Release Notes for Cisco Wireless Controllers and Lightweight Access Points, Cisco Wireless Release 8.2.170.0

First Published: June 08, 2018

This release notes document describes what is new in Cisco Wireless Release 8.2.x, instructions to upgrade to this release, and open and resolved caveats for this release. Unless otherwise noted, in this document, all Cisco Wireless Controllers are referred to as *Cisco WLCs*, and all Cisco lightweight access points are referred to as *access points* or *Cisco APs*.

Note For Cisco wireless solution software compatibility information, see the *Cisco Wireless Solutions Software Compatibility Matrix* at http://www.cisco.com/c/en/us/td/docs/wireless/compatibility/matrix/compatibility-matrix.html.

Note For information specific to the Cisco Mobility Express solution, see "Cisco Mobility Express Solution Release Notes" section on page 33.

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

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	• Added – Open bugs: CSCvf66696, CSCve64652, CSCvj95336 – Resolved bugs: CSCvh65876, CSCvf66680,CSCvf66723, CSCvi97023, CSCvh21953
July 17, 2018	• Added – Resolved bug:CSCvj70569

Cisco Wireless Controller and Cisco Lightweight Access Point Platforms

The section contains the following subsections:

- Supported Cisco Wireless Controller Platforms, page 2
- Supported Access Point Platforms, page 3

Supported Cisco Wireless Controller Platforms

The following Cisco WLC platforms are supported in this release:

- Cisco 2500 Series Wireless Controllers (Cisco 2504 Wireless Controller)
- Cisco 5500 Series Wireless Controllers (5508 and 5520 Wireless Controllers)
- Cisco Flex 7500 Series Wireless Controllers (Cisco Flex 7510 Wireless Controller)
- Cisco 8500 Series Wireless Controllers (8510 and 8540 Wireless Controllers)
- Cisco Virtual Wireless Controllers on the Cisco Services-Ready Engine (Cisco SRE) or the Cisco Wireless LAN Controller Module for Cisco Integrated Services Routers G2 (UCS-E)

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

For information about features that are not supported on the Cisco WLC platforms, see "Features Not Supported on Cisco WLC Platforms" section on page 18.

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 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 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 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 8.2.170.0, 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 features that are not supported on some access point platforms, see the "Features Not Supported on Cisco Access Point Platforms" section on page 21.

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* document.

What's New in Release 8.2.170.0

There are no new features or enhancements in this release. For more information about updates in this release, see the Caveats section.

ETSI New Regulatory Compliance Information

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

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

Software Release Types and Recommendations

Table 2 Release Types

Release Type	Description	Benefit
Maintenance Deployment (MD) releases	Software releases that provide bug-fix support and ongoing software maintenance. These releases are categorized as Maintenance Deployment (MD) and may be part of the AssureWave program.[1] These are releases with long life and ongoing software maintenance.	Provides you with a software release that offers stability and long support duration with periodic maintenance releases (MRs).
Early Deployment (ED) releases	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.

[1] AssureWave is a Cisco program that focuses on satisfying customer quality requirements in key industry segments in the mobility space. This program links and expands on product testing conducted within development engineering, regression testing, and system test groups within Cisco. The AssureWave program has established partnerships with major device and application vendors to help ensure broader interoperability with our new release. The AssureWave certification marks the successful completion of extensive wireless LAN controller and access point testing in real-world use cases with a variety of mobile client devices applicable in a specific industry.

For detailed release recommendations, see the software release bulletin:

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

For more information about the Cisco Wireless solution compatibility matrix, see http://www.cisco.com/c/en/us/td/docs/wireless/compatibility/matrix/compatibility-matrix.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

- In previous software versions, it was possible to enable 802.11r Fast Transition (FT) on a WLAN without WPA/WPA2 authentication. This behavior has been corrected in this release. However, if you have the FT parameters enabled on a non-WPA/WPA2 WLAN prior to your upgrade, you may find that the WLAN is subsequently disabled after the upgrade. WLAN cannot be enabled until you disable the FT parameters.
- WLAN-AP group association functionality:
  - Functionality prior to Release 7.4.130.0—If a WLAN was added to an AP group prior to Release 7.4.130.0, the RF radio policy is set to All after an XML upload/download. This is because the default value of RF policy was not added. This issue was addressed through CSCud37443. However, this corrects only the newly created WLAN-AP group associations and not the previous ones. Therefore, if you have configured a WLAN-AP group association prior to Release 7.4.130.0, you must remove the WLAN from the AP group and add it again in Release 7.4.130.0 or a later release.

    Also, the XML configuration for radio policy was not present in releases prior to 8.0. This issue is addressed through CSCul59089.
  - Change in functionality with Release 7.4.130.0—The RF radio policy is by default set to None for all WLAN-AP group associations created in Release 7.4.130.0. Any previous WLAN-AP group associations that are carried over will continue to be set to All unless a WLAN is removed from the AP group and added again.

    The XML upload/download for AP group RF radio policy is available only from Release 8.0.
- When you change the WLAN profile name, then FlexConnect APs (using AP-specific VLAN mapping) will become WLAN-specific. If FlexConnect Groups are properly configured, the VLAN mapping will become Group-specific.
- After upgrading to Release 8.2, the Cisco WLC might lose all IPv4 connectivity. The Cisco WLC can no longer service incoming SSH/Web sessions and is unable to ping other IPv4 stations. However, the default router is able to ping the Cisco WLC's management interface.

  Every 10 seconds, a message similar to the following is sent to the msglog:

  ```
  *dtlArpTask: Jan 06 23:50:37.312: %OSAPI-4-GW_ADD_FAILED: osapi_net.c:1032 Unable to
  add the gateway 192.168.145.1. System command returned failure. Errorcode:256
  ```

  This occurs in the following conditions:

  a. LAG is not configured.

  b. The management interface is untagged and is mapped to one physical port.

  c. When an untagged dynamic interface is added and mapped to port 2, the default route for the management interface is lost.

  The workaround is to configure all interfaces with VLANs.

Note In Release 8.2, it is not possible to have multiple untagged interfaces; however, this issue is resolved in Release 8.3. You can track this issue via CSCux75436.

- Effective with Release 8.2.100.0, you cannot download some of the older configurations from the Cisco WLC because of the Multicast and IP address validations introduced in this release. The platform support for global multicast and multicast mode are listed in the following table.

Table 3 Platform Support for Global Multicast and Multicast Mode

Platform	Global Multicast	Multicast Mode	Support
Cisco 5520, 8510, and 8540 WLCs	Enabled	Unicast	No
	Enabled	Multicast	Yes
	Disabled	Unicast	Yes
	Disabled	Multicast	No
Cisco Flex 7510 WLC	Multicast is not supported.		
Cisco 5508 WLC	Enabled	Unicast	Yes
	Enabled	Multicast	Yes
	Disabled	Unicast	Yes
	Disabled	Multicast	No
Cisco 2504 WLC	Only multicast mode is supported.		
Cisco vWLC	Multicast is not supported.		

- To enable all CLI commands on IOS APs, enter the hidden command **debug capwap console cli** command.
- Cisco WLC Release 7.3.112.0, which is configured for new mobility, might revert to old mobility after upgrading to Release 7.6, even though Release 7.6 supports new mobility. This issue occurs when new mobility, which is compatible with the Cisco 5760 Wireless LAN Controller and the Cisco Catalyst 3850 Series Switch, are in use. However, old mobility is not affected.

  The workaround is as follows:

  a. Enter the following commands:

  ```
  config boot backup
  show boot

  Primary Boot Image.................. 7.6.100.0
  Backup Boot Image................... 7.3.112.0 (default) (active)
  ```

  b. After the reboot, press **Esc** on the console, and use the boot menu to select **Release 7.6**.

  c. After booting on Release 7.6, set back the primary boot, and save the configuration by entering the following command:

  config boot primary

Note The epings are not available in the Cisco 5500 Series WLC when New Mobility is enabled.

Note If you downgrade from a Cisco WLC release that supports new mobility to a Cisco WLC release that does not support new mobility, for example, Cisco Wireless Release 7.6 to Release 7.3.x and you download the 7.6 configuration file with new mobility in enabled state, the release that does not support new mobility will have the new mobility feature in enabled state.

- If you downgrade from Release 8.2.170.0 to a 7.x release, the trap configuration is lost and must be reconfigured.

- 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 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 8.2.170.0, 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 8.2.170.0.

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.
- We recommend that you install the recommended Cisco Wireless LAN Controller Field Upgrade Software (FUS) listed in Table 4, 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 http://www.cisco.com/c/en/us/td/docs/wireless/controller/release/notes/fus_rn_OL-31390-01.html.

Table 4 FUS Upgrade Guidance

WLC Controller Model	Recommended FUS Version
2504	2.0, see CSCuu46671
5508	1.9, see CSCul68057
5520	No FUS
7510	2.0, see CSCus97953
8510	2.0, see CSCus97953
8540	No FUS
WiSM2	1.9, see CSCul68057

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.

Note 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.

- 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 8.2.170.0 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 8.2.170.0. Table 5 shows the upgrade path that you must follow before downloading Release 8.2.170.0.

Caution 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.

Table 5 Upgrade Path to Cisco WLC Software Release 8.2.x

Current Software Release	Upgrade Path to 8.2.x Software
7.6.x	You can upgrade directly to 8.2.x.
8.0.x	You can upgrade directly to 8.2.x.
8.2.x	You can upgrade directly to 8.2.170.0.

- 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.

- 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.
- 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 8.2.170.0. 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 8.2.170.0 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.
    ```

- 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 5500 Series WLC), or enter **5** (on Cisco WLC platforms other than 5500 series) 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 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*.

Note Predownloading Release 8.2.170.0 on a Cisco Aironet 1240 access point is not supported when upgrading from a previous Cisco WLC release. If predownloading is attempted on a Cisco Aironet 1240 access point, an AP disconnect will occur momentarily.

- 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 8.2.170.0 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

Upgrading to Cisco WLC Software Release 8.2.x(GUI)

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 8.2.170.0 software:

a. Click this URL to go to the Software Center:

http://www.cisco.com/cisco/software/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
- 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).

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 Choose **Commands** > **Download File** to open the Download File to Controller page.

Step 5 From the **File Type** drop-down list, choose **Code**.

Step 6 From the **Transfer Mode** drop-down list, choose **TFTP**, **FTP**, or **SFTP**.

Step 7 In the **IP Address** text box, enter the IP address of the TFTP, FTP, or SFTP server.

Step 8 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 9 In the **File Path** text box, enter the directory path of the software.

Step 10 In the **File Name** text box, enter the name of the software file (*filename*.aes).

Step 11 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 12 Click **Download** to download the software to the Cisco WLC.

A message appears indicating the status of the download.

Step 13 After the download is complete, click **Reboot**.

Step 14 If you are prompted to save your changes, click **Save and Reboot**.

Step 15 Click **OK** to confirm your decision to reboot the Cisco WLC.

Step 16 For Cisco WiSM2 on the Catalyst switch, check the port channel and re-enable the port channel if necessary.

Step 17 If you have disabled the 802.11a/n and 802.11b/g/n networks in Step 4, re-enable them.

Step 18 To verify that the 8.2.170.0 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.

Special Notes for Licensed Data Payload Encryption on Cisco Wireless LAN Controllers

Datagram Transport Layer Security (DTLS) is required for all Cisco 600 Series OfficeExtend Access Point deployments to encrypt data plane traffic between the APs and the Cisco WLC. You can purchase Cisco Wireless LAN Controllers with either DTLS that is enabled (non-LDPE) or disabled (LDPE). If DTLS is disabled, you must install a DTLS license to enable DTLS encryption. The DTLS license is available for download on Cisco.com.

Important Note for Customers in Russia

If you plan to install a Cisco Wireless LAN Controller in Russia, you must get a Paper PAK, and not download the license from Cisco.com. The DTLS Paper PAK license is for customers who purchase a Cisco WLC with DTLS that is disabled due to import restrictions, but have authorization from local regulators to add DTLS support after the initial purchase. Refer to your local government regulations to ensure that DTLS encryption is permitted.

Note Paper PAKs and electronic licenses that are available are outlined in the respective Cisco WLC platform data sheets.

Downloading and Installing a DTLS License for an LDPE Cisco WLC

Step 1 To download the Cisco DTLS license:

a. Go to the Cisco Software Center at this URL:

https://tools.cisco.com/SWIFT/LicensingUI/Home

b. From the Product License Registration page from the **Get Other Licenses** drop-down list, click **IPS, Crypto, Other ...**.

c. In the **Wireless** section, click **Cisco Wireless Controllers (2500/5500/7500/WiSM2) DTLS License** and click **Next**.

d. Follow the on-screen instructions to generate the license file. The license file information will be sent to you in an e-mail.

Step 2 Copy the license file to your TFTP server.

Step 3 Install the DTLS license either by using the Cisco WLC web GUI interface or the CLI:

- To install the license using the WLC web GUI, choose:

  Management > **Software Activation** > **Commands** > **Action**: **Install License**

- To install the license using the CLI, enter this command:

  license install tftp:*//ipaddress /path /extracted-file*

  After the installation of the DTLS license, reboot the system. Ensure that the DTLS license that is installed is active.

Upgrading from an LDPE to a Non-LDPE Cisco WLC

Step 1 Download the non-LDPE software release:

a. Go to the Cisco Software Center at:

http://www.cisco.com/cisco/software/navigator.html?mdfid=282585015&i=rm

b. Choose the Cisco WLC model.

c. Click **Wireless LAN Controller Software**.

d. In the left navigation pane, click the software release number for which you want to install the non-LDPE software.

e. Choose the non-LDPE software release: AIR-X-K9-X-X.X.aes

f. Click **Download**.

g. Read the Cisco End User Software License Agreement and then click **Agree**.

h. Save the file to your hard drive.

Step 2 Copy the Cisco WLC software file (*filename*.aes) to the default directory on your TFTP server or FTP server.

Step 3 Upgrade the Cisco WLC with this version by performing Step 3 through Step 18 detailed in the "Upgrading Cisco Wireless Release" section on page 5.

Interoperability with Other Clients

This section describes the interoperability of Cisco WLC Software, Release 8.2.170.0 with other client devices.

Table 6 Test Bed Configuration for Interoperability

Hardware/Software Parameter	Hardware/Software Configuration Type
Release	8.2.170.0
Cisco WLC	Cisco 55xx Series Controller
Access points	AIR-CAP3802E-B-K9, AIR-AP1852I-B-K9, AIR-AP2802I-B-K9
Radio	802.11ac, 802.11a, 802.11g, 802.11b, 802.11n
Security	Open, PSK (WPA-TKIP), PSK (WPA-TKIP, WPA2-AES), 802.1X (WPA-TKIP and WPA2-AES) (LEAP, EAP-FAST)
RADIUS	ACS 5.3, ISE 1.4
Types of tests	Connectivity, traffic, and roaming between two access points

The following tables list the client types on which the tests were conducted. The clients included laptops, hand-held devices, phones, and printers.

Laptop.

Table 7 Laptop Client Type List

Client Type and Name	Version
Intel 3160	18.40.0.9
Intel 6205	15.16.0.2
Intel 6300	15.16.0.2
Intel 7260	18.33.3.2
Intel 7265	19.10.1.2
Intel 8260	19.10.1.2
Broadcom 4360	6.30.163.2005
Linksys AE6000 (USB)	5.1.2.0
Netgear A6200 (USB)	6.30.145.30
Netgear A6210(USB)	5.1.18.0
D-Link DWA-182 (USB)	6.30.145.30
Engenius EUB 1200AC(USB)	1026.5.1118.2013
Asus AC56(USB)	1027.515.2015
Dell 1520/Broadcom 43224HMS	5.60.48.18
Dell 1530 (Broadcom BCM4359)	5.100.235.12
Dell 1540	6.30.223.215
Dell 1560	6.30.223.262
MacBook Pro	OSX 10.12.3
MacBook Air old	OSX 10.11.5
MacBook Air new	OSX 10.12.6
Macbook Pro with Retina Display	OSX 10.12
Macbook New 2015	OSX 10.12

Tablet.

Table 8 Tablet Client Type List

Client Type and Name	Version
Amazon Kindle	Andriod 6.2.2
Apple iPad Air	iOS 10.1.1
Apple iPad Air 2	iOS 10.2.1
Apple iPad mini with Retina display	iOS 10
Apple iPad Pro	iOS 10
Apple iPad2	iOS 10
Apple iPad3	iOS 10
Google 10.2" Pixel C	Android 7.1.1
Google Nexus 9	Android 6.0.1

Table 8 Tablet Client Type List

Client Type and Name	Version
MC40N0	Android 4.4.4
MC9090-C030	OS 5.1.478 (Build 15706.3.5.2)
MC9190G	OS 6.00.000
MC92	Android 4.4.4
Microsoft Surface Pro 2	Windows 8.1 Driver: 14.69.24039.134
Microsoft Surface Pro 3	Windows 8.1 Driver: 15.68.3093.197
Microsoft Surface Pro 4	Windows 10 Driver: 15.68.9040.67
Motorola MC 55A	OS 5.2.23121(Build 23121.5.3.6)
Motorola MC 75A	OS 5.2.23137 (Build 23137.5.3.9)
Samsung Galaxy Note 3 – SM-N900	Android 5.0
Samsung Galaxy Tab 10.1- 2014 SM-P600	Android 4.4.2
Samsung Galaxy Tab Pro SM-T320	Android 4.4.2
Symbol MC70	Windows Mobile 05.01.0476
Symbol MC9090	Windows Mobile 5.1.478 (Build 15706.3.5.2)
Symbol TC55	Android 4.1.2
Symbol TC75	Android 4.4.3
Symbol VC5090	5.0.1400
Toshiba Thrive AT105	Android 4.0.4
Zebra MC55A	OS 5.2.29344 (Build 29344.5.3.12.40)
Zebra TC8000	Android 4.4.3

Phones and Printers.

Table 9 Phone and Printer Client Type List

Client Type and Name	Version
Apple iPhone 4S	iOS 10.2
Apple iPhone 5	iOS 10.2
Apple iPhone 5c	iOS 10
Apple iPhone 5s	iOS 10.2
Apple iPhone 6	iOS 10.2
Apple iPhone 6 Plus	iOS 10.2
Apple iPhone 6s	iOS 10.2
Cisco 7921G	1.4.5.3.LOADS
Cisco 7925G	1.4.5.3.LOADS

Table 9 Phone and Printer Client Type List

Client Type and Name	Version
Cisco 8861	Sip88xx.10-2-1-16
Cisco 9971	Sip88xx.10-2-1-16
Google Nexus 5	Android 6.0.1
Google Nexus 5X	Android 6.0.1
Google Pixel	Android 7.1.1
HP Color LaserJet Pro M452nw	version 2.4.0.125
HTC One	Android 5.0
LG G4	Android 5.1
Nokia Lumia 925	Windows Phone 8.10.12393.890
Nokia Lumia 1520	Windows Phone 8.10.14219.341
OnePlus One	Android 4.3
OnePlus Three	Android 6.0.1
Samsung Galaxy Mega SM900	Android 4.4.2
Samsung Galaxy Nexus GTI9200	Android 4.4.2
Samsung Galaxy S III	Android 4.3
Samsung Galaxy S4	Android 5.0.1
Samsung Galaxy S4 – GT-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 6.0.1
Samsung Galaxy S7	Android 6.0.1
Sony Xperia Z Ultra	Android 4.4.2
Xiaomi Mi 4c	Android 5.1.1
Xiaomi Mi 4i	Android 5.1.1

Features Not Supported on Cisco WLC Platforms

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

- Features Not Supported on Cisco 2504 WLC, page 19
- Features Not Supported on Cisco WiSM2 and Cisco 5508 WLC, page 19
- Features Not Supported on Cisco Flex 7510 WLCs, page 20
- Features Not Supported on Cisco 5520, 8510, and 8540 WLCs, page 21
- Features Not Supported on Cisco Virtual WLCs, page 21
- Features Not Supported on Mesh Networks, page 25

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

Features Not Supported on Cisco 2504 WLC

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

  Note However, AVC for local mode APs is supported.

- Bandwidth Contract
- Service Port
- AppleTalk Bridging
- Right-to-Use Licensing
- Smart 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.

Features Not Supported on Cisco WiSM2 and Cisco 5508 WLC

- 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.
- Smart Licensing

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.

- TrustSec SXP
- 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
- Smart Licensing

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

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

Note Smart Licensing is not supported on Cisco 8510 WLC.

Features Not Supported on Cisco Virtual WLCs

- Cisco Aironet 1850 and 1830 Series APs
- 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
- EoGRE (Supported in only local switching mode)
- Workgroup Bridges
- Client downstream rate limiting for central switching
- SHA2 certificates
- Cisco OfficeExtend Access Points

Features Not Supported on Cisco Access Point Platforms

- Features Not Supported on Cisco Aironet 1550 APs (with 64-MB Memory), page 22

Features Not Supported on Cisco Aironet 1550 APs (with 64-MB Memory)

- PPPoE
- PMIPv6

Note To see the amount of memory in a Cisco Aironet 1550 AP, enter the following command:

```
(Cisco Controller) >show mesh ap summary
```

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

Table 10 Features Not Supported on Cisco Aironet 1810 OEAP, 1810W, 1830, 1850, 2800 and 3800 Series APs

Operational Modes	• Spectrum Expert Connect • Workgroup Bridge (WGB) mode as a part of Cisco Mobility Express • Mesh mode • Flex plus Mesh • 802.1x supplicant for AP authentication on the wired port
Protocols	• 802.11u • Full Cisco Compatible Extensions (CCX) support • Rogue Location Discovery Protocol (RLDP) • Native IPv6 • Telnet • Internet Group Management Protocol (IGMP)v3
Security	• Locally Significant Certificate (LSC) • TrustSec SXP • CKIP, CMIC, and LEAP with Dynamic WEP • Static WEP key for TKIP or CKIP [1] • WPA2 + TKIP **Note** WPA +TKIP and TKIP + AES protocols are supported.
Quality of Service	• Cisco Air Time Fairness (ATF)

Table 10 Features Not Supported on Cisco Aironet 1810 OEAP, 1810W, 1830, 1850, 2800 and 3800 Series APs (continued)

Location Services	• Data RSSI (Fast Locate) • Wi-Fi Tag
FlexConnect Features	• Per Client AAA (QoS Override) • Link aggregation (LAG) • Bidirectional rate-limiting • Split Tunneling • EoGRE • 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 • Proxy ARP • PPPoE • SIP snooping with FlexConnect local switching

[1] For more details, see the Wi-Fi Alliance Technical Note TKIP document in the Wi-Fi Organization's website.

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

Table 11 Features Not Supported on Cisco Aironet 1810 OEAP and 1810W Series APs

Operational Modes	• SIP with FlexConnect in local switching mode • Monitor Mode • Multiple client on wired ports
FlexConnect Features	• Local AP Authentication

Features Not Supported on Cisco Aironet 1830 and 1850 Series APs

Table 12 Features Not Supported on Cisco Aironet 1830 OEAP and 1850 Series APs

Operational Modes	• Monitor Mode
FlexConnect Features	• Local AP Authentication

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

Caveats describe unexpected behavior in a product. The Open Caveats section lists open caveats that apply to the current release and may apply to previous releases. A caveat that is open for a prior release and is still unresolved applies to all future releases until it is resolved.

To view the details of the software bugs pertaining to your product, perform the following task:

Click the Caveat ID/Bug ID number in the table.

The corresponding Bug Search Tool page is displayed with details of the Caveat ID/Bug ID.

The Bug Search Tool (BST), which is the online successor to the Bug Toolkit, is designed to improve the effectiveness in network risk management and device troubleshooting. The BST allows partners and customers to search for software bugs based on product, release, and keyword, and aggregates key data, such as bug details, product, and version. The tool has a provision to filter bugs based on credentials to provide external and internal bug views for the search input.

To view the details of a caveat whose ID you do not have, perform the following procedure:

1. Access the BST using your Cisco user ID and password:

https://tools.cisco.com/bugsearch/

2. In the Bug Search window that is displayed, enter the necessary information in the corresponding fields.

For more information about how to use the Cisco Bug Search Tool effectively, including how to set email alerts for bugs and to save bugs and searches, see the Bug Search Tool Help & FAQ page.

Open Caveats

Table 13 Open Caveats

Caveat ID Number	Description
CSCuu49801	Country code issue with AE, AL
CSCux15561	Cisco 3500, 1260 AP gets into 'ap:' mode after power cycle
CSCux28505	Cisco 8510 WLC stopped working with high traffic during boot
CSCux59359	Guest anchor clients moving from Cisco 8510 WLC foreign to anchor gets stuck in the DHCP_reqd state
CSCux78581	Cisco 1810 APs do not support multiple clients on LAN ports
CSCuy75333	Cisco 2504 WLC config restoration fails due to multicast mode command
CSCuz03702	Wired client behind WGB fails to pass traffic after roaming
CSCuz11374	Cisco WLC selects an incorrect DHCP relay even though it is configured on an interface
CSCuz18914	Fast Transition (FT) Over-the-Air roam does not work
CSCuz27736	Cisco 3800 AP on Flex-AP deauthenticates after FT roam (Freq- 3-4%)
CSCuz29774	Cisco 1852 APs lose connectivity to the ME controller when AVC is enabled
CSCuz49804	Fix AID leak problems
CSCuz88573	Unexpected reload in emWeb
CSCva00087	WLC reloads unexpectedly on apfVerifyCountryString spamApTask2
CSCva07307	Voice tagged frames drop at AP radio after upgrade to 8.2 and later release
CSCva16449	Cisco 1552 APs not showing temperature on Cisco WLC on 8.2 release
CSCva27276	Cisco 2802 AP: local profiling detects windows client as 'Microsoft-Workstation'
CSCva27419	Channel changed trap with Unknown Radio Type on dual band radio
CSCva29463	Cisco 3800 AP: WLAN client fails >=1500 bytes ICMP traffic in standalone mode
CSCva29554	FlexConnect AAA overridden ACL is not plumbed in the Cisco WLC
CSCva53980	Issue in CleanAir when client serving band is 5 GHz
CSCva71002	WLC GUI client filter fails with spaces used in the client Name
CSCva85361	Cisco WLC is losing IPv6 connectivity
CSCva99864	EAP-TLS fails with Windows and ME using 'Smart card or certificate' authentication
CSCvb02180	ARP table full. Unable to delete ARP mapping IP
CSCvb18640	Mobility Express: Manual Channel-Widths Overwritten by DCA
CSCvb23576	Excluded clients can connect to Cisco 2800 APs in FlexConnect local switching
CSCvb31857	WLC rejects client association with 802.11k assisted roaming on Cisco 2800 5-GHz AP
CSCvb36432	SSIDs vanishes from standalone AP after reboot
CSCvb62874	Radio interface Input queue gets filled on Autonomous APs.
CSCvb72389	CWA: Redirect traffic from client goes through CAPWAP tunnel instead of VxLan

Table 13 Open Caveats

Caveat ID Number	Description
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
CSCvb99468	AireOS WLC reloads unexpectedly in emWeb when serving an EmWebForm exclusion-list
CSCvc25658	Cisco 2800,3800 padding from small CAPWAP fragments transmitted over the air to clients
CSCvc51666	Cisco Wave 1 AP transmits on disabled rate 24Mb
CSCvc55430	WLC HA redundancy management interface not reachable for a short time after failover
CSCvc57427	Cisco WiSM2 - Memory leak while handling Cisco AVP POLICY_ROLE_TYPE(cisco_avp_pair="role")
CSCvc62540	Smart Licensing Next Communication Attempt pre-dates the Controller time after reboot
CSCvc78347	Cisco 1832 AP expectedly reloads in ZN6IntArg5parseEPKcS1_biPji+0x0/0x320 for SIP call
CSCvc78510	Cisco 2702 AP aux port goes to disabled after the AP is rebooted
CSCvc93398	CIsco 2800, 3800 AP MU-MIMO forms MU groups with 2SS clients
CSCvc94524	Cisco 2800, 3800 AP: iPhone and Android phones are not getting IPv6 addresses
CSCvd16800	Client associated to MAP does not get AAA override in Flex+Bridge mode
CSCvd21969	AAA AVC Override - AVC profile retained after roaming
CSCvd27065	EAP-FAST EAP-Chaining on wired Cisco 1810W AP port does not work
CSCvd27365	Cisco WLC reports incorrect number of clients associated on the AP due to AID leak
CSCvd53205	DCA lists in RF profiles are broken in the WLC configuration after the backup and restore is done
CSCvd68141	Cisco 5520, 8540, VM WLCs stopped working at task nmspRxServerTask
CSCvd72432	LocalEAP LDAP request with incorrect password locks the user
CSCvd78452	APs joining the WLC in flex-mode fails to use the flex ACLs in the group policies
CSCvd90377	WLC is applying wrong ACL to clients when doing CWA
CSCve14291	CAP1830: "show version" shows old software version as "AP running image" and longer up time
CSCve24687	Channelization issue occurs when Cisco 3802 AP reverts to channel 36 for 75% of APs at a site
CSCve64652	Cisco Access Point 802.11r Fast Transition Denial of Service Vulnerability
CSCve65242	Cisco 702w AP radio resets with reason code 71
CSCvf15991	Client data traffic drops when AAA override and link-local-bridging are enabled due to timing issue
CSCvf27533	Cisco 2800, 3800 AP in a constant reboot loop when wIPS sub-mode is enabled

Table 13 Open Caveats

Caveat ID Number	Description
CSCvf32021	WLC not marking TID in CAPWAP for TSPEC/TCLASS client after roam it is marked
CSCvf65133	Dynamic interface template fails to apply on Cisco WLC with DHCP Option 82 setting
CSCvf66696	Cisco WLC Control & Provisioning of Wireless Access Points Protocol Denial of Service Vulnerability
CSCvf74377	AP3800 Sniffer mode: 802.11 acks, RTS, CTS, QoS Null packets do not get captured
CSCvg27613	DHCP Proxy is enabled and DHCP Server info is removed from the Dynamic Interface, disables the WLAN
CSCvg43654	Cisco Wave 2 APs in FlexConect mode do not forward DHCP NAK to wireless client
CSCvg67509	Cisco 1810W AP reloads unexpectedly over a kernel panic
CSCvh58467	Kernel Panic with PC at skb_release_data+0xe0/0x230
CSCvi51858	WLC not sending proper VSA list at acct-stop when client moves to another SSID
CSCvi73402	Cisco 1810W AP not giving IPs to cell phones using WPA/TKIP protocol
CSCvj38456	WLC is losing its EoGRE configuration after reboot
CSCvj81526	Ciso 1830 AP name became all 0 after "capwap ap erase all"
CSCvj82806	Flex AP loses VLAN mapping if VLAN tagging is enabled. Follow for CSCvc67465 in 8.2 release
CSCvj95336	Cisco Wireless LAN Controller Software Information Disclosure Vulnerability

Resolved Caveats

Table 14 Resolved Caveats

Caveat ID Number	Description
CSCuz17350	Cisco 2800, 3800 APs: XOR Rx-SOP should switch to correct config upon band switch
CSCva66176	AP drop of from Network due to large set of Mobility groups in down/down
CSCva93255	Cisco 1810 AP: unable to upgrade bec Cisco 1810 AP tmp too small for image upgrade
CSCvc07521	Cisco 3800 AP sends A-MSDU larger than client can handle
CSCvc24070	Rx-sop global config to Auto dos not re-set some of the AP to Auto
CSCvc30656	FFT based inter modulation filter
CSCvc89971	Cisco WLC msglog shows AP is being contained on slot 1
CSCvd16380	Cisco 3800 AP detecting DFS false triggers
CSCvd21155	WLC stopped working when multicasting traffic and accessing WLC GUI
CSCvd23185	WGB wired clients not seen by WLC
CSCvd34299	8.5: Cisco 1852, 3800 APs - LAG configuration NOT getting enabled
CSCve33506	WLC fails to reassemble fragmented packet with low MTU
CSCve35938	Dual DFS detection implementation on IOS-based APs
CSCve38191	Duplicated SSID after WLC fallback causes disconnection issues; "ghost" SSID
CSCve57121	Cisco 2800, 3800 and 1560 series APs fail to pass traffic
CSCve57918	WLC IGMP queries not sent consistently
CSCve66630	Clients cannot stay connected to Cisco 2802, 3802 APs SSID with TKIP or TKIP+AES
CSCve70752	SNMP issue: Tx power level returns null causing Cisco PI, WLC sync to not update AP information
CSCve81183	Cisco 2800, 3800 APs - Rx hang in 8.2.154.17 release
CSCve98689	Repeated CDP-4-DUPLEX_MISMATCH is observed when Cisco Wave 2 APs are connected to Cisco switch
CSCvf02705	The IP-SGT binding is removed from SXP peer after a WLC redundancy switchover
CSCvf16302	Flash on lightweight IOS APs gets corrupted
CSCvf17085	The radio of Cisco 3800 series AP stopped working after an image reload
CSCvf22342	Cisco 3800, 2800 AP running 8.2.154.64 release: TxFSM Stuck
CSCvf23975	Cisco 2800 AP radio stays down although CDP negotiated with full power after power cycle
CSCvf25015	AP reloads unexpectedly with ENTROPY-0-ENTROPY_ERROR:unable to collect sufficient entropy
CSCvf28459	Write of the Private File nvram:/lwapp_ap.cfg Failed on compare RCA needed (try = 1)
CSCvf28800	Cisco 2800 AP running 8.2.154.67 release: FIQ reloads unexpectedly due to aptrace

Table 14 Resolved Caveats

Caveat ID Number	Description
CSCvf31881	Cisco 2800 AP detects Intel Dual Band Wireless-AC 8260 as rogue client/AP
CSCvf33154	Wireless to Wireless multicast failure on Cisco 2800, 3800 APs with WPA-PSK-TKIP
CSCvf38379	Cisco 8540, 5520 WLCs does not boot - "System could not find 68xx Nic Card"
CSCvf44583	Cisco 2800, 3800 APs transmitting at MCS/802.11n rates to clients with WMM disabled
CSCvf45989	WLC DP core 0 hung due to RML interrupt handler
CSCvf47017	Cisco 2800, 3800 AP - not able to boot and get stuck "BootROM: Image checksum verification FAILED"
CSCvf52723	IOS AP FlexConnect local switching - client cannot pass traffic when using 802.1X + NAC
CSCvf57360	Cisco Wave2 AP clients constantly deleted with active voice traffic and optimized roaming enabled
CSCvf59621	Cisco 3800, 2800 AP running 8.3.124.40 release: TxFSM Stuck
CSCvf60803	Cisco 2800, 3800 APs: click gets stuck in NBAR timer code
CSCvf66680	Cisco WLC Control And Provisioning of Wireless Access Points Information Disclosure
CSCvf66723	Cisco Wireless LAN Controller Directory Traversal Vulnerability
CSCvf67467	System reloads unexpectedly as Reaper Reset:Task wipsTask taking too much CPU
CSCvf81919	Cisco 3800 AP stops working: selipc causing double free
CSCvf84211	WLC dataplane reloads unexpectedly due to core 0 hung and RML interrupt handling
CSCvf93914	AP 3702 5GHz radio constantly flapping
CSCvg08894	Cisco 3802 AP reloads unexpectedly on Watchdog reset reason: capwapd 8.2.161.0 release
CSCvg20743	The client RSSI/SNR is shown as unavailable when connected to Cisco 2800, 3800 APs
CSCvg40792	Client global IPv6 not correctly mapped to MAC address under certain conditions
CSCvg60758	Cisco Wave 2 APs drops TCP retransmit from server
CSCvg62039	False radar detection on AP 1832 with 40MHz CW
CSCvg83585	APs cannot send NDP Tx on all channels and cant be found as neighbors on nearby APs
CSCvg85651	Management Packets are marked with wrong DSCP
CSCvg87547	AP: Client disconnected due to idle timeout wrongly kicking in when client is going to power save
CSCvg94522	TxFSM stuck on Radio 0 with new signature
CSCvh08020	AP stuck in ap: after upgrade - flashfs[0]: writing to flash handle Illegal Operation
CSCvh21953	Cisco Aironet 1560, 1800, 2800 and 3800 Series Access Point Denial of Service Vulnerability

Table 14 Resolved Caveats

Caveat ID Number	Description
CSCvh23785	AireOS WLC: Multiple wireless clients failing the broadcast Key refresh (M5).
CSCvh47521	Cisco IOS AP shows Decrypt failed messages on driver debug
CSCvh65876	Cisco Wireless LAN Controller Software GUI Privilege Escalation Vulnerability
CSCvh79685	WLC Warning messages DP Packet pool and WQE pool is not normal
CSCvh87451	Cisco 1832 AP Rx not working with AP not responding to probe requests
CSCvi02072	Cisco Wave 2 APs: ETSI 5G adaptive Wi-Fi compliance fix
CSCvi17380	TxFSM stuck on Radio 0 with TCQVerify patch.
CSCvi55973	Cisco 602 AP flapping when 2.4G and 5G radio are disabled, error msg Session ID mismatch
CSCvi90766	Cisco AP with regulatory domain Morocco cannot join the Cisco WLC
CSCvi97023	Cisco Wireless LAN Controller Cross-Site Scripting Vulnerability
CSCvj70569	Cisco 2800, 3800,4800 APs: Incorrect Tx power on power on till we configure Tx power using Cisco WLC

Cisco Mobility Express Solution Release Notes

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 comprises of at least one 802.11ac Wave 2 Cisco Aironet Series access point (AP) with an in-built software-based wireless controller (WLC) managing other APs in the network.

The AP acting as the WLC is referred to as the primary AP while the other APs in the Cisco Mobility Express network, which are managed by this primary AP, are referred to as subordinate APs.

In addition to acting as a WLC, the primary AP also operates as an AP to serve clients along with the subordinate APs.

For more information about the solution, including setup and configuration, see the *Cisco Mobility Express User Guide for Release 8.2*, at:

http://www.cisco.com/c/en/us/td/docs/wireless/access_point/mob_exp/82/user_guide/b_ME_User_Guide_82.html

Supported Cisco Aironet Access Points

APs Supported as Primary (Support Integrated Wireless Controller Capability)	APs Supported as Subordinate
Cisco Aironet 1850 Series Cisco Aironet 1830 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 2600 Series Cisco Aironet 2700 Series Cisco Aironet 3500 Series Cisco Aironet 3600 Series Cisco Aironet 3700 Series

Mobility Express Features

The following features and functionalities are present in this release:

- CLI-based Initial configuration wizard
- Up to three Network Time Protocol (NTP) servers, with support for FQDN names.
- Simple Network Management Protocol (SNMP) version 3 polling, supported via CLI only.
- 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 HTTP for networks containing only AP 1850, AP 1830, or both kinds of access points.

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 500 clients
  - 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).
- Initial configuration wizard.
- Priming at distribution site.
- Default Service Set Identifier (SSID), set from factory. Available for initial provisioning only.
- Management—Through a 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.

Note Cisco 2800 and 3800 APs may experience issues forming RF neighborhood when NDP encryption is turned on in a mix deployment environment.

- 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 (SNMP).
- Management—SSH, Telnet, Admin users.
- Reset to factory defaults.
- Serviceability—Core file and core options, Logging and syslog.
- Cisco Prime Infrastructure.
- Cisco CMX 10.x—Only CMX Presence is supported. CMX Connect, Location and Analytics are not supported.
- 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 Clients
- Voice with Call Admission Control (CAC), with Traffic Specification (TSpec)
- Fast SSID
- 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.
- Updates to the Client View page in the Monitoring Dashboard.
- Client ping test and packet capture.
- Changing the country code on the controller and APs on the network.

- NTP servers for automatically setting the date and time.
- Software update using HTTP.
- CCKM support.

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

Cisco Mobility Express software for Cisco Wireless Release 8.2.170.0, is as follows:

Software Type and purpose	For AP 1850	For AP 1830
Software to be used only for conversion from Unified Wireless Network Lightweight APs software to Cisco Mobility Express software.	AIR-AP1850-K9-8.2.170.0.tar	AIR-AP1830-K9-8.2.170.0.tar
AP software image bundle, to be used for software update, or supported access points images, or both.	AIR-AP1850-K9-ME-8-2-170-0.zip	AIR-AP1830-K9-ME-8-2-170-0.zip
AP software in the bundle	ap1g4	ap1g4

Installing Mobility Express Software

See the “Getting Started” section in the *Mobility Express User Guide* at the following URL:

http://www.cisco.com/c/en/us/td/docs/wireless/access_point/mob_exp/82/user_guide/b_ME_User_Guide_82.html

Caveats

The open caveats applicable to the Cisco Mobility Express solution are listed under the “Caveats” section on page 25. All caveats associated with the Cisco Mobility Express solution have *Cisco Mobility Express* specified in the headline.

Service and Support

For all Support related information, see http://www.cisco.com/c/en/us/support/index.html.

Related Documentation

Cisco Wireless Controller

For more information about the Cisco WLCs, lightweight access points, and mesh access points, 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 User Guide*

  http://www.cisco.com/c/en/us/td/docs/wireless/access_point/mob_exp/82/user_guide/b_ME_User_Guide_82.html

Additional References

- *Cisco Aironet Universal AP Priming and Cisco AirProvision User Guide*

  http://www.cisco.com/c/en/us/td/docs/wireless/access_point/ux-ap/guide/uxap-mobapp-g.html
- *Cisco Aironet Access Points Ordering Guide*

  http://www.cisco.com/c/en/us/products/collateral/wireless/aironet-1830-series-access-points/guide-c07-738528.html

Wireless Products Comparison

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

http://www.cisco.com/c/dam/assets/prod/wireless/cisco-wireless-products-comparison-tool/index.html

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation* at: http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html.

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation, as an RSS feed and deliver content directly to your desktop using a reader application. The RSS feeds are a free service.