



# Release Notes for Cisco Wireless Controllers and Lightweight Access Points, Cisco Wireless Release 8.2.151.0

---

**First Published: March 15, 2017**

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**      **Revision History**

Modification Date	Modification Details
January 29, 2018	<ul style="list-style-type: none"> <li>• <a href="#">Features Not Supported on Cisco Virtual WLCs, page 22</a> <ul style="list-style-type: none"> <li>– Modified information about FlexConnect central switching.</li> </ul> </li> </ul>
October 16, 2017	<ul style="list-style-type: none"> <li>• <a href="#">Features Not Supported on Cisco Aironet 1810 OEAP, 1810W, 1830, 1850, 2800, and 3800 Series APs, page 24</a> <ul style="list-style-type: none"> <li>– Added SIP snooping with FlexConnect in local switching mode</li> </ul> </li> </ul>
October 10, 2017	<ul style="list-style-type: none"> <li>• <a href="#">Features Not Supported on Cisco Virtual WLCs, page 22</a> <ul style="list-style-type: none"> <li>– Added Wired Guest and FlexConnect central switching.</li> </ul> </li> </ul>
April 19, 2017	<ul style="list-style-type: none"> <li>• <a href="#">Resolved Caveats, page 32</a> <ul style="list-style-type: none"> <li>– Added <a href="#">CSCvc32590</a> and <a href="#">CSCvc87146</a>.</li> </ul> </li> </ul>
April 10, 2017	<ul style="list-style-type: none"> <li>• <a href="#">What's New in this Release, page 4</a> <ul style="list-style-type: none"> <li>– Added information about change in functionality of CPU ACL.</li> </ul> </li> </ul>

## 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 19](#).

## 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 8.2.151.0, 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 22.



**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 this Release

- [Temporal Key Integrity Protocol \(TKIP\) Support, page 4](#)
- [Change in Functionality of CPU ACL, page 5](#)

## Temporal Key Integrity Protocol (TKIP) Support

The TKIP security protocol option support is now extended to the following Cisco APs:

- Cisco Aironet 1810 Series APs
- Cisco Aironet 1830 Series APs
- Cisco Aironet 1850 Series APs
- Cisco Aironet 2800 Series APs
- Cisco Aironet 3800 Series APs

The following supported TKIP security protocol combination table is applicable to the above listed Cisco Wave2 APs only. The legacy APs continue to support the protocols without any change in this release.

**Table 2** *Supported TKIP Security Protocol Combination for Cisco Wave2 APs in Release 8.2.151.0*

AP Mode	Authentication Owner	State	Policy	Supported
Local	NA	NA	WPA TKIP/802.1x	Yes
Local	NA	NA	WPA TKIP/PSK	Yes
FlexConnect	Central Authentication	Connected	WPA TKIP/802.1x	Yes
FlexConnect	Central Authentication	Connected	WPA TKIP/PSK	Yes
FlexConnect	Local Authentication	Connected	WPA TKIP/802.1x	No
FlexConnect	Local Authentication	Connected	WPA TKIP/PSK	Yes
FlexConnect	Local Authentication	Standalone	WPA TKIP/802.1x	No
FlexConnect	Local Authentication	Standalone	WPA TKIP/PSK	Yes
Any	Any	Any	WPA2 TKIP/Any	No

For more information about this feature, see [WPA1 and WPA2](#) section in the *Cisco Wireless Controller Configuration Guide*.

## Change in Functionality of CPU ACL

The functionality of CPU ACL is changed as follows:

- Prior to this release: A permit statement in one direction (from client to Cisco WLC) also permitted traffic in the return direction (from Cisco WLC to client).
- From this release: CPU must be changed to have explicit permit statements in both the directions.

# Software Release Types and Recommendations

**Table 3** 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. <sup>1</sup>  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 4 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.		

**Table 4 Platform Support for Global Multicast and Multicast Mode (continued)**

Platform	Global Multicast	Multicast Mode	Support
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:

- 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)
```

- After the reboot, press **Esc** on the console, and use the boot menu to select **Release 7.6**.
- 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 8.2.151.0 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 8.2.151.0, 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 8.2.151.0.



**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 5](#), 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](http://www.cisco.com/c/en/us/td/docs/wireless/controller/release/notes/fus_rn_OL-31390-01.html).

**Table 5** *FUS Upgrade Guidance*

WLC Controller Model	Recommended FUS Version
2504	2.0, see <a href="#">CSCuu46671</a>
5508	1.9, see <a href="#">CSCul68057</a>
5520	No FUS
7510	2.0, see <a href="#">CSCus97953</a>
8510	2.0, see <a href="#">CSCus97953</a>
8540	No FUS
WiSM2	1.9, see <a href="#">CSCul68057</a>



**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 8.2.151.0 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 8.2.151.0. [Table 6](#) shows the upgrade path that you must follow before downloading Release 8.2.151.0.



**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 6 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 8.2.151.0.

- 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 8.2.151.0. 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 8.2.151.0 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 8.2.151.0 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 8.2.151.0 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 8.2.151.0 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 8.2.151.0 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:
- Go to the Cisco Software Center at this URL:  
<https://tools.cisco.com/SWIFT/LicensingUI/Home>
  - From the Product License Registration page from the **Get Other Licenses** drop-down list, click **IPS, Crypto, Other ...**
  - In the **Wireless** section, click **Cisco Wireless Controllers (2500/5500/7500/WiSM2) DTLS License** and click **Next**.
  - 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 8.2.151.0 with other client devices.

**Table 7** Test Bed Configuration for Interoperability

Hardware/Software Parameter	Hardware/Software Configuration Type
Release	8.2.151.0
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 8** *Laptop Client Type List*

<b>Client Type and Name</b>	<b>Version</b>
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 9** *Tablet Client Type List*

<b>Client Type and Name</b>	<b>Version</b>
Apple iPad Air	iOS 10
Apple iPad Air 2	iOS 10
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
MC40N0	Android 4.4.4

**Table 9** *Tablet Client Type List*

<b>Client Type and Name</b>	<b>Version</b>
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 10** *Phone and Printer Client Type List*

<b>Client Type and Name</b>	<b>Version</b>
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
Cisco 8861	Sip88xx.10-2-1-16

**Table 10** Phone and Printer Client Type List

<b>Client Type and Name</b>	<b>Version</b>
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 20](#)
- [Features Not Supported on Cisco WiSM2 and Cisco 5508 WLC, page 20](#)
- [Features Not Supported on Cisco Flex 7510 WLCs, page 21](#)
- [Features Not Supported on Cisco 5520, 8510, and 8540 WLCs, page 22](#)
- [Features Not Supported on Cisco Virtual WLCs, page 22](#)
- [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 23

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

Operational Modes	<ul style="list-style-type: none"> <li>• Spectrum Expert Connect</li> <li>• Workgroup Bridge (WGB) mode as a part of Cisco Mobility Express</li> <li>• Mesh mode</li> <li>• Flex plus Mesh</li> <li>• 802.1x supplicant for AP authentication on the wired port</li> </ul>
Protocols	<ul style="list-style-type: none"> <li>• 802.11u</li> <li>• Full Cisco Compatible Extensions (CCX) support</li> <li>• Rogue Location Discovery Protocol (RLDP)</li> <li>• Native IPv6</li> <li>• Telnet</li> <li>• Internet Group Management Protocol (IGMP)v3</li> </ul>
Security	<ul style="list-style-type: none"> <li>• Locally Significant Certificate (LSC)</li> <li>• TrustSec SXP</li> <li>• CKIP, CMIC, and LEAP with Dynamic WEP</li> <li>• Static WEP key for TKIP or CKIP <sup>1</sup></li> </ul>
Quality of Service	<ul style="list-style-type: none"> <li>• Cisco Air Time Fairness (ATF)</li> </ul>
Location Services	<ul style="list-style-type: none"> <li>• Data RSSI (Fast Locate)</li> <li>• Wi-Fi Tag</li> </ul>
FlexConnect Features	<ul style="list-style-type: none"> <li>• Per Client AAA (QoS Override)</li> <li>• Bidirectional rate-limiting</li> <li>• Link aggregation (LAG)</li> <li>• Split Tunneling</li> <li>• EoGRE</li> <li>• Multicast to Unicast (MC2UC)</li> <li>• Traffic Specification (TSpec) <ul style="list-style-type: none"> <li>– Cisco Compatible Extensions (CCX)</li> <li>– Call Admission Control (CAC)</li> </ul> </li> <li>• DHCP Option 60</li> <li>• NAT/PAT support</li> <li>• VSA/Realm Match Authentication</li> <li>• Proxy ARP</li> <li>• PPPoE</li> <li>• SIP snooping with FlexConnect in local switching mode</li> </ul>



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

Operational Modes	<ul style="list-style-type: none"> <li>• Monitor Mode</li> <li>• Multiple client on wired ports</li> </ul>
FlexConnect Features	<ul style="list-style-type: none"> <li>• Local AP Authentication</li> </ul>


## Features Not Supported on Cisco Aironet 1830 and 1850 Series APs

**Table 13** *Features Not Supported on Cisco Aironet 1830 OEAP and 1850 Series APs*

Operational Modes	<ul style="list-style-type: none"> <li>• Monitor Mode</li> </ul>
FlexConnect Features	<ul style="list-style-type: none"> <li>• Local AP Authentication</li> </ul>

## Features Not Supported on Cisco Aironet 2800 and 3800 Series APs

**Table 14** *Features Not Supported on Cisco Aironet 1830 OEAP and 1850 Series APs*

Security	<ul style="list-style-type: none"> <li>• WPA2 + TKIP</li> </ul>
	
	<b>Note</b> WPA +TKIP and TKIP + AES protocols are supported.

## 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 15** Open Caveats for 8.2.151.0

Caveat ID Number	Description
<a href="#">CSCuu21625</a>	Session not cleared on Cisco 5508 WLC anchor with Cisco 3850 AP foreign causing authentication issues
<a href="#">CSCuu49801</a>	Country code issue with AE,AL
<a href="#">CSCuv99434</a>	Roams using PMF + OKC not working correctly
<a href="#">CSCuw95402</a>	SNMP not returning correct information for roaming client
<a href="#">CSCux06806</a>	ATF EnforcementConfig for network radio is not pushed to uploaded configuration
<a href="#">CSCux23710</a>	Cisco IW3702 APs LED status observed behavior is inconsistent with CCO user guide
<a href="#">CSCux28505</a>	Cisco 8510 WLC reloads unexpectedly with “fp_main_task” in the 8_2_1_124 image during boot
<a href="#">CSCux42874</a>	Management Frame Protection (MFP): Mobility Agent (MA) dropped key request from Mobility Controller (MC)
<a href="#">CSCux56652</a>	Local profile shows wrong statistics and percentage information
<a href="#">CSCux59359</a>	Cisco 8510 WLC behind NAT on New mobility and client stuck in DHCP_REQD state
<a href="#">CSCux77970</a>	Web-authentication: AAA override uplink rate limit values are not getting reflected in web-authentication
<a href="#">CSCux78581</a>	Cisco 1810 APs: multiple clients are not supported on LAN ports
<a href="#">CSCux95662</a>	PMIPv6 client fails to get an IP if there is no DHCP server configured
<a href="#">CSCuy02774</a>	PMIPv6 client binding clean up issues
<a href="#">CSCuy04572</a>	Wrong time stamp sent on rogue traps when delta value set on the controller
<a href="#">CSCuy20175</a>	Windows clients machine/user authentication failing when doing inter-WLC roaming
<a href="#">CSCuy26870</a>	In ME-Controller GUI, showing incorrect Tx power range
<a href="#">CSCuy34975</a>	Cisco 5508 WLC running 8.0.120.0 release, reloads unexpectedly when adding SSID to friendly rule
<a href="#">CSCuy57687</a>	No RF-group membership information when RF-gr member is MA
<a href="#">CSCuy74931</a>	Override 802.1x supplicant credentials lost after reboot
<a href="#">CSCuy87193</a>	Cisco WLC reloads unexpectedly (due to EmWeb) when adding 1500+ local net users
<a href="#">CSCuy91177</a>	Client MSCB removed on optimized roam
<a href="#">CSCuz03702</a>	New mobility: wired client behind WGB fails to pass traffic after roaming
<a href="#">CSCuz11156</a>	AAA overridden ACL not applied after WPA2/802.1x fast roaming

**Table 15**      **Open Caveats for 8.2.151.0**

<b>Caveat ID Number</b>	<b>Description</b>
<a href="#">CSCuz11374</a>	Cisco WLC: selects wrong DHCP relay even though it is configured in the interface
<a href="#">CSCuz18799</a>	Cisco 2800, 3800 APs sends VHT SGI frames to STA that does not support SGI
<a href="#">CSCuz18869</a>	WLC picking up the unicast DHCP for unknown destination
<a href="#">CSCuz18914</a>	Cisco 8.0.140.0 release: FT over-the-air roam does not work
<a href="#">CSCuz22198</a>	Cisco 5508 WLC unexpectedly reloads with %OSAPI-0-TIMER_CREATE_FAILED: timerlib.c
<a href="#">CSCuz27736</a>	Cisco 3800 APs on Flex- AP sends deauthenticate after FT roam (Freq- 3-4%)
<a href="#">CSCuz29774</a>	Cisco 1852 APs losing connectivity to ME controller with AVC enabled
<a href="#">CSCuz33090</a>	Cisco 3802 AP - four antennas are always supported in VHT Capabilities IE
<a href="#">CSCuz45986</a>	Cisco 8500 WLC: CWA is not working with guest anchor with accounting enabled
<a href="#">CSCuz46892</a>	ME: external AP rebooted because it detected another ME controller
<a href="#">CSCuz47732</a>	Cisco WLC reloads unexpectedly on task name "radiusTransportThread"
<a href="#">CSCuz49685</a>	Cisco 1810 OEAP SNMP: not seeing error when trying to disable Port 3
<a href="#">CSCuz49804</a>	Fix AID leak problems
<a href="#">CSCuz65017</a>	Cisco 3800 APs not updating HT 'Op Mode' bits in presence of legacy AP
<a href="#">CSCuz65175</a>	ME 1852 APs: HTTP profiling causes CPU spikes and degraded performance
<a href="#">CSCuz65797</a>	New mobility: guest anchor controller unexpected reload observed at mmMaListen
<a href="#">CSCuz68479</a>	Cisco 3800 APs not reassembling wireless fragmented frames
<a href="#">CSCuz69729</a>	Cisco 3700 AP running 8.4.140.0 release - 802.11ac WGB not associates with root channel width 40-MHz above or below
<a href="#">CSCuz78490</a>	DHCP: usage indicator will not show 100% usage even if all IP's are in use
<a href="#">CSCuz88573</a>	Cisco WLC experiences unexpected reload in emWeb
<a href="#">CSCuz90785</a>	Cisco 8.2 release: traffic black hole WEP errors on Cisco IW3702 WGB during roaming mesh
<a href="#">CSCva00087</a>	Cisco WLC reloads unexpectedly on apfVerifyCountryString spamApTask2
<a href="#">CSCva07048</a>	Cisco WLC Data Plane reloads unexpectedly on WQE stuck
<a href="#">CSCva07307</a>	Voice tagged frames drop at AP radio after upgrade to 8.2 and later

**Table 15**      **Open Caveats for 8.2.151.0**

<b>Caveat ID Number</b>	<b>Description</b>
<a href="#">CSCva14667</a>	GET on Cisco AP groups Table after set - response missing
<a href="#">CSCva16449</a>	Cisco 1552 AP is not showing the temprature on Cisco WLC running 8.2 release
<a href="#">CSCva25999</a>	Rate limit not followed as per QoS role defined for guest user
<a href="#">CSCva26117</a>	NAT translation output for locally switched traffic not observed in AP
<a href="#">CSCva26821</a>	Auto Anchor Deployment: scheduling deletion of mobile station fails
<a href="#">CSCva27276</a>	Cisco 2802 APs: local profiling detects windows client as "Microsoft-Workstation"
<a href="#">CSCva27419</a>	Channel changed trap with unknown radio type on dual band radio
<a href="#">CSCva27711</a>	Cisco FlexConnect: AP radio resets during FT when central DHCP is enabled on the WLAN
<a href="#">CSCva29463</a>	Cisco 2800, 3800 APs: WLAN client fails >=1500 bytes ICMP traffic in standalone mode
<a href="#">CSCva29554</a>	Cisco 802.11ac Wave2 APs: FlexConnect AAA overridden ACL is not plumbed in the WLC
<a href="#">CSCva31890</a>	MIB table bsnMobileStationPerRadioPerVapTable has no data
<a href="#">CSCva40580</a>	Cisco 8.3 release: bulksync between active and standby WLC never completes and is stuck in 'in-progress' mode
<a href="#">CSCva42290</a>	Cisco WLC is not setting the QoS Map Set bit or the WNM Notification bit in the Extended Capabilities IE of an association response
<a href="#">CSCva51719</a>	Cisco 1850 ME: mismatch QoS profile priority
<a href="#">CSCva52938</a>	Cisco 2800, 3800 APs reporting incorrect CDP info to the switch
<a href="#">CSCva53980</a>	Issue in Cisco CleanAir when client is serving 5-GHz band
<a href="#">CSCva55165</a>	IPv6 Multicast from PMIPv6 client shows client MAC on layer3 or layer2 switch
<a href="#">CSCva65380</a>	Multicast mobility mode configuration enabled with IP is not getting saved
<a href="#">CSCva66176</a>	AP drop of from network due to large set of mobility groups in down/down state
<a href="#">CSCva71002</a>	Cisco WLC GUI: client filter fails with spaces used in the client name
<a href="#">CSCva72044</a>	Cisco 1572 mesh AP with no distance command implementation
<a href="#">CSCva82261</a>	Cisco 1532 APs up-link drops when sending heavy upstream traffic
<a href="#">CSCva85361</a>	Cisco WLC loosing IPv6 Connectivity
<a href="#">CSCva95121</a>	Stale IP route left on Flex AP configuration if booting up in standalone mode

**Table 15**      **Open Caveats for 8.2.151.0**

<b>Caveat ID Number</b>	<b>Description</b>
<a href="#">CSCva99864</a>	EAP-TLS fails with Windows and ME using “Smart card or certificate” authentication
<a href="#">CSCvb02180</a>	ARP table full. unable to delete ARP mapping
<a href="#">CSCvb05067</a>	Local EAP fails after wrong user name login is used
<a href="#">CSCvb18640</a>	Mobility Express: manual channel-widths overwritten by DCA
<a href="#">CSCvb19483</a>	Cisco 1850 ME unable to download login-banner
<a href="#">CSCvb23576</a>	Excluded clients can connect to Cisco 2800 APs in Flexconnect local switching
<a href="#">CSCvb29996</a>	Cisco 1810W AP hardware reloads unexpectedly when watchdog resets and the crash file shows PC=0xc03b3ffc, LR=0xc008af24
<a href="#">CSCvb31857</a>	Cisco WLC rejects 802.11k supported client association when assisted roaming is enabled on FRA enabled Cisco 2800 AP on 5G
<a href="#">CSCvb36432</a>	SSIDs vanishes from standalone AP after reboot
<a href="#">CSCvb64042</a>	WLC HA transfer download failure with legitimate network latency
<a href="#">CSCvb64560</a>	CISCO-LWAPP-AAA-MIB: DEFVAL format incorrect for some objects
<a href="#">CSCvb72367</a>	Transfer upload datatype run-config is missing several configuration sections
<a href="#">CSCvb89227</a>	For last AP connection failure reason: messages not getting properly on join statistics
<a href="#">CSCvb91652</a>	PMIPv6 sluggish in CLI and GUI response as well as sporadic lack of snmp response
<a href="#">CSCvb91832</a>	Cisco1810W AP radio reloads unexpectedly due to firmware failure @0x009C30A0/0x0000, memory corruption
<a href="#">CSCvc00328</a>	Cisco 3800 APs: Microsoft Surface pro gives less throughput
<a href="#">CSCvc09805</a>	Cisco WLC on 8.2 release: rejects client association even when only one AP is broadcasting SSID and multiple client attempts
<a href="#">CSCvc12703</a>	Cisco 1810W APs: LAN port 2 maps to wrong VLAN on N+1 failover to primary
<a href="#">CSCvc25658</a>	Cisco 2800, 3800 APs: padding from small CAPWAP fragments transmitted over the air to clients
<a href="#">CSCvc26521</a>	Cisco 1850 APs: during continuous configuration change, AP reboots with a coredump
<a href="#">CSCvc28168</a>	Cisco WLC set ZERO 802.11e QoS UP for part of the downstream voice packets and APs trust it
<a href="#">CSCvc40852</a>	Cisco 8.2.140.0 release: active controller in HA pair shows different socket errors
<a href="#">CSCvc49492</a>	Cisco 1852 AP detects high noise level on 5-GHz radio
<a href="#">CSCvc50775</a>	Web authentication redirection stop working when AP manager is configured on a dynamic interface

**Table 15**      **Open Caveats for 8.2.151.0**

<b>Caveat ID Number</b>	<b>Description</b>
<a href="#">CSCvc51666</a>	IOS AP transmits on disabled 24Mb data rate
<a href="#">CSCvc55328</a>	AP reloads unexpectedly due to kernel panic at WLoadRateGrp
<a href="#">CSCvc57427</a>	Cisco WiSM2: memory leak while handling Cisco AVP POLICY_ROLE_TYPE(cisco_avp_pair=role)
<a href="#">CSCvc75113</a>	MIB compile error on CISCO-LWAPP-TUNNEL-MIB.my version 8.2
<a href="#">CSCvc78510</a>	Cisco 2702 AP aux port goes to disabled after the AP is rebooted
<a href="#">CSCvc81168</a>	Cisco 2702 AP unable to upgrade and failing with error "Unable to create temp dir flash:/update"
<a href="#">CSCvc84483</a>	Cisco 3800 APs: kernel panic seen in alpha running 8.2.145.26 release
<a href="#">CSCvc87409</a>	Cisco 2800 AP Tx-reset causing radio reset
<a href="#">CSCvb61023</a>	DHCP option 82 (remote-id) not present in some APs
<a href="#">CSCvc94524</a>	Cisco 2800, 3800 iPhone and android phones are not getting IPv6 addresses
<a href="#">CSCvb93189</a>	AP drops retransmitted M3 from WLC
<a href="#">CSCvc06547</a>	AP re-transmits packet even though client sends ACK
<a href="#">CSCvc65568</a>	Cisco Wireless IP Phone 8821 fails 802.11r FT roam with "Invalid FTIE MIC"
<a href="#">CSCvd18773</a>	Cisco 8.2 clients unable to authenticate 'Sending assoc-resp with status 12 station'
<a href="#">CSCvd21969</a>	AAA AVC override - AVC profile retained after roaming
<a href="#">CSCvb86237</a>	Cisco 8510 WLC reloads unexpectedly on Task Name: TempStatus
<a href="#">CSCvd18025</a>	Anchor1 WLC does not free client sessions after client roaming to anchor2 WLC-client entries stale
<a href="#">CSCvc87433</a>	Web authentication with proxy does not work after Cisco 8.2 release
<a href="#">CSCvc65641</a>	WLC reports tracebacks reported very frequently but no crashes

## Resolved Caveats

**Table 16** *Resolved Caveats for 8.2.151.0*

<b>Caveat ID Number</b>	<b>Description</b>
<a href="#">CSCur63031</a>	AP error:%ENTROPY-0-ENTROPY_ERROR: Unable to collect sufficient entropy
<a href="#">CSCur68316</a>	Cisco 802AP-891 in FlexConnect mode are losing VLAN mapping after power cycle
<a href="#">CSCuw41092</a>	AP not send traffic indication in beacon for power-save client after FT
<a href="#">CSCux48308</a>	Broadcast delivery stops with key rotation Cisco 1552 AP in RAP and Cisco 819W running release 153.3JBB5 is in WGB mode
<a href="#">CSCux51833</a>	Client fails on RAP with AAA Override ACL when AP is in Flex+Bridge mode
<a href="#">CSCux78389</a>	RADIUS failover should failover both authentication account server on WLAN
<a href="#">CSCux85357</a>	WLC sends GARP for Cisco FlexConnect local switching clients after HA switch-over
<a href="#">CSCux88967</a>	On MAC filter failure, client session timeout can not association again
<a href="#">CSCux95319</a>	Clients roaming between central to local authentication may apply for local to FlexConnect mode APs (not supported) causing 802.1x table failures
<a href="#">CSCux96500</a>	Cisco WiSM2 WLC reloads unexpectedly on bcastReceiveTask
<a href="#">CSCuy30583</a>	Cisco 5520 WLC reloads unexpectedly on show imm chassis shows no results
<a href="#">CSCuy53072</a>	SNMP cLMobilityGroupMembersTable returns wrong value from WLC in PI
<a href="#">CSCuy53596</a>	Cisco CleanAir fatal error and radio reset on Flex+Bridge AP
<a href="#">CSCuy64520</a>	Access Points (AP) sending CDP packets to the wireless clients
<a href="#">CSCuy71409</a>	Client detailed params not synced to standby in fast SSID scenario
<a href="#">CSCuy75241</a>	Cisco 5508 WLC system unexpectedly reloads with task mmMobility
<a href="#">CSCuy82849</a>	Memory leak found @mm_heartbeat module on guest anchor WLC
<a href="#">CSCuz11717</a>	3-sec delay before sending “dot1x auth initiate” to SPAM with WSSI
<a href="#">CSCuz16883</a>	Address registration issues for mobility scenarios
<a href="#">CSCuz35221</a>	Mobility hand off fails in new mobility 802.1x CWA client reconnect
<a href="#">CSCuz40066</a>	Guest Anchor: foreign to foreign roam fails on GA scenario
<a href="#">CSCuz40970</a>	Cisco 8510 WLC: WLC unexpectedly reloads on task osapiBsnTimer
<a href="#">CSCuz50774</a>	Cisco WLC lossing pings to itself, reaper cleaning up exited task osapi_ping_rx
<a href="#">CSCuz78555</a>	Bulk sync status “In-progress” after standby boots up



**Table 16 Resolved Caveats for 8.2.151.0**

<b>Caveat ID Number</b>	<b>Description</b>
<a href="#">CSCva01578</a>	Cisco 2800, 3800 APs not showing syslog server IP with DHCP option-7
<a href="#">CSCva01762</a>	Cisco 1815, 1850 APs: Over-ride global credentials cleared on GUI after reboot
<a href="#">CSCva03376</a>	UX-AP3702i after primed carrier set 5-GHz only allowing four UNII3 channels
<a href="#">CSCva22440</a>	Cisco 3800 AP: QBSS STA Count keeps incrementing with STA associating again
<a href="#">CSCva28211</a>	AireOS UX AP: 'JP' should be used as world mode in beacon/probes
<a href="#">CSCva28524</a>	Cisco WLC with 8.3 release- creating SNMP community fails
<a href="#">CSCva31178</a>	Cisco AP with 8.3 release - radio reset due to offchannel stuck
<a href="#">CSCva32411</a>	Clients losing connectivity when re-authenticates with 802.1x over Cisco 702w AP
<a href="#">CSCva48201</a>	Unable to set static IP for AP from controller GUI
<a href="#">CSCva52825</a>	Cisco 2800, 3800 APs does not do PMTU discovery during join or image download
<a href="#">CSCva63541</a>	Cisco 2800, 3800 AP CAPWAP DTLS data encryption may cause AP drops due to large traffic
<a href="#">CSCva72724</a>	Cisco 2602 AP reloads unexpectedly on "disc_tx_requeue_client" "dot11_get_rate_shift"
<a href="#">CSCva74487</a>	Cisco 8540 WLC reloads unexpectedly on running show commands task: emWeb
<a href="#">CSCva74927</a>	AP disjoins with 'Failed to get ARP entry for WLC' error
<a href="#">CSCva83234</a>	Cisco 2800, 3800 APs: Kernel reloads unexpectedly during image download
<a href="#">CSCva83884</a>	Cisco WLC system reloads unexpectedly on aaaQueueReader
<a href="#">CSCva87295</a>	Flex AP radio reset during FT with Central DHCP and NAT-PAT enabled
<a href="#">CSCva90343</a>	Unable to do VLAN to RLAN mapping at FlexConnect Group
<a href="#">CSCva91457</a>	Cisco WLC: unexpectedly reloads repeatedly with reason: spamApTask4
<a href="#">CSCva95251</a>	DSCP traffic is not limited to maximum QoS Profile value
<a href="#">CSCvb09381</a>	Unable to add or modify SNMP strings on a Cisco 5520 WLC HA Pair running 8.1.122.0 release
<a href="#">CSCvb25233</a>	Enable VLAN-RLAN mapping in FlexConnect Group
<a href="#">CSCvb28231</a>	Cisco 5508 WLCs reloads unexpectedly due to memory corruption
<a href="#">CSCvb35173</a>	Cisco 2800, 3800 APs: Radio reloads unexpectedly, beacon stuck - due to lost Txq reference

**Table 16** *Resolved Caveats for 8.2.151.0*

<b>Caveat ID Number</b>	<b>Description</b>
<a href="#">CSCvb43105</a>	Cisco 2800, 3800 APs outer DSCP not same as inner with DSCP Trust upstream NSS
<a href="#">CSCvb44169</a>	emWeb reaper reset after “clear mdns service-database all”
<a href="#">CSCvb44699</a>	NMSP queue full due to rouge AP task
<a href="#">CSCvb48603</a>	Evaluation of Cisco WLC for OpenSSL September 2016
<a href="#">CSCvb52310</a>	Silent Boot on Cisco 2800, 3800 APs
<a href="#">CSCvb54166</a>	Malformed 802.11v element on HSR WGB with WLC 8.2 or later release
<a href="#">CSCvb69962</a>	Client traps not showing session ID’s
<a href="#">CSCvb71168</a>	RSA256-AES256 DTLS encryption lowers PMTU but AP does not respect it
<a href="#">CSCvb72380</a>	Cisco 2800, 3800 APs: performance profile show all values as 0 after clearing the configuration for XOR radio
<a href="#">CSCvb73104</a>	Cisco 1600 AP: radio D1 reset: FW: irq/mac stat=40000/10000000 command timeout
<a href="#">CSCvb78834</a>	Cisco WLC reloads unexpectedly with task name emweb
<a href="#">CSCvb79274</a>	WGB wired client expiring periodically
<a href="#">CSCvb80511</a>	CWA is not working for flex-bridge APs pointing ACL Rx from RADIUS does not exist
<a href="#">CSCvb81003</a>	Cisco WLC reloads unexpectedly as emWeb uses 100%
<a href="#">CSCvb81359</a>	Cisco 8540 WLC HA. RMI ping and access to standby fail when using non-default ap-manager
<a href="#">CSCvb85576</a>	Evaluation of Cisco WLC for CVE-2016-5195 (DIRTY CoW)
<a href="#">CSCvb89781</a>	Cisco 2700-B AP unable to join WLC: unable to create temp dir “flash:/update”
<a href="#">CSCvb90403</a>	Cisco 1810W AP: hardware watchdog reset at PC= 0xc03b3ffc, LR= 0xc011e2dc
<a href="#">CSCvb90793</a>	AP name unknown in SNMP bsnDot11StationDeauthenticate traps
<a href="#">CSCvb91603</a>	Data rate in 5-GHz cannot be locked to 6 Mbps for Cisco 1810AP
<a href="#">CSCvb92562</a>	Evaluation of all for OpenSSL 1.0.1 September 2016
<a href="#">CSCvb94413</a>	Cisco 2800, 3800 APs: low Tx power observed in certain RF conditions
<a href="#">CSCvb94436</a>	TKIP support for Cisco 1800 series APs
<a href="#">CSCvb94610</a>	Restore command to disable GARP
<a href="#">CSCvb94697</a>	Cisco 2800, 3800 APs: 802.11n macbook client has dropping connectivity while connecting to Cisco 3800 APs
<a href="#">CSCvb94799</a>	mc2uc packet lost with Cisco 3802E APs
<a href="#">CSCvb95147</a>	Cisco 1572EAC APs unable to use 80 MHz

**Table 16**      **Resolved Caveats for 8.2.151.0**

<b>Caveat ID Number</b>	<b>Description</b>
<a href="#">CSCvc00358</a>	Cisco WLC reloads unexpectedly “apfRogueTask_0” missed software watchdog
<a href="#">CSCvc09824</a>	Cisco 2800 APs: band select statistics counter show zero
<a href="#">CSCvc11544</a>	Default neighbor pruning timer needs to be increased to keep neighbor entries for 1 hour
<a href="#">CSCvc13175</a>	Cisco 5520 WLCs: GLC-T SFP stopped working (1G Port down)
<a href="#">CSCvc15149</a>	Cisco 8.2.140.0 release - not beaconing a SSID when it is in an AP group and SSID enabled later
<a href="#">CSCvc16755</a>	Cisco 3802 AP custom power level not initialized after reboot
<a href="#">CSCvc18129</a>	Cisco WLC reloads unexpectedly on RF profile or client exclusion sync on HA scenario
<a href="#">CSCvc18699</a>	Cisco 1800 APs: high pings drops, traffic connectivity drops seen 8.2.131.40 release
<a href="#">CSCvc23658</a>	Clients not removed from Cisco FlexConnect and CAPWAP in APs FlexConnect central-sw
<a href="#">CSCvc25669</a>	rfidTask’ is causing a high CPU on the WLC
<a href="#">CSCvc31133</a>	Unable to enable WLAN with enabled selected option in GUI. Security: FT + Open
<a href="#">CSCvc31304</a>	Cisco 8.3.111.0 release: AP syslog flood for TLV-DEC-ERR: cannot process TLV for TLV_DMS_CLIENT_REQUEST_PAYLOAD(325/0)
<a href="#">CSCvc32590</a>	Cisco 2802 AP with Pakistan (G) regulatory domain fails to join a Pakistan country code enabled controller
<a href="#">CSCvc32706</a>	Cisco 3800 APs: not seeing all COS neighbors
<a href="#">CSCvc32856</a>	Cisco 2800, 3800 APs: sends a AQ event as soon as RRM changes channel causing bad channel selection and changes
<a href="#">CSCvc33258</a>	Cisco WLC: unable to config Rx-SOP threshold for Cisco IW3702 AP
<a href="#">CSCvc33511</a>	SNMPv3 access failing with either unknown user or no response
<a href="#">CSCvc38214</a>	Cisco 2800, 3800: APs sending acknowledgements to client at 54 data rate although basic rate is 12 and 24
<a href="#">CSCvc40470</a>	AP radio hang chatter: wl0: rxRingStuckDetect(271): Rx-hang detected!!
<a href="#">CSCvc42566</a>	Cisco 1702I AP - radio resets observed due to Cisco CleanAir error count exceeded
<a href="#">CSCvc42939</a>	Cisco 3800: AP duplicating multicast packets
<a href="#">CSCvc43232</a>	Cisco 2800, 3800 AP uses 802.11n data rates to send data packets to 802.11b only clients thus failing to associate
<a href="#">CSCvc43328</a>	Cisco 2800, 3800 APs sending acknowledgements to client at 54Mbps data rate although basic rate is 12Mbps and 24Mbps in 8.2.140.0 esc image

**Table 16** *Resolved Caveats for 8.2.151.0*

<b>Caveat ID Number</b>	<b>Description</b>
<a href="#">CSCvc45038</a>	Cisco 2800, 3800 APs beacon drift 25ms with offchannel/cleanair scanning @3sec mc9060 client drops
<a href="#">CSCvc48232</a>	Cisco 2800, 3800 APs reloads unexpectedly due to kernel panic at mhsm_transition
<a href="#">CSCvc50228</a>	Cisco 2800, 3800 APs sending data packets to the 802.11g clients sometimes with messed up data rates
<a href="#">CSCvc50377</a>	Cisco Flex7510 WLC running 8.0.110.11 release: emWeb reloads unexpectedly while doing “show run-config”
<a href="#">CSCvc52004</a>	iOS device connect to the 802.1x network slowly
<a href="#">CSCvc52619</a>	Local EAP do not support any of ciphers used by Cisco Wireless IP Phone 8821
<a href="#">CSCvc53578</a>	Cisco 2800, 3800 AP: 802.11b only clients does not associate if HT is disabled
<a href="#">CSCvc53675</a>	Cisco 1852 AP - kernel backtrace at ol_ath_tx_mgmt_wmi_send+0x0/0x1e4
<a href="#">CSCvc59252</a>	Cisco 1852 AP showing only power level 1 instead of power level 1 to 8 under 5-GHz radio
<a href="#">CSCvc61560</a>	WLC RADIUS authentication on aaaQueueReader “Unable to fit RADIUS packet in allocated memory”
<a href="#">CSCvc64343</a>	Cisco 1530 AP in Japan domain in mesh mode: detects a lot of radars
<a href="#">CSCvc70133</a>	802.11ac Wave2 AP in Flex mode: MC40 802.11g client sending association request with 802.11g rates in extended rates display issue
<a href="#">CSCvc76148</a>	Cisco 2800, 3800 APs beacon drift causing Motorola mc9060 client drops
<a href="#">CSCvc86514</a>	Cisco 2800, 3800 AP CAPWAP reset when extended radio coredump is enabled
<a href="#">CSCvc86979</a>	Cisco 2800 AP silently reboots with NUL print every 10 mins in a loop
<a href="#">CSCvc87146</a>	Cisco 2800, 3800 APs: disables Per-WLAN beacon on detection
<a href="#">CSCvc87207</a>	Cisco 2800 APs: 802.11b/g radio dropping RTP packets
<a href="#">CSCvc89939</a>	Cisco AP running 8.2.145.33 release: 40 MHz ext offset
<a href="#">CSCvc90559</a>	Rx hang seen on alpha running 8.2.145.36 release
<a href="#">CSCvc94165</a>	Low PMTU 1005-AP’s joined with RSA256-AES256
<a href="#">CSCvc95222</a>	Cisco 1810w AP LAN port dropping IPTV packets
<a href="#">CSCvc95291</a>	Rx hang seen on alpha running 8.2.145.39 release
<a href="#">CSCvd03656</a>	Cisco 2800, 3800 APs not updating NDP to WLC due to status: NSS_INVALID_PARAM
<a href="#">CSCvd07215</a>	Cisco 1810, 2800 APs do not learn DHCP lease time from DHCP server and defaults to 24hours
<a href="#">CSCvd07243</a>	Unable to change AP name nor location from the GUI

**Table 16**      **Resolved Caveats for 8.2.151.0**

<b>Caveat ID Number</b>	<b>Description</b>
<a href="#">CSCvd07657</a>	Cisco 1810 AP fails to get ARP response intermittently leading to a full reboot
<a href="#">CSCvd16939</a>	Cisco 1800 AP band-select does not work
<a href="#">CSCvd19354</a>	Cisco reloads unexpectedly while editing config rf-profile hsr-mode disable   enable config rf-profile 11b
<a href="#">CSCvd20843</a>	Beacon stuck due to off-channel stuck
<a href="#">CSCvd23510</a>	Cisco 2800, 3800 APs, and 1800 ME: SSH affected by CVE-2016-7406 - 7409
<a href="#">CSCvd25183</a>	Cisco 2800, 3800 AP does not advertise the extension channel correctly when DCA assigns bandwidth
<a href="#">CSCvd33680</a>	Radio reloads unexpectedly in Cisco 3800 AP running 8.2 release
<a href="#">CSCvd35231</a>	Cisco 1810W AP: Reloads with Reason 0: unknown aka silent reboot
<a href="#">CSCvd35988</a>	Cisco 5520 WLC: HA is causing DENY rule on WLC. Telnet and GUI access to WLC management IP or service IP is restricted from outside network
<a href="#">CSCvd51674</a>	Cisco 1810w APs reboots silently and reverts to highest power table value

# 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](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 2800 Series Cisco Aironet 3500 Series Cisco Aironet 3600 Series Cisco Aironet 3700 Series Cisco Aironet 3800 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 8.2.151.0, 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-K9-8.2.151.0.tar	AIR-AP1830-K9-8.2.151.0.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](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.

### 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](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](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](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](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.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2017 Cisco Systems, Inc. All rights reserved.

