WLC reloads unexpectedly on Task Name: nmspTxServerTask
CSCvg32924	SNMPTask (module:k_mib_cisco_lwapp_local) causing memory leak in 16B buffer
CSCvg34444	IW3702 WGB one way broadcast traffic on 5 GHz (but good in 2.4 GHz) in a MESH network 1572 AP
CSCvg35115	Cisco 3802 running 8.3.130 shows radio core without the crash file
CSCvg38669	ERROR-MeshSecurity: Processing EAPOL from CAWAWP, Mesh mode is not started
CSCvg38681	FlexConnect APs WLAN-VLAN mappings inheritance is lost when a WLAN is deleted from AP group
CSCvg39960	Cisco WLC reloads unexpectedly on task - sntpReceiveTask
CSCvg40792	Client global IPv6 not correctly mapped to MAC address under certain conditions
CSCvg42682	Key Reinstallation attacks against WPA protocol
CSCvg44078	WLC unable to timeout clients; stale client entries
CSCvg46125	Cisco WLC reloads unexpectedly multiple times
CSCvg46620	Dataplane watchdog timeout due to NBAR max flows exceeded
CSCvg46708	Cisco 5508 WLC reloading due to memory leak in Anon Pages emweb
CSCvg49007	APIC-EM PnP Status as "Error" when should be "Provisioned" for 2802I & 1852I on Release 8.3.132.0
CSCvg49532	HA : "config service statistics" not synced
CSCvg50082	Prevent unexpected WLC reload related to CSCvf87731
CSCvg53640	Cisco 1830 AP Triggered FW assert for radio failure (beacons stuck)
CSCvg57548	Beacon stuck observed on radio 0

Caveat ID Number	Description
CSCvg59338	NMSP drops observed in high density deployments
CSCvg60452	aIOS and flex standalone failure on FT-dot1x authentication or M3 RSN IE
CSCvg60758	Cisco Wave 2 APs drops TCP retransmit from server
CSCvg62039	False radar detection on AP 1832 with 40MHz CW
CSCvg62359	Cisco 2800, 3800 APs: Click scheduler 0 stuck at Sched/FSys:1/0 Epoch
CSCvg63216	WLC RFID queue breached with more than 4000 tags.
CSCvg64993	WLC mDns secure printer service response missing TXT record with mDNS snooping enabled
CSCvg66702	OUI Update failure and WLC System reloads unexpectedly while updating the OUI file
CSCvg67318	TPC version is not included in the run-config commands
CSCvg70384	Cisco 1832/1852 AP radio reloads unexpectedly at 0x009A497D
CSCvg73522	Cisco 5508 WLC reloads unexpectedly due to memory leak in snmpApPowerTrap()
CSCvg75933	Webauth related ports are not blocked by CPU ACL
CSCvg77711	System reloads at random on running mesh commands
CSCvg78101	Local EAP profiles changed not retained after it is applied
CSCvg82215	Cisco 3504 WLC undergoes unexpected silent reloads when using mGig port
CSCvg83585	APs cannot send NDP Tx on all channels and cant be found as neighbors on nearby APs
CSCvg85175	Cisco WLC reloads unexpectedly with task name spamApTask0
CSCvg85651	Management Packets are marked with wrong DSCP
CSCvg86324	WLC reloads unexpectedly with SNMP operation with Flex ACL
CSCvg89807	Silver QoS profile is assigned to RLAN when configuration is imported

Caveat ID Number	Description
CSCvg91108	WQE size constantly increasing, error messages
CSCvg91708	WLC emweb reloads unexpectedly at commandConfigSpamApAntennaMonitor
CSCvg91734	Cisco 1852/1832 AP: AP data traffic stall in HD environment
CSCvg93191	8.3.134.40: AP3800 beacon stuck when radio reloads unexpectedly with signature "B0B0"
CSCvg95268	Allow flex/bridge mode APs in FIPS mode
CSCvg97208	AP1852: Apple clients connection fails in 802.11r adaptive mode in WLAN
CSCvg97712	Cisco 1850 AP console flooded with "Total NR report Length exceeds Max Buffer Size -1067447752"
CSCvg98098	AP1852: 5-GHz radio firmware crash @0x00981CED and @0x0099010D
CSCvg98786	IOS AP DTLS flap issue seen in pre commit sanity
CSCvg99890	'config certificate generate' line of uploaded config is corrupted
CSCvh00256	Cisco WLC has multiple open ports, cannot be properly secured
CSCvh00398	WSA: Flex RADIUS Stats data parsing fails
CSCvh01089	False beacon stuck issue due to no beacon updates in WCP message Host Triggered a radio crash
CSCvh01470	Cisco 5520, 8540 : Little Endian issue while adding rules in IPtables for SNMP trap over IPsec
CSCvh05911	Cisco WLC reloads unexpectedly after enabling FIPS
CSCvh07545	AP2800/3800 Kernel Panic due to processing of RX frames before driver is initialized
CSCvh08020	AP stuck in ap: after upgrade - flashfs[0]: writing to flash handle Illegal Operation
CSCvh12768	IOS 3700 AP could not join WLC over CAPWAPv6 tunnel using DHCPv6 address
CSCvh14989	Client in RUN state on anchor with 0.0.0.0 IP address
CSCvh16615	Cisco 5520 WLC reloads unexpectedly in a loop with task nmspRxServerTask

Caveat ID Number	Description
CSCvh16970	Cisco WLC does not apply ACL Template from PI correctly
CSCvh18096	CPU ACL does not block HTTPS traffic to management interface from wired client
CSCvh21486	WLC reloads unexpectedly due to Task "apfMsConnectionTask" when MBUF debug is enabled
CSCvh23785	AireOS WLC: Multiple wireless clients failing the broadcast Key refresh (M5)
CSCvh25039	SNMP causes unexpected reloads
CSCvh25368	WLC memory leak on CDP
CSCvh27570	cLSiIdrClusterAffectedChannels OID returning unexpected values
CSCvh28179	Kernal panic with PC is at skb_release_data+0xe0/0x230
CSCvh32031	ME: Update Root CA Certificate for Mobility Express Cisco.com Software Download Method
CSCvh47521	Cisco AP decrypt failed
CSCvh49418	WSA dx-sync enabled by default on 8.3 code - ask is to disable it on 8.3
CSCvh53094	Unable to access GUI of Cisco WLC with webadmin certificates
CSCvh53814	COS Flex LS: IPv6 RA dropped with high level of multicast on wired interface
CSCvh70354	Alpha WLC: Memory Leak in radiusTransportThr
CSCvh72803	AP stops working during sh tech collection command that includes show capwap client config
CSCvh74663	IOS AP stops working during sh tech collection command that includes show capwap client config using SSH
CSCvi11287	Cisco 2800 AP consistently reboots around 1 second after joining to the WLC
CSCvi14641	Cisco 2802, 3802 APs cannot connect with 100Mbps LAN speed

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 Master AP. Other access points, referred to as Subordinate APs, associate to this Master AP.

The Master 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 Master (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 Master 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 master.

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 Master 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 Master AP and to select a new AP as Master 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 8.3.143.0.

Access Points Supported As Master	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-K9-8-3-143-0.tar	AIR-AP1560-K9-ME-8-3-143-0.zip
1830	AIR-AP1830-K9-8-3-143-0.tar	AIR-AP1830-K9-ME-8-3-143-0.zip
1850	AIR-AP1850-K9-8-3-143-0.tar	AIR-AP1850-K9-ME-8-3-143-0.zip
2800	AIR-AP2800-K9-8-3-143-0.tar	AIR-AP2800-K9-ME-8-3-143-0.zip
3800	AIR-AP3800-K9-8-3-143-0.tar	AIR-AP3800-K9-ME-8-3-143-0.zip

Installing Mobility Express Software

See the "Getting Started" section in the *Mobility Express User Guide* at http://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