Release Notes for Cisco Wireless Controllers and Lightweight Access Points, Cisco Wireless Release 8.2.141.0

First Published: December 08, 2016

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 38.

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

Revision History

Table 1 Release History

Modification Date	Modification Details
January 29, 2018	• Features Not Supported on Cisco Virtual WLCs, page 20 – Modified information about FlexConnect central switching.
October 16, 2017	• Features Not Supported on Cisco Aironet 1810 OEAP, 1810W, 1830, 1850, 2800, and 3800 Series APs, page 22 – Added SIP snooping with FlexConnect in local switching mode
October 10, 2017	• Features Not Supported on Cisco Virtual WLCs, page 20 – Added Wired Guest and FlexConnect central switching.
June 5, 2017	• Open Caveats – Removed CSCvc24200
February 13, 2017	• Open Caveats – Added: CSCvd06463
January 11, 2017	• Features Not Supported on Cisco Aironet 1810 OEAP and 1810W Series APs, page 24 – Added: Local AP Authentication under FlexConnect Features • Features Not Supported on Cisco Aironet 1830 and 1850 Series APs, page 24 – Added: Local AP Authentication under FlexConnect Features
December 12, 2016	• What's New in Release 8.2.141.0, page 4 – Added: Release Information • Guidelines and Limitations, page 6 – Added: Behavior change for WLAN listed

Cisco Wireless Controller and Cisco Lightweight Access Point Platforms

The section contains the following subsections:

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 8.2.141.0, 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 8.2.141.0

Release 8.2.141.0 places emphasis on improvements of features ranging from device stability, QoS handling, performance improvement for 802.11ac client interoperability, IEEE 802.11h behavior selection, and other access point-related enhancements on Cisco Aironet 2800 Series, Cisco Aironet 3800 Series, and other Cisco 802.11ac Wave 2 access points.

Command to Configure Smart DFS

config 802.11h smart-dfs {enable | disable}

enable	Enables non occupancy time doubling for Radar interfere channel.
disable	Disables non occupancy time doubling and use legacy time (30 minutes) for Radar interference channel.

For information about this command, see Cisco Wireless Controller Command Reference.

There are no new features introduced in this release. For more information about updates in this release, see the "Caveats" section on page 24.

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 to Cisco WLC Software Release 8.2.x

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 8.2.141.0 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 8.2.141.0, 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 8.2.141.0.

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 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 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

Table 4 FUS Upgrade Guidance

WLC Controller Model	Recommended FUS Version
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 8.2.141.0 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 8.2.141.0. Table 5 shows the upgrade path that you must follow before downloading Release 8.2.141.0.

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 8.2.141.0.

- 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 8.2.141.0. 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 8.2.141.0 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 8.2.141.0 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 8.2.141.0 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 8.2.141.0 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 8.2.141.0 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 to Cisco WLC Software Release 8.2.x" section on page 6.

Interoperability with Other Clients

This section describes the interoperability of Cisco WLC Software, Release 8.2.141.0 with other client devices.

Table 6 Test Bed Configuration for Interoperability

Hardware/Software Parameter	Hardware/Software Configuration Type
Release	8.2.141.0
Cisco WLC	Cisco 55xx Series Controller
Access points	2802, 3702, 3802
Radio	802.11ac, 802.11a, 802.11g, 802.11n2, 802.11n5
Security	Open, WEP, PSK (WPA and WPA2), 802.1X (WPA-TKIP and WPA2-AES) (LEAP, PEAP, EAP-FAST, EAP-TLS)

Table 6 Test Bed Configuration for Interoperability (continued)

RADIUS	ACS 5.2, 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 10.11.6
MacBook Air old	OSX 10.11.5
MacBook Air new	OSX 10.11.5
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
Apple iPad2	iOS 10
Apple iPad3	iOS 10
Apple iPad mini with Retina display	iOS 10

Table 8 Tablet Client Type List

Client Type and Name	Version
Apple iPad Air	iOS 10
Apple iPad Air 2	iOS 10
Apple iPad Pro	iOS 10
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 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
Google Nexus 9	Android 6.0.1
Symbol MC9090	Windows Mobile 5.1.478 (Build 15706.3.5.2)
Symbol MC70	Windows Mobile 05.01.0476

Phones and Printers.

Table 9 Phone and Printer Client Type List

Client Type and Name	Version
Cisco 7921G	1.4.5.3.LOADS
Cisco 7925G	1.4.5.3.LOADS
Cisco 8861	Sip88xx.10-2-1-16
Cisco-9971	Sip88xx.10-2-1-16
Apple iPhone 4S	iOS 10
Apple iPhone 5	iOS 10
Apple iPhone 5c	iOS 10
Apple iPhone 5s	iOS 10
Apple iPhone 6	iOS 10
Apple iPhone 6 Plus	iOS 10
Apple iPhone 6s	iOS 10
HTC One	Android 5.0
OnePlusOne	Android 4.3
Google Nexus 5	Android 6.0.1
Huawei Ascend P7	Android 4.4.2
LG G4	Android 5.1
Nokia Lumia 1520	Windows Phone 8.10.14219.341

Table 9 Phone and Printer Client Type List

Client Type and Name	Version
Samsung Galaxy S4 – GT-I9500	Android 5.0.1
Samsung Galaxy S5-SM-G900A	Android 4.4.2
Samsung Galaxy S III	Android 4.3
Samsung Galaxy Nexus GTI9200	Android 4.4.2
Samsung Galaxy Mega SM900	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
Canon Printer	4
HP Printer (K7C858, 5540)	NBP1CN1531AR
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:

- Features Not Supported on Cisco 2504 WLC, page 18
- Features Not Supported on Cisco WiSM2 and Cisco 5508 WLC, page 19
- Features Not Supported on Cisco Flex 7510 WLCs, page 19
- Features Not Supported on Cisco 5520, 8510, and 8540 WLCs, page 20
- Features Not Supported on Cisco Virtual WLCs, page 20
- Features Not Supported on Mesh Networks, page 24

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 21

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	• Encryption – Temporal Key Integrity Protocol (TKIP) • Locally Significant Certificate (LSC) • TrustSec SXP • CKIP, CMIC, and LEAP with Dynamic WEP • Static WEP key for TKIP or CKIP [1]
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) • Bidirectional rate-limiting • Link aggregation (LAG) • 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 • Split tunnels • PPPoE • SIP snooping with FlexConnect in local switching mode

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

Note For Cisco Aironet1850 Series AP technical specifications with details on currently supported features, see the *Cisco Aironet 1850 Series Access Points Data Sheet*.

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	• 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 for Release 8.2.141.0

Caveat ID Number	Description
CSCur68316	Cisco 802-891 AP: when in FlexConnect mode lose VLAN mapping after a power cycle
CSCuu21625	Session does not get cleared on Cisco 5508 WLC anchor with Cisco Catalyst 3850 switch foreign causing authentication issues
CSCuu49801	Country Code issue with AE, AL
CSCuu6396ios4	Apple clients cannot reconnect to Cisco 1850i AP on forceful deauthentication
CSCuw41092	AP not send traffic indication in beacon for power-save client after FT
CSCuw95402	SNMP not returning correct information for roaming client
CSCux06806	Cisco AirTime Fairness EnforcementConfig for network radio is not pushed to the uploaded configuration
CSCux23710	Cisco IW3702: LED status behavior inconsistent with CCO user guide
CSCux28505	Cisco 8510 WLC reloads unexpectedly on “fp_main_task” in the 8_2_1_124 image
CSCux42874	Management Frame Protection (MFP): Mobility Agent (MA) dropped key request from Mobility Controller (MC)
CSCux48308	Broadcast delivery stops with key rotation on Cisco 1552 root access point (RAP) and Cisco 819W AP running 153.3JBB5 WGB
CSCux56652	Local profile shows wrong statistics and percentage information
CSCux59359	Guest clients associated with foreign Cisco 8510 WLC behind NAT on new mobility is stuck on DHCP_REQD state
CSCux77970	AAA override uplink rate limit values are not getting reflected in web-authentication
CSCux78581	Multiple clients are not supported on LAN ports of Cisco 1810 APs

Table 13 Open Caveats for Release (continued)8.2.141.0

Caveat ID Number	Description
CSCux88967	On MAC filter failure client session timeout can not associate back
CSCuy26870	In ME-Controller GUI, incorrect Tx Power Range is displayed
CSCuy74931	Override 802.1x supplicant credentials lost after reboot
CSCuy87193	Cisco WLC reloads unexpectedly (due to EmWeb) when adding 1500+ local net users
CSCuy91177	Client MSCB removed on Optimized Roam
CSCuz03702	New mobility: wired client behind WGB fails to pass traffic after roaming
CSCuz11374	WLC: selects wrong DHCP relay even though configured on the interface
CSCuz11717	3-sec delay before sending “dot1x auth initiate” to SPAM with WSSI
CSCuz18799	Cisco 2800, 3800 APs send VHT SGI frames to STA that does not support SGI
CSCuz18869	WLC picking up the unicast DHCP for unknown destination
CSCuz22198	Slient reload on Cisco 5508 WLC with %OSAPI-0-TIMER_CREATE_FAILED: timerlib.c
CSCuz27736	Cisco 3800 AP on Flex- AP sends deauthentication after FT roam (Freq- 3-4%)
CSCuz29774	Cisco 1852 APs losing connectivity to ME controller with AVC enabled
CSCuz33090	Cisco 3802 AP - antennas supported is always 4 in VHT Capabilities IE
CSCuz33818	Profiler database is full and Cisco WLC clears the entry twice
CSCuz45986	CWA not working on Cisco 8500 WLC as Guest Anchor with accounting enabled
CSCuz46892	ME: external AP rebooted because it detected another ME controller
CSCuz49685	Cisco 1810 OEAP SNMP: Not seeing error when trying to disable Port3
CSCuz49804	Fix AID leak problems
CSCuz50774	Cisco WLC lossing pings to itself, Reaper cleaning up exited task osapi_ping_rx
CSCuz65017	Cisco 3800 AP not updating HT Op Mode bits in the presence of legacy AP
CSCuz65175	Cisco 1852 ME: HTTP profiling causes CPU spikes and degraded performance

Table 13 Open Caveats for Release (continued)8.2.141.0

Caveat ID Number	Description
CSCuz67292	Client not moving to RUN state after CAS perform posturing on client
CSCuz68479	Cisco 3800 AP not reassembling wireless fragmented frames
CSCuz69729	802.11ac WGB does not associate with root channel width 40 MHz above or below
CSCuz78490	DHCP:usage indicator will not show 100% usage even if all IP's are in use
CSCuz88573	Unexpected reload in emWeb
CSCuz90785	Cisco release 8.2MR1:traffic black hole WEP errors on Cisco IW3702 WGB during roaming mesh
CSCva00087	Cisco WLC reloads unexpectedly on apfVerifyCountryString spamApTask2
CSCva01762	Cisco 1815/50 AP: Over-ride global credentials cleared on GUI after reboot
CSCva03376	Cisco UX-AP3702i after primed carrier set 5-GHz only allowing four UNII3 ch
CSCva07048	Cisco WLC DP reloads unexpectedly with wqe stuck
CSCva07307	Voice tagged frames drop at AP radio after upgrade to Cisco 8.2 and later releases
CSCva16449	Cisco AIR-CAP1552 not showing temprature on WLC running Cisco 8.2 release
CSCva22440	Cisco 3800 AP: QBSS STA Count keeps incrementing with STA associating again
CSCva25999	Rate limit not followed as per QoS role defined for the guest user
CSCva26117	NAT translation o/p for locally switched traffic not observed in AP
CSCva27276	Cisco 2802 AP: local profiling detects windows client as Microsoft-Workstation
CSCva27419	Channel changed trap with Unknown Radio Type on dual band radio
CSCva27711	Cisco FlexConnect: AP radio reset during FT when Central DHCP is enabled WLAN
CSCva28211	AireOS UX AP : country code 'JP' should be used as world mode in beacon and probe res
CSCva28524	Cisco WLC running on 8.3 release: creating SNMP community fails
CSCva29463	Cisco 2800, 3800 AP: WLAN client fails >=1500 bytes ICMP traffic in standalone mode

Table 13 Open Caveats for Release (continued)8.2.141.0

Caveat ID Number	Description
CSCva29554	ClickOS: FlexConnect AAA overridden ACL is not plumbed in the WLC
CSCva31178	Cisco AP running 8.3 release: radio reset due to off-channel stuck
CSCva31890	MIB table bsnMobileStationPerRadioPerVapTable has no data
CSCva40580	Cisco 8.3 release: BulkSync on active WLC never completes and is stuck in 'in-progress'
CSCva42290	No QoS map set or WNM Notification bit in Ext. Cap. IE in association response
CSCva43211	ME: Unable to import configuration file as other AP is becoming the primary
CSCva48201	Unable to set static IP for AP from controller GUI
CSCva51719	ME: Mismatch QoS profile priority in Cisco 1850
CSCva52825	Cisco 2800, 3800 APs: do not do PMTU discovery during join or image download
CSCva52938	Cisco 2800, 3800 APs reporting incorrect CDP info to the switch
CSCva53980	Issue in Cisco CleanAir when client serving band is 5-GHz
CSCva55165	IPv6 MLD from PMIPv6 client show client MAC on layer3/2 switch
CSCva63541	Cisco 2800, 3800 AP CAPWAP restarts continuously during FTP transfer of large file
CSCva65643	Cisco WLC reports load profile failed but clients connected under threshold
CSCva66176	Cisco AP drop off from the network due to large set of Mobility groups in down/down
CSCva71002	WLC GUI client filter fails with spaces used in the client name
CSCva72724	Cisco 2602 AP reloads unexpectedly due to disc_tx_requeue_client dot11_get_rate_shift
CSCva74487	Cisco 8540 WLC reloads unexpectedly on running show commands task :emWeb
CSCva74927	Cisco 2800, 3800 APs in Flex mode- AP disconnects with 'Failed to get ARP entry for WLC' error
CSCva83884	Cisco WLC system reloads unexpectedly on aaaQueueReader
CSCva87295	Cisco Flex AP radio reset during FT with Central DHCP and NAT-PAT enabled
CSCva90343	Unable to do VLAN to RLAN mapping at FlexConnect Group

Table 13 Open Caveats for Release (continued)8.2.141.0

Caveat ID Number	Description
CSCva90917	Cisco 1560 AP does not hold multicast data for given DTIM count
CSCva95251	DSCP traffic is not limited to maximum QoS Profile value
CSCva99864	EAP-TLS fails with Windows and ME using “Smart card or certificate” authentication
CSCvb02180	ARP table full, unable to delete ARP mapping IP
CSCvb05067	Local EAP fails after wrong username login
CSCvb09381	Unable to add or modify SNMP strings on a Cisco 5520 WLC HA pair running 8.1.122.0 release
CSCvb18640	Mobility Express: manual channel-widths overwritten by DCA
CSCvb19483	Cisco 1850 ME unable to download login-banner
CSCvb22856	AP kernel panic: Cisco 1810W AP reloads unexpectedly with no cores
CSCvb23576	Excluded clients can connect to Cisco 2800 APs in Cisco FlexConnect local switching
CSCvb28231	Cisco controller reloads unexpectedly due to memory corruption
CSCvb29996	Cisco 1810W AP hardware watchdog reloads unexpectedly PC=0xc03b3ffc, LR=0xc008af24
CSCvb31857	Cisco WLC rejects client association with 802.11k assisted roaming on Cisco 2800 AP with dual 5-GHz
CSCvb35173	Cisco 2800, 3800 APs radio reloads unexpectedly
CSCvb36432	SSIDs vanishes from standalone AP after reboot
CSCvb43105	Cisco 2800, 3800 APs: outer DSCP not same as inner with DSCP Trust upstream NSS
CSCvb44699	NMSP queue full due to rouge AP task
CSCvb48603	Evaluation of Cisco WLC for OpenSSLSeptember 2016
CSCvb49804	Cisco AP does not forward frames to some STAs under high traffic
CSCvb52310	Silent Boot on Cisco 2800, 3800 APs
CSCvb54166	Malformed 802.11v element on HSR WGB with WLC running Cisco 8.2+ release software
CSCvb64560	CISCO-LWAPP-AAA-MIB: DEFVAL format incorrect for some objects
CSCvb69962	Client traps not showing session ID
CSCvb72367	Transfer upload data type run-config is missing several config sections

Table 13 Open Caveats for Release (continued)8.2.141.0

Caveat ID Number	Description
CSCvb81359	Cisco 8540 WLC HA: RMI ping and access to standby fail when using non-default ap-manager
CSCvb89227	For last ap connection failure reason: messages not getting properly on join statistics
CSCvb89781	Cisco 2700-B AP unable to join WLC: Unable to create temp dir “flash:/update”
CSCvb90403	Cisco 1810W AP hardware watchdog reset at PC= 0xc03b3ffc, LR= 0xc011e2dc
CSCvb90793	AP name unknown in SNMP bsnDot11StationDeauthenticate traps
CSCvb91652	PMIPv6 sluggish CLI or GUI response as well as sporadic lack of SNMP response
CSCvb91832	Cisco 1810W AP radio firmware reloads unexpectedly at 0x009C30A0, QCA 02677365
CSCvb91836	Cisco 1810W AP watchdog resets unexpectedly (wcpd no heartbeat)
CSCvb94610	Restore command to disable GARP
CSCvb97775	Cisco 3802 AP watchdog resets unexpectedly (CAPWAPd)
CSCvb99751	AP kernel panic: Cisco 2800 reloads unexpectedly on No PC, LR is at skb_free_head+0x7c/0x88
CSCvc00328	Cisco 3800 AP: Microsoft Surface Pro gives less throughput
CSCvc00358	Cisco WLC reloads unexpectedly on “apfRogueTask_0” missing software watchdog
CSCvc06628	Cisco 1552C AP: d0 radio reset due to beacon Stuck or Tx jammed
CSCvc06762	Cisco 3800AP: WGB/WGB wired client join fails for radioB with inter-ssid roaming
CSCvc09805	Cisco WLC running 8.2 release: WLC rejects client association even when only 1 AP broadcasting SSID & multiple client attempts
CSCvc09807	Cisco 1810W AP: noticing AP not ACKing some EAP frames intermittently
CSCvc10831	Cisco 1852 AP - automatic TFTP of AP core dump fails
CSCvc10906	Cisco 1810 OEAP lose association to WLC after configuration update
CSCvc12513	Polaris-XOR in Cisco 2800, 3800 APs: DBS max width is not working; DCA width is not getting applied
CSCvc12703	Cisco 1810W AP LAN port 2 maps to wrong VLAN on N+1 failover to Primary
CSCvc13082	Cisco 2800, 3800 APs: 5-GHz radio reloads unexpectedly due to Rx-HANG detected

Table 13 Open Caveats for Release (continued)8.2.141.0

Caveat ID Number	Description
CSCvc13868	802.11ac APs reset to 80 MHz during migration or failover
CSCvc14508	Cisco 3800 AP reloads unexpectedly with watchdog reset on 8.2.130.0 release
CSCvc15149	Cisco 2800, 3800 APs running on 8.2 MR4 release - not beaconing a SSID when it is in an AP group and SSID enabled later
CSCvc17272	APs beaconing in 2.4 GHz when the WLAN is configured for 5 GHz
CSCvc18699	Cisco 1850 AP running 8.2.131.40 release: high pings drops, traffic connectivity drop seen
CSCvc18705	Cisco 1850 AP getting stuck in unexpected reload loop after executing reload command from CLI. QCA 02706497
CSCvc18720	Radio 0 not beaconing after radar detection on active channel and moved to non-dfs channel
CSCvc20632	Cisco 1810 AP reloads unexpectedly at CAPWAPd
CSCvc24179	Kernel panic - not syncing: Out of memory: compulsory panic_on_oom is enabled
CSCvc24687	Cisco 2800, 3800 APs running 8.2.131.47 release - kernel panic
CSCvc25128	Cisco 1850 APs client joins in expected radio with delay when band steering is enabled on Cisco WLAN
CSCvc25693	AP1850: observed multiple AP flaps /watchdog reset (CAPWAPd)
CSCvc25827	Cisco 2800, 3800 APs reloads unexpectedly during bi-directional traffic in dual MAC client long run in flex mode
CSCvc26521	Cisco 1850 AP: During continuous configuration change, AP reboots with a coredump, QCA 02717759
CSCvc28168	WLC set ZERO 802.11e QoS UP for part of the downstream voice packets and APs trust it
CSCvc30561	COS AP's clients cannot subscribe to multicast stream after a while
CSCvc31133	Unable to enable WLAN with enabled selected option in GUI
CSCvc32046	Cisco 1810 AP radio reloads unexpectedly under clients storm scenario @0x0098083D, QCA 02706243
CSCvc32339	Cisco AP falls into u-boot mode under normal operation
CSCvc32590	Cisco 2802 AP with Pakistan (G) regulatory domain fails to join the controller
CSCvc32706	Cisco 3800 APs: Not seeing all COS neighbors

Table 13 Open Caveats for Release (continued)8.2.141.0

Caveat ID Number	Description
CSCvc32856	Cisco 2800, 3800 APs send a AQ Event as soon as RRM changes channel causing bad channel selection and changes
CSCvc33968	Cisco WLC- SNMP set fails: resourceUnavailable (This is likely a out-of-memory failure within the agent)
CSCvc34897	Cisco 2800, 3800 APs do not ACK client's EAP packets intermittently. Client fail to connect or takes longer
CSCvc36010	Cisco 3700 AP running 8.2 MR4 image: reloads unexpectedly due to 'LWAPP Rogue Monitoring process'
CSCvc40852	Active controller in HA pair shows different socket errors
CSCvd06463	IOS AP doing AMSDU aggregation for voice traffic in queue 0 despite BA request declined by Cisco Wireless IP Phone 8821

Resolved Caveats

Table 14 Resolved Caveats for Release 8.2.141.0

Caveat ID Number	Description
CSCuw97966	10G Link down after reboot on WLC8510 on Nexus 5k
CSCux21803	Client not receiving broadcast ARP request after AP failover
CSCuy70039	WLC should not forward DHCPINFORM when client is in DHCP_REQD
CSCuy84275	Issue with Wi-Fi-calling and ms-services recognition with Protocol Pack 15 with Engine23
CSCuz15637	Aggregation not working with Cisco 1852 AP and Intel 7265, QCA 02677308
CSCuz17680	WLC reloads unexpectedly after enabling the enhanced client traps
CSCuz45296	WLC sends account update multiple times in the same millisecond
CSCuz71319	Cisco 7500 WLC reloads unexpectedly when browsing Flex AVC stats
CSCuz74051	ME: WGB associate failed with IOS AP
CSCuz84473	Cisco 3600 AP: clients join with AP in admin down state
CSCuz89745	HA has continuously reloads unexpectedly on Taskname: iappSocketTask

Table 14 Resolved Caveats for Release 8.2.141.0 (continued)

Caveat ID Number	Description
CSCuz94683	Cisco 2800, 3800 APs: NSS API failures during overnight run
CSCuz97248	ME - Client unable to ping default gateway after getting IP
CSCva02176	Cisco 1800, 2800, 3800 AP sends deauthentication frame instead of disassociation for disassociation Imminent
CSCva12055	Link down after reboot on Cisco 8540 and 5520 WLCs
CSCva20321	Radio go stop-on-failure and the LAP cannot re-join to Cisco WLC for a while
CSCva27809	Cisco 1850 AP reboots when joining the WLC from standalone mode (VAP start failure)
CSCva27977	Cisco 2800, 3800 APs on flex mode Multicast not working for fresh WLANs
CSCva30302	Cisco Mesh APs running 8.1 release reloads unexpectedly when you add allowed VLANs to the MAP
CSCva35509	Incorrect rates reported in Cisco 1572 AP MA and RAP deployment
CSCva36161	Cisco 1600 series AP reloads unexpectedly after client trying to connect to disabled SSID
CSCva56521	Cisco 1600 AP false DFS detection
CSCva63310	Unable to enable mode Trunk on mesh mode AP with Cisco WLC on 8.2 code
CSCva65826	Wireless LAN Controller reboots unexpectedly
CSCva66595	Cisco 2800, 3800 APs: New bootloader auto-upgrade
CSCva76982	Need a command to disable DFS Blacklist Time Doubling
CSCva83393	Cisco 2800, 3800 APs: reloads unexpectedly and console goes into hung state
CSCva85198	Cisco ME, 1810: CAPWAP DTLS teardown state after image upgrade
CSCva90980	EoGRE high ping latency, SNMP polling fails
CSCva91922	Cisco 1800, 2800, 3800 APs- PoE status on WLC shows Power injector when powered via PoE
CSCva92053	Cisco 2800, 3800 APs: kernel reloads unexpectedly because of Kmalloc called with GFP_KERNEL Flag
CSCvb02220	Cisco 2800, 3800 APs: clients get IP via management interface instead of dynamic interface
CSCvb02472	Controller reloads unexpectedly on radiusTransportThread, memory corruption
CSCvb06740	Cisco 2800, 3800 APs: show version missing bootloader version
CSCvb12066	Cisco Flex - VLAN support does not get automatically added

Table 14 Resolved Caveats for Release 8.2.141.0 (continued)

Caveat ID Number	Description
CSCvb13455	Cisco WLC is not snooped by sub._apple-mobdev2._tcp.local
CSCvb18339	DTLS connection failed because max control DTLS connections reached
CSCvb18565	Cisco 2800, 3800 APs: delay forwarding packets from Radio to LAN
CSCvb21385	Compatibility issues with Internet Explorer 11 and WLC New GUI
CSCvb22629	Cisco 3802 AP longevity radio stop or start test causes BUG: spinlock lockup
CSCvb25999	Cisco 2800, 3800 APs: RF domain name parse error
CSCvb29483	SNMP traps are not sent to the receiver
CSCvb30105	Cisco 1852 AP - CAPWAPd reloads unexpectedly due to DTLS segmentation error
CSCvb32659	Syslog message for DP_BUFFER_POOL_EARLY_WARNING
CSCvb33101	Cisco 702w AP ethernet stop passing traffic
CSCvb33401	Cisco 2800, 3800 APs: reloads unexpectedly due to kernel panic in 8.2.121.14 release
CSCvb33406	Cisco 2800, 3800 APs: reloads unexpectedly due to wcpd in 8.2.121.14 release
CSCvb34951	Cisco WLC not sending AP up/down trap
CSCvb35018	Cisco WiSM2 reloads unexpectedly with task mdnsHATask
CSCvb35053	Cisco 2802E AP reloads unexpectedly due to kernel panic
CSCvb35815	High CPU in Cisco 2504 AP with directly connected AP on upgrade to Cisco 8.2 or 8.3 release software
CSCvb36119	Cisco 3800 AP does not do 80 MHz data rates with WGB clients
CSCvb38281	Cisco 2800, 3800 APs: does not allow printer traffic after association
CSCvb38831	Cisco 702w AP reloads unexpectedly during Multicast receive path
CSCvb38912	Cisco Flex ACL does not get applied when client roams in ‘CENTRAL_WEB_AUTH’
CSCvb43169	Cisco 2800, 3800 APs: not doing soft reset if RADAR is detected with in CAC period
CSCvb44311	SKB Double free kernel panic reloads Cisco 2800, 3800 APs unexpectedly possibly from click[ME_2K:PC is at consme_skb+0x14/0x140]
CSCvb47025	Cisco 1832I AP: Beacons stuck, QCA 02635653

Table 14 Resolved Caveats for Release 8.2.141.0 (continued)

Caveat ID Number	Description
CSCvb49111	Cisco 2800, 3800 AP kernel panic: unexpectedly reloads due to MVL radio statistics in 8.2.124.15 release
CSCvb50962	Cisco 2800, 3800 APs radio interface dropping wireless client data traffic
CSCvb53368	Validate rogue clients against AAA not working
CSCvb54036	Cisco 2800, 3800 APs: beacons stuck
CSCvb55698	Cisco 2800 AP - Rx hang for 2.4-GHz
CSCvb55993	Cisco 18xx APs: switching SSID on same AP fails due to AP sending INTER_VAP_ROAM, so WLC delayed by 10 seconds
CSCvb56598	Client associating to FlexConnect WLAN recieve irrelevant VLAN's ARP
CSCvb58173	Cisco 2800, 3800 APs: watchdog reset due to gateway
CSCvb59058	Cisco 1850 AP: DFS false in ETSI domain 40/80 MHz
CSCvb59734	AP sending incorrect information about ciphers configured in WLAN
CSCvb60500	Cisco 2800 AP kernel panic: system reloads unexpectedly because of memory corruption, SKB_Consume
CSCvb60972	ME - channel and width could not change using GUI
CSCvb61259	Cisco 2800, 3800 APs running 8.2 MR3 release: sending incorrect Flex AID causing client disconnect
CSCvb62478	WLAN is allowed to be enabled when FT enabled without FT-psk/FT-802.1x
CSCvb64452	Cisco 1800, 2800, 3800 APs- DTLS not tear down when PWRINJ failure
CSCvb64912	Packet retries command gets changed after reboot in Cisco 1532AP
CSCvb65617	Cisco CleanAir Slot 1 down events in Cisco 3800 AP
CSCvb65706	Cisco AP reloads unexpectedly in a loop due to "AP image integrity check FAILED"!
CSCvb67633	Cisco 3800 AP upstream issue with 80 MHz data rates with WGB clients
CSCvb67909	Cisco 2800, 3800 AP: if connect to Cisco 3560 CX switch, the AP is unable to boot kernel
CSCvb68541	Cisco 1850 AP reloads unexpectedly on radio failure (firmware) at 0x00990C98, QCA 02653512
CSCvb70134	Cisco 1810W AP radio firmware reloads unexpectedly on [02] 0x0098160C, QCA 02653531
CSCvb71494	Cisco 2800, 3800 APs ICMP test failing

Table 14 Resolved Caveats for Release 8.2.141.0 (continued)

Caveat ID Number	Description
CSCvb71797	Cisco 1810W AP radio firmware reloads unexpectedly on [02]:0x00989C62, QCA 02653521
CSCvb71928	Device reloads unexpectedly during loading FlexConnect configuration
CSCvb71964	Cisco 1810W AP reloads unexpectedly on radio firmware assert @0x000CEBB1 and 0x00980AB2, QCA 02657120
CSCvb72084	Cisco 8.2.121.11, 8.2.124.15 release: unexpected reload fatal condition at broffu_fp_dapi_cmd.c
CSCvb73404	Cisco 1810W AP radio firmware reloads unexpectedly on [02] 0x009807D9, QCA 02655868
CSCvb73540	Cisco 1810 AP firmware reloads unexpectedly on radio 0 @0x0098E38C, QCA 02658721
CSCvb73745	Cisco 2800, 3800 AP: wcpd reloads unexpectedly in wcp MVL driver
CSCvb75093	Cisco 2800, 3800 AP: measured Tx power out does not exceed 6 dBm per-path
CSCvb75564	Cisco 1852 AP beacon at 6M when its disabled, lowest mandatory rate is 12M, QCA 02675818
CSCvb75590	Cisco 1810W AP: radio1 firmware unexpectedly reloads @0x009A477D
CSCvb78906	Invalid logs about “Subnet mismatches while registering IP address”
CSCvb82264	Cisco 1552C AP radio disabled due to beacon stuck with stop-on-fail
CSCvb82735	Cisco 2800 AP: Internal AP reloads unexpectedly at ZN16CapwapFragmenter14frag_iter_openEP1PRNS
CSCvb83097	Cisco 1800, 2800, 3800 AP does not apply the 802.11p tag
CSCvb83517	Cisco 1810W AP LAN ports not forwarding IGMPv2 traffic
CSCvb86711	Cisco 2800, 3800 AP running 8.2.131.18 release: kernel panic when PC is at eth_type_trans”
CSCvb87315	Cisco 2800, 3800 AP: ERP IE is missing in beacons for 802.11g only SSID
CSCvb89745	Cisco 1810 AP: radio unexpected failure due to firmware at 0x009A46D9, QCA 02674060
CSCvb90247	Cisco 8.3 running on Cisco 1815: multicast to multicast video stream is bad
CSCvb90308	Continuous message on ap console: wlChkAdapter FALSE regval = ffffffff
CSCvb90324	Cisco 1800 AP SSH disabled after few mode changes
CSCvb91826	Cisco 1810W AP watchdog reset wcpd on Cisco 8.2.130.0 release

Table 14 Resolved Caveats for Release 8.2.141.0 (continued)

Caveat ID Number	Description
CSCvb91881	Cisco 2800, 3800 AP: deauthenticating (class3) the connected clients
CSCvb96077	Cisco 2800, 3800 AP: sometimes does not send authentication response
CSCvb97562	Cisco 2800, 3800 AP: IP reassembler failing for fragmented packets causing connectivity failures
CSCvc01923	Cisco 2800, 3800 AP: RTS frames sent at hardcoded 6 Mbps instead of minimum mandatory rate
CSCvc05515	Cisco 3802 AP reloads unexpectedly in flex or local mode oom-killer: gfp_mask=0x2040d0, order=0, oom_score_adj=0
CSCvc07159	Cisco 2800, 3800 AP: low throughput in 40 MHz as association response is sent at 20 MHz
CSCvc07374	Cisco 2800, 3800 APs: radio down due to Cisco Cleanair off channel stuck
CSCvc10919	Cisco WLC Loaded EoGRE pulls CAPWAP traffic under slow path, brings down performance
CSCvc17019	Cisco 2800, 3800 APs running 8.2.131.40 release: Rx hang on radio 1
CSCvc19125	Cisco 1810 AP radio reloads unexpectedly on @0x9433A0 in 8.2.130.0, QCA 2689921
CSCvc20813	Cisco 2800, 3800 APs running 8.2 MR4 release - after trying configure change on the WLAN, clients not able to join some APs
CSCvc22291	Cisco WLC keeping some Cisco 2800, 3800 in 20 MHz when 40 MHz is selected in the RF profile
CSCvc24165	Cisco AP reloads unexpectedly due to kernel panic at mhsm_transition in ap8x driver

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 provides a wireless LAN controller functionality bundled into, the Cisco Aironet 1850 and 1830 Series APs currently. This functionality provides a simplified Wi-Fi architecture with limited enterprise-level WLAN capability to small and medium deployments.

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

The primary AP operates as a wireless LAN 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 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 Client
- 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.

New Features and Functionalities

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

- 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 8.2.141.0, is as follows:

Software Pype 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-K9-8.2.141.0.tar	AIR-AP1830-K9-8.2.141.0.tar
AP software image bundle, to be used for software update, or supported access points images, or both.	AIR-AP1850-K9-ME-8-2-100-0.zip	AIR-AP1830-K9-ME-8-2-100-0.zip

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 24. All caveats associated with the Cisco Mobility Express solution have *Cisco Mobility Express* specified in the headline.

Related Documentation

- 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

- 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

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/83/user_guide/b_ME_User_Guide_83.html
- *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

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.