Release Notes for Cisco Wireless Controllers and Cisco Lightweight Access Points, Cisco Wireless Release 8.0.140.0

First Published: August 25, 2016

This document describes what is new in 8.0.140.0 release, instructions to upgrade to this release, and information about the open and resolved caveats for this release. Unless otherwise noted, 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*.

Revision History

Table 1 Revision History

Modification Date	Modification Details
November 10, 2017	• Open Caveats, page 24 – Added CSCvc65568
October 10, 2017	• Features Not Supported on Cisco Virtual WLCs, page 22 – Added Wired Guest and FlexConnect central switching.
February 13, 2017	• Open Caveats – Added: CSCvd06463
December 5, 2016	• Added information about change in WLAN-AP group association functionality to the "Upgrading to Cisco WLC Software Release 8.0.140.0" section on page 9
October 14, 2016	• Updated: What's New in Release 8.0.140.0, page 3

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

Cisco Wireless Controller and Cisco AP Platforms

The section contains the following subsections:

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

Supported Cisco Wireless Controller Platforms

The following Cisco WLC platforms are supported in this release:

- Cisco 2500 Series Wireless Controllers
- Cisco 5508 Wireless Controllers
- Cisco Flex 7500 Series Wireless Controllers
- Cisco 8510 Series Wireless Controllers
- Cisco Virtual Wireless Controllers on Cisco Services-Ready Engine (SRE) or Cisco Wireless Controller Module for Integrated Services Routers G2 (UCS-E)
- Cisco Wireless Controllers for high availability (HA Cisco WLCs) for the Cisco 2500 Series (no AP SSO support), 5500 Series, Wireless Services Module 2 (WiSM2), Flex 7500 Series, and 8500 Series WLCs
- Cisco WiSM2 for Catalyst 6500 Series Switches

For information about features that are not supported on the Cisco WLC platforms, see Features Not Supported on Cisco WLC Platforms, page 20.

Supported Access Point Platforms

The following access point platforms are supported in this release:

- Cisco Aironet 1040, 1130, 1140, 1240, 1250, 1260, 1600, 1700, 2600, 2700, 3500, 3600, 3700, Cisco 600 Series OfficeExtend, 700, AP801, and AP802 Series indoor access points
- Cisco Aironet 1520 (1522, 1524), 1530, 1550 (1552), 1570, and Industrial Wireless 3700 Series outdoor and industrial wireless access points

For information about features that are not supported on some access point platforms, see Features Not Supported on Access Point Platforms, page 22.

Cisco AP801 and AP802 are integrated access points on the Cisco 800 Series Integrated Services Routers (ISRs). For more information about the stock-keeping units (SKUs) for the access points and the ISRs, see the following data sheets:

- AP860:

  http://www.cisco.com/c/en/us/products/collateral/routers/800-series-routers/data_sheet_c78_461543.html

- AP880:

  http://www.cisco.com/c/en/us/products/collateral/routers/887-integrated-services-router-isr/data_sheet_c78_459542.html http://www.cisco.com/c/en/us/products/collateral/routers/800-series-routers/data_sheet_c78-613481.html

http://www.cisco.com/c/en/us/products/collateral/routers/880-3g-integrated-services-router-isr/data_sheet_c78_498096.html

http://www.cisco.com/c/en/us/products/collateral/routers/880g-integrated-services-router-isr/data_sheet_c78-682548.html

- AP890:

  http://www.cisco.com/c/en/us/products/collateral/routers/800-series-routers/data_sheet_c78-519930.html

  AP802 is an integrated access point on the next generation Cisco 880 Series ISRs.

  Before you use an AP802 series lightweight access point with Cisco WLC software release 8.0.140.0, you must upgrade the software in the Next Generation Cisco 880 Series ISRs to Cisco IOS 15.1(4)M or later releases.

Unsupported Cisco Wireless Controller Platforms

The following Cisco WLC platforms are not supported:

- Cisco 4400 Series Wireless Controller
- Cisco 2100 Series Wireless Controller
- Cisco Catalyst 3750G Integrated Wireless Controller
- Cisco Wireless Controller software on Cisco SRE running on ISM 300, SM 700, SM 710, SM 900, and SM 910
- Cisco Catalyst 6500 Series and 7600 Series WiSM1
- Cisco Wireless Controller Module (NM/NME)

What’s New in Release 8.0.140.0

There are no new features or enhancements in this release. This release addresses critical issues with the controller software. For more information, see the Caveats, page 23 section.

Cisco 7925G Phone Support Restriction

Cisco 7925G Phones when using PEAP authentication, use legacy RC4 and DES security ciphers. Due to the changes in the Cisco AireOS to improve security, when Local EAP is used, the phones will fail authentication for PEAP. To continue to use the Cisco 7925G phones, we recommend that you change the authentication method to EAP-Fast or move the WLAN to use an external RADIUS server instead of Local EAP.

Future 8.0 releases will provide a workaround to enable backward compatibility for Local EAP with legacy crypto on client devices.

Software Release Support for Access Points

Table 2 lists the Cisco WLC software releases that support specific Cisco access points. The First Support column lists the earliest Cisco WLC software release that supports the access point. For access points that are not supported in ongoing releases, the Last Support column lists the last release that supports the access point.

Note Third-party antennas are not supported with Cisco indoor access points.

Table 2 Software Support for Access Points

Access Points		First Support	Last Support
700 Series	AIR-CAP702I-x-K9	7.5.102.0	—
	AIR-CAP702I-xK910	7.5.102.0	—
700W Series	AIR-CAP702Wx-K9	7.6.120.0	—
	AIR-CAP702W-xK910	7.6.120.0	—
1000 Series	AIR-AP1010	3.0.100.0	4.2.209.0
	AIR-AP1020	3.0.100.0	4.2.209.0
	AIR-AP1030	3.0.100.0	4.2.209.0
	Airespace AS1200	—	4.0
	AIR-LAP1041N	7.0.98.0	—
	AIR-LAP1042N	7.0.98.0	—
1100 Series	AIR-LAP1121	4.0.155.0	7.0.x
1130 Series	AIR-LAP1131	3.1.59.24	8.0.x
1140 Series	AIR-LAP1141N	5.2.157.0	8.0.x
	AIR-LAP1142N	5.2.157.0	—
1220 Series	AIR-AP1220A	3.1.59.24	7.0.x
	AIR-AP1220B	3.1.59.24	7.0.x
1230 Series	AIR-AP1230A	3.1.59.24	7.0.x
	AIR-AP1230B	3.1.59.24	7.0.x
	AIR-LAP1231G	3.1.59.24	7.0.x
	AIR-LAP1232AG	3.1.59.24	7.0.x
1240 Series	AIR-LAP1242G	3.1.59.24	8.0.x
	AIR-LAP1242AG	3.1.59.24	—
1250 Series	AIR-LAP1250	4.2.61.0	8.0.x
	AIR-LAP1252G	4.2.61.0	—
	AIR-LAP1252AG	4.2.61.0	—
1260 Series	AIR-LAP1261N	7.0.116.0	—
	AIR-LAP1262N	7.0.98.0	—
1300 Series	AIR-BR1310G	4.0.155.0	7.0.x

Table 2 Software Support for Access Points (continued)

Access Points		First Support	Last Support
1400 Series	Standalone Only	—	—
1600 Series	AIR-CAP1602I-x-K9	7.4.100.0	—
	AIR-CAP1602I-xK910	7.4.100.0	—
	AIR-SAP1602I-x-K9	7.4.100.0	—
	AIR-SAP1602I-xK9-5	7.4.100.0	—
	AIR-CAP1602E-x-K9	7.4.100.0	—
	AIR-SAP1602E-xK9-5	7.4.100.0	—
1700 Series	AIR-CAP1702I-x-K9	8.0.100.0	—
	AIR-CAP1702I-xK910	8.0.100.0	—
AP801		5.1.151.0	8.0.x
AP802		7.0.98.0	—
AP802H		7.3.101.0	—
2600 Series	AIR-CAP2602I-x-K9	7.2.110.0	—
	AIR-CAP2602I-xK910	7.2.110.0	—
	AIR-SAP2602I-x-K9	7.2.110.0	—
	AIR-SAP2602I-x-K95	7.2.110.0	—
	AIR-CAP2602E-x-K9	7.2.110.0	—
	AIR-CAP2602E-xK910	7.2.110.0	—
	AIR-SAP2602E-x-K9	7.2.110.0	—
	AIR-SAP2602E-x-K95	7.2.110.0	—
2700 Series	AIR-CAP2702I-x-K9	7.6.120.0	—
	AIR-CAP2702I-xK910	7.6.120.0	—
	AIR-CAP2702E-x-K9	7.6.120.0	—
	AIR-CAP2702E-xK910	7.6.120.0	—
	AIR-AP2702I-UXK9	8.0.110.0	—
3500 Series	AIR-CAP3501E	7.0.98.0	—
	AIR-CAP3501I	7.0.98.0	—
	AIR-CAP3502E	7.0.98.0	—
	AIR-CAP3502I	7.0.98.0	—
	AIR-CAP3502P	7.0.116.0	—
3600 Series	AIR-CAP3602I-x-K9	7.1.91.0	—
	AIR-CAP3602I-xK910	7.1.91.0	—
	AIR-CAP3602E-x-K9	7.1.91.0	—
	AIR-CAP3602E-xK910	7.1.91.0	—
	USC5101-AI-AIR-K9	7.6	

Table 2 Software Support for Access Points (continued)

Access Points		First Support	Last Support
3700 Series	AIR-CAP3702I	7.6	—
	AIR-CAP3702E	7.6	—
	AIR-CAP3702P	7.6	—
600 Series	AIR-OEAP602I	7.0.116.0	—
Note The Cisco 3600 Access Point was introduced in Release 7.1.91.0. If your network deployment uses Cisco 3600 Access Points with Release 7.1.91.0, we highly recommend that you upgrade to Release 7.2.115.2 or a later release.			
1500 Mesh Series	AIR-LAP-1505	3.1.59.24	4.2.207.54M
	AIR-LAP-1510	3.1.59.24	4.2.207.54M
1520 Mesh Series	AIR-LAP1522AG	-A and N: 4.1.190.1 or 5.2 or later[1]	—
		All other reg. domains: 4.1.191.24M or 5.2 or later[1]	—
	AIR-LAP1522HZ	-A and N: 4.1.190.1 or 5.2 or later[1]	—
		All other reg. domains: 4.1.191.24M or 5.2 or later[1]	—
	AIR-LAP1522PC	-A and N: 4.1.190.1 or 5.2 or later[1]	—
		All other reg. domains: 4.1.191.24M or 5.2 or later[1]	—
	AIR-LAP1522CM	7.0.116.0 or later.	—
	AIR-LAP1524SB	-A, C and N: 6.0 or later	—
		All other reg. domains: 7.0.116.0 or later.	—
	AIR-LAP1524PS	-A: 4.1.192.22M or 5.2 or later[1]	—

Table 2 Software Support for Access Points (continued)

Access Points		First Support	Last Support
1530	AIR-CAP1532I-x-K9	7.6	—
	AIR-CAP1532E-x-K9	7.6	—
1550	AIR-CAP1552C-x-K9	7.0.116.0	—
	AIR-CAP1552E-x-K9	7.0.116.0	—
	AIR-CAP1552H-x-K9	7.0.116.0	—
	AIR-CAP1552I-x-K9	7.0.116.0	—
	AIR-CAP1552EU-x-K9	7.3.101.0	—
	AIR-CAP1552CU-x-K9	7.3.101.0	—
	AIR-CAP1552WU-x-K9	8.0.100.0	—
1552S	AIR-CAP1552SA-x-K9	7.0.220.0	—
	AIR-CAP1552SD-x-K9	7.0.220.0	—
1570 version ID 01 (V01)	AIR-AP1572EAC-x-K9	8.0.110.0	—
	AIR-AP1572ICy[2]-x-K9	8.0.110.0	—
	AIR-AP1572ECy-x-K9	8.0.110.0	—
1570 version ID 02 (V02)[3]	AIR-AP1572EAC-B-K9	8.0.135.0	—
	AIR-AP1572EC1-B-K9	8.0.135.0	—
	AIR-AP1572EC2-B-K9	8.0.135.0	—
	AIR-AP1572IC1-B-K9	8.0.135.0	—
	AIR-AP1572IC2-B-K9	8.0.135.0	—
IW3700	IW3702-2E-UXK9	8.0.120.0	—
	IW3702-4E-UXK9	8.0.120.0	—

[1] These access points are supported in a separate 4.1.19x.x mesh software release or in Release 5.2 or later releases. These access points are not supported in the 4.2, 5.0, or 5.1 releases.

An access point must always be connected to the POE-IN port to associate with the Cisco WLCs. The POE-OUT port is for connecting external devices only.

[2] y—Country DOCSIS Compliance, see ordering guide for details.

[3] Cisco 1570 V02 APs are supported on only specific Cisco Wireless Controller software releases. For more information, see *Cisco Wireless Solutions Software Compatibility Matrix*.

Software Release Types and Recommendations

This section contains the following topics:

- Types of Releases, page 8
- Software Release Recommendations, page 8

Types of Releases

Table 3 Types of Releases

Type of Release	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 long-lived releases with ongoing software maintenance.	Provides you with a software release that offers stability and long support duration with periodic maintenance releases (MRs).
Early Deployment (ED) 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 controller and access point testing in real-world use cases with a variety of mobile client devices applicable in a specific industry.

Software Release Recommendations

Table 4 Software Release Recommendations

Type of Release	Deployed Release	Recommended Release
Maintenance Deployment (MD) release	7.0 MD release train (latest update 7.0.252.0 in Q1CY15) 7.4 MD released train (latest update 7.4.140.0 in May 2015)	8.0 MD release train (latest recommended release is 8.0.133.0)
Early Deployment (ED) releases for pre-802.11ac deployments	7.2 ED releases 7.3 ED releases	8.0 MD release train (latest recommended release is 8.0.133.0)
Early Deployment (ED) releases for 802.11ac deployments	7.5 ED release 7.6 ED release	8.0 MD release train (latest recommended release is 8.0.133.0)

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 8.0.140.0

Guidelines and Limitations

- 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.
- Cisco WLC Release 7.3.112.0, which is configured for new mobility, might revert to old mobility after upgrading to Release 7.6 or later, even though Release 7.6 supports new mobility. This issue occurs when new mobility, which is compatible with the Cisco 5760 Wireless 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 Mobility epings are not available 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, 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 8.0.140.0 to a 7.x release, the trap configuration is lost and must be reconfigured.
- If you have ACL configurations in the Cisco WLC and downgrade from a 7.4 or a later release to a 7.3 or an earlier release, you might experience XML errors on rebooting the Cisco WLC. However, these errors do not have any impact on any functionality or configurations.
- If you are upgrading from a 7.4.X or an earlier release to a later release, the Called Station ID type information is mapped to the RADIUS Accounting Called Station ID type; the RADIUS Authentication Called Station ID type, by default, is set to ap-macaddr-ssid. You can configure the RADIUS Authentication Called Station ID type information by using the **config radius auth callStationIdType** command.
- When FlexConnect access points (known as H-REAP access points 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 8.0.140.0, the access points 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 or a later 7.0.x release to Release 8.0.140.0.
- We recommend that you install Release 1.9.0.0 of Cisco Wireless 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.

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 Controller Field Upgrade Software (FUS). This is not required if you are using other controller hardware models.

Note FUS 2.0 upgrade is required for those WLCs with PIC version 1.0.19 and are impacted by CSCuu46671.

- On 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 8.0.140.0 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 8.0.140.0. Table 5 shows the upgrade path that you must follow before downloading Release 8.0.140.0.

Caution If you upgrade from a release that is prior to Release 7.5 directly to Release 7.6.X or a later release, the predownload process on Cisco AP2600 and AP3600 fails. After the Cisco WLC is upgraded to Release 7.6.X or a later release, the new image is loaded on Cisco AP2600 and AP3600. After the upgrade to a Release 7.6.X image, the predownload functionality works as expected. The predownload failure is only a one-time failure, which is limited to the predownload process.

Table 5 Upgrade Path to Cisco WLC Software Release 8.0.140.0

Current Software Release	Upgrade Path to 8.0.140.0 Software[1]
7.4.x releases	You can upgrade directly to 8.0.140.0.
7.6.x releases	You can upgrade directly to 8.0.140.0.
8.0.1x.0	You can upgrade directly to 8.0.140.0.

[1] If the network includes a mesh deployment and the new mesh PSK key security feature is used, it is not possible to upgrade Cisco WLC from Release 8.0MR4 to Release 8.1 or downgrade to Release 8.0.13x.0 or an older release to prevent disruption of the mesh network. However, you can upgrade to Release 8.2 or a later release and future 8.0 maintenance releases directly. If a downgrade or upgrade is necessary, you should revert the mesh security protocol to EAP authentication.

- 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 to all access points.
- You can upgrade to a new release of the Cisco WLC software or downgrade to an earlier release even if Federal Information Processing Standard (FIPS) is enabled.
- When you upgrade to the latest software release, the software on the access points associated with the Cisco WLC is also automatically upgraded. When an access point is loading software, each of its LEDs blinks in succession.
- We recommend that you access the Cisco WLC GUI using Microsoft Internet Explorer 9 or a later version or Mozilla Firefox 17 or a later version.

Note Older browsers, for example 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 Management Information Base (MIB) files. MIBs can be downloaded from the Software Center on Cisco.com.

- The Cisco WLC software is factory installed on your Cisco WLC and is automatically downloaded to the access points after a release upgrade and whenever an access point joins a Cisco WLC. We recommend that you install the latest software version available for maximum operational benefit.
- Ensure that you have a TFTP, FTP, or SFTP server available for the software upgrade. Follow these guidelines when setting up a server:
  - Ensure that your TFTP server supports files that are larger than the size of Cisco WLC software Release 8.0.140.0. 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 8.0.140.0 Cisco WLC software and your TFTP server does not support files of this size, the following error message appears:

    "TFTP failure while storing in flash."
  - If you are upgrading through the distribution system network port, the TFTP or FTP server can be on any subnet because the distribution system port is routable.
- When you plug a Cisco WLC into an AC power source, the bootup script and power-on self test is run to initialize the system. During this time, press **Esc** to display the bootloader Boot Options menu. The menu options for the Cisco 5500 Series WLC differ from the menu options for the other Cisco WLC platforms.

  Bootloader menu for Cisco 5500 Series WLC:

```
   Boot Options
Please choose an option from below:
 1. Run primary image
 2. Run backup image
 3. Change active boot image
 4. Clear Configuration
 5. Format FLASH Drive
6. Manually update images
Please enter your choice:
```

  Bootloader menu for other Cisco WLC platforms:

```
   Boot Options
Please choose an option from below:
 1. Run primary image
 2. Run backup image
 3. Manually update images
 4. Change active boot image
 5. Clear Configuration
Please enter your choice:
```

  Enter **1** to run the current software, enter **2** to run the previous software, enter **4** (on a 5500 series Cisco WLC), or enter **5** (on another Cisco WLC platform) 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 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 FlexConnect Configuration Guide*.

Note Predownloading Release 8.0.140.0 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.
- If you want to downgrade from Release 8.0.140.0 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 these functions on the Cisco WLC, you must 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 for a license
  - Enable the 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
  - For TCP MSS to take effect

Upgrading to Cisco WLC Software Release 8.0.140.0 (GUI)

Step 1 Upload your Cisco WLC configuration files to a server to back them up.

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 the 8.0.140.0 Cisco WLC software:

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

   https://software.cisco.com/download/navigator.html

b. Choose **Wireless** from the center selection window.

c. Click **Wireless LAN Controllers**.

   The following options are available:

   – Integrated Controllers and Controller Modules

   – Standalone Controllers

d. Depending on your Cisco WLC platform, select one of these options.

e. Click the Cisco WLC model number or name.

   The **Download Software** page is displayed.

f. Click a Cisco WLC software release number. The software releases are labeled as follows to help you determine which release to download:

   - **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.

g. Click a software release number.

h. Click the filename (*filename*.aes).

i. Click **Download**.

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

k. Save the file to your hard drive.

l. Repeat steps a. through k. to download the remaining file.

Step 3 Copy the Cisco WLC software file (*filename*.aes) to the default directory on your TFTP, FTP, or SFTP server.

Step 4 (Optional) Disable the Cisco WLC 802.11a/n and 802.11b/g/n networks.

Note For busy networks, Cisco WLCs with high utilization, or small Cisco WLC platforms, we recommend that you disable the 802.11a/n and 802.11b/g/n networks as a precautionary measure.

Step 5 Choose **Commands** > **Download File** to open the Download File to Controller page.

Step 6 From the **File Type** drop-down list, choose **Code**.

Step 7 From the **Transfer Mode** drop-down list, choose **TFTP**, **FTP**, or **SFTP**.

Step 8 In the **IP Address** text box, enter the IP address of the TFTP, FTP, or SFTP server.

Step 9 If you are using a TFTP server, the default values 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) that the TFTP server attempts to download the software, in the **Timeout** text box.

Step 10 In the **File Path** text box, enter the directory path of the software.

Step 11 In the **File Name** text box, enter the name of the software file (*filename*.aes).

Step 12 If you are using an FTP server, follow these steps:

a. In the **Server Login Username** text box, enter the username to log on to the FTP server.

b. In the **Server Login Password** text box, enter the password to log on to the FTP server.

c. In the **Server Port Number** text box, enter the port number on the FTP server through which the download occurs. The default value is 21.

Step 13 Click **Download** to download the software to the Cisco WLC.

A message appears indicating the status of the download.

Step 14 After the download is complete, click **Reboot**.

Step 15 If you are prompted to save your changes, click **Save and Reboot**.

Step 16 Click **OK** to confirm your decision to reboot the Cisco WLC.

Step 17 For Cisco WiSM2 on the Catalyst switch, check the port channel and re-enable the port channel if necessary.

Step 18 If you have disabled the 802.11a/n and 802.11b/g/n networks in Step 4, re-enable them.

Step 19 To verify that the 8.0.140.0 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 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 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 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 Download the Cisco DTLS license.

a. Go to the Cisco Product License Registration at this URL:

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

b. Click **Get Other Licenses** drop down menu.

c. Choose **IPS, Crypto, Other Licenses**.

d. Under **Wireless**, choose **Cisco Wireless Controllers (2500/5500/7500/8500/WiSM2) DTLS License**.

e. Complete the remaining steps 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. You can install the license either by using the Cisco WLC web GUI interface or the CLI:

- To install the license using the 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 this URL:

   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 19 detailed in the "Upgrading to Cisco WLC Software Release 8.0.140.0" section on page 9.

Interoperability With Other Clients in Release 8.0.140.0

This section describes the interoperability of Release 8.0.140.0 of the Cisco WLC software with other client devices.

Table 6 describes the configuration used for testing the client devices.

Table 6 Test Bed Configuration for Interoperability

Hardware/Software Parameter	Hardware/Software Configuration Type
Release	8.0.13x.0
Controller	Cisco 5508 Controller
Access points	3502, 3602, 2602, 1702, 2702, 3702, 702W
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)
RADIUS	ACS 5.3, ISE 1.2
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 lists the laptop client types on which the tests were conducted.

Table 7 Laptop Client Type List

Client Type and Name	Version
Intel 4965	13.4
Intel 5100/5300	14.3.2.1
Intel 6200	15.15.0.1
Intel 6300	15.16.0.2
Intel 6205	15.16.0.2
Intel 1000/1030	14.3.0.6
Intel 8260	18.32.0.5
Intel 7260	18.32.0.5
Intel 7265	18.32.0.5

Table 7 Laptop Client Type List

Client Type and Name	Version
Intel 3160	18.32.0.5
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)	1027.7.515.2015
Dell 1395/1397/Broadcom 4312HMG(L)	5.30.21.0
Dell 1501 (Broadcom BCM4313)	v5.60.48.35/v5.60.350.11
Dell 1505/1510/Broadcom 4321MCAG/4322HM	5.60.18.8
Dell 1515(Atheros)	8.0.0.239
Dell 1520/Broadcom 43224HMS	5.60.48.18
Dell 1530 (Broadcom BCM4359)	5.100.235.12
Dell 1540	6.30.223.215
Cisco CB21	1.3.0.532
Atheros HB92/HB97	8.0.0.320
Atheros HB95	7.7.0.358
MacBook Pro	OSX 10.11.1
MacBook Air old	OSX 10.11.1
MacBook Air new	OSX 10.11.1
Macbook Pro with Retina Display	OSX 10.11.1
Macbook New 2015	OSX 10.11.1

- Tablet: Table 8 lists the tablet client types on which the tests were conducted.

Table 8 Tablet Client Type List

Client Type and Name	Version
Apple iPad2	iOS 9.2(13C75)
Apple iPad3	iOS 9.2(13C75)
Apple iPad mini with Retina display	iOS 9.2(13C75)
Apple iPad Air	iOS 9.2(13C75)
Apple iPad Air 2	iOS 9.2(13C75)
Apple iPad Pro	iOS 9.2(13C75)
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

Table 8 Tablet Client Type List

Client Type and Name	Version
Microsoft Surface Pro 3	Windows 8.1 Driver: 15.68.3073.151
Microsoft Surface Pro 2	Windows 8.1 Driver: 14.69.24039.134
Google Nexus 9	Android 6.0
Google Nexus 7 2nd Gen	Android 5.0

- Phones: Table 9 lists the phone client types on which the tests were conducted.

Table 9 Phone 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
Apple iPhone 4S	iOS 9.2(13C75)
Apple iPhone 5	iOS 9.2(13C75)
Apple iPhone 5s	iOS 9.2(13C75)
Apple iPhone 5c	iOS 9.2(13C75)
Apple iPhone 6	iOS 9.2(13C75)
Apple iPhone 6 Plus	iOS 9.2(13C75)
HTC One	Android 5.0
OnePlusOne	Android 4.3
Samsung Galaxy S4 – GT-I9500	Android 5.0.1
Sony Xperia Z Ultra	Android 4.4.2
Nokia Lumia 1520	Windows Phone 8.1
Google Nexus 5	Android 5.1
Google Nexus 6	Android 5.1.1
Samsung Galaxy S5-SM-G900A	Android 4.4.2
Huawei Ascend P7	Android 4.4.2
Samsung Galaxy S III	Android 4.4.2
Google Nexus 9	Android 6.0
Samsung Galaxy Nexus GTI9200	Android 4.4.2
Samsung Galaxy Mega SM900	Android 4.4.2
Samsung Galaxy S6	Android 5.1.1
Samsung Galaxy S5	Android 5.0.1
Xiaomi Mi 4i	Android 5.0.2
Microsoft Lumia 950 XL	Windows 10

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 2500 Series WLCs
- Features Not Supported on WiSM2 and Cisco 5500 Series WLCs
- Features Not Supported on Cisco Flex 7500 WLCs
- Features Not Supported on Cisco 8500 WLCs
- Features Not Supported on Cisco Virtual WLCs
- Features Not Supported on Mesh Networks

Features Not Supported on Cisco 2500 Series WLCs

- Autoinstall
- Bandwidth Contract
- Service Port
- AppleTalk Bridging
- Right-to-Use licensing
- PMIPv6
- AP stateful switchover (SSO) and client SSO
- Multicast-to-Unicast

Note The features that are not supported on Cisco WiSM2 and Cisco 5500 Series WLCs are also not supported on Cisco 2500 Series WLCs.

Note Directly connected APs are supported only in the Local mode.

Features Not Supported on WiSM2 and Cisco 5500 Series WLCs

- Spanning Tree Protocol (STP)
- Port Mirroring
- VPN Termination (such as IPsec and L2TP)
- VPN Passthrough Option

  Note You can replicate this functionality on a Cisco 5500 Series WLC by creating an open WLAN using an ACL.

- Configuration of 802.3 bridging, AppleTalk, and Point-to-Point Protocol over Ethernet (PPPoE)

- Fragmented Pings on any interface
- Right-to-Use licensing

Features Not Supported on Cisco Flex 7500 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 like an AP-manager interface by default, and the access points can join on this interface.

- TrustSec SXP
- IPv6/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 flexconnect** 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 IGMP or MLD snooping.

- PMIPv6

Features Not Supported on Cisco 8500 WLCs

- TrustSec SXP
- Internal DHCP Server

Features Not Supported on Cisco Virtual WLCs

- Internal DHCP server
- TrustSec SXP
- Access points in local mode
- Mobility/Guest Anchor
- Wired Guest
- Multicast

Note FlexConnect local-switched multicast traffic is bridged transparently for both wired and wireless on the same VLAN. FlexConnect access points do not limit traffic based on IGMP or MLD snooping.

- FlexConnect central switching

Note FlexConnect local switching is supported.

- AP and Client SSO in High Availability
- PMIPv6
- WGB
- Mesh (use Flex + Bridge mode for mesh enabled FlexConnect deployments)

Note Outdoor APs in the FlexConnect mode are supported.

- Application Visibility and Control (AVC)
- Client downstream rate limiting for central switching
- SHA2 certificates

Features Not Supported on Access Point Platforms

- Features Not Supported on 1130 and 1240 APs, page 22
- Features Not Supported on 1520 and 1550 APs (with 64 MB memory), page 23

Features Not Supported on 1130 and 1240 APs

All the features introduced in Release 7.2 and later releases are not supported on 1130 and 1240 APs. In addition to these, the following features are not supported on 1130 and 1240 APs:

- Central-DHCP functionality
- Split tunneling
- Configuration of Network Address Translation (NAT) and Port Address Translation (PAT) on FlexConnect locally switched WLANs

- Point to Point Protocol (PPP) and Point to Point Protocol over Ethernet (PPPoE) for APs in FlexConnect mode
- 802.11u
- 802.11r Fast Transition
- LLDP
- Rate Limiting per AP
- mDNS AP
- EAP-TLS and PEAP for Local Authentication support as EAP method
- WLAN-to-VLAN mapping when AP part of FlexConnect Group
- Per user AAA AireSpace ACL name override
- Local MFP
- DNS-based (fully qualified domain name) access control lists (ACLs)
- Flex + Bridge mode (introduced in Release 8.0.100.0)

Features Not Supported on 1520 and 1550 APs (with 64 MB memory)

- PPPoE
- PMIPv6

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

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

Features Not Supported on Mesh Networks

- Multicountry support
- Load-based 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

- Cisco Bug Search Tool, page 24
- Open Caveats, page 24

- Resolved Caveats, page 25

Cisco Bug Search Tool

The Bug Search Tool (BST), which is the online successor to 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 listed in this document:

1. Access the BST (use your Cisco user ID and password) at https://bst.cloudapps.cisco.com/bugsearch/
2. Enter the bug ID in the **Search For:** field.

Note Using the BST, you can also find information about the bugs that are not listed in this section.

Open Caveats

Use the BST to view the details of a caveat listed in this section. For more information about the BST, see the "Cisco Bug Search Tool" section on page 24

Table 10 Open Caveats

Caveat ID Number	Headline
CSCur40006	WLC: Group size exceeded with static RF Group member add
CSCur88123	Invalid PSK for layer 2 security after controller reboot
CSCus53495	DFS detection due to Broadcom spurious emissions in Cisco 2700, 3700 Series APs
CSCus79046	CAPWAP AP does NOT fallback to IPv6 if ACL blocks IPv4 CAPWAP packets
CSCus79791	Client connected to 802.11n AP shows as 802.11ac client on WLC
CSCus90178	AIR-OEAP602I has TCP port 5162 open
CSCut81253	Ethernet Bridging does not work on RAP with 5-GHz backhaul
CSCut83422	vWLC SN changed after management interface IP change
CSCut90276	AireOS Traceback: APF-4-PROC_ACTION_FAILED
CSCuu14124	RF-profile losing the channel and coverage values after downloading configuration file
CSCuu71471	MTU value stacks in HA
CSCuv10692	AckFailureCount getting huge value in short period
CSCuv79354	Cannot configure IP address x.x.x.255 or x.x.x.0 as gateway in GUI

Table 10 Open Caveats (continued)

Caveat ID Number	Headline
CSCuw03323	Cisco 702w AP draws additional power (22.1 watts) when LAN port 4 is disabled.
CSCuw09545	Incorrect DHCP “Pool Usage” on the WLC when queried via SNMP
CSCuw27160	RF Grouping Algorithm > update interval not synchronized on controllers
CSCuw70789	AP using a reserved port to join the WLC
CSCux01697	WLC negative SNR values reported
CSCux25323	Unable to configure the native VLAN on FlexConnect ap.
CSCux80925	Media Stream - Not greyed out on Traffic profile Violation
CSCux99806	WGB in Cisco 2602 AP goes for a sleep and end up not responding for 100ms
CSCuy63742	Accounting commands send inconsistently to TACACS+ server for rapid commands
CSCuy70124	WLC does not send trap for port down on HA standby WLC
CSCuz69650	Cisco 1140 AP beacon outage issue
CSCva13929	Flex Data DTLS enabled AP gets stranded with WAN link flap
CSCva47491	AP load information does not clear or reset after AP Radios are disable
CSCvd06463	IOS AP doing AMSDU aggregation for voice traffic in queue 0 despite BA request declined by Cisco Wireless IP Phone 8821
CSCvc65568	Cisco Wireless IP Phone 8821 fails 802.11r FT roam with 'Invalid FTIE MIC'

Resolved Caveats

Use the BST to view the details of a caveat listed in this section. For more information about the BST, see the “Cisco Bug Search Tool” section on page 24.

Table 11 Resolved Caveats

Caveat ID Number	Headline
CSCug98522	PMIPv6: MAG delivering multiple DNS servers to clients
CSCuo04528	Way to save MSGLOGS or TRAPLOGs in a buffer on Cisco WLC flash when rebooted
CSCup29095	Cisco Mesh: Prime Infrastructure not showing the neighbor details in mesh links page of Parent
CSCup85228	AP IO memory leak in DPAA module
CSCup92480	802.11ac module reloads unexpectedly due to PCI reset
CSCup97263	Cisco Flex 7510 WLC System reloads unexpectedly on Dot1x_NW_MsgTask_2
CSCuq36265	Cisco Aironet 3600 with 802.11ac module non-broadcast SSID client connectivity issues

Table 11 Resolved Caveats (continued)

Caveat ID Number	Headline
CSCuq45110	M1 is sometimes encrypted; leading to M1 refusal on station side
CSCuq71837	Control Path Last Flap Time shown wrong on mobility statistics
CSCuq75748	Multicast configuration SET failing to commit
CSCuq86263	False DFS detection on Cisco1600 AP
CSCuq89123	WLC: No debugs enabled, but debug invalid module messages in log
CSCur02514	Cisco 8.0.100.0 release: SNMP trap is not sent out on HA switch-over
CSCur17406	AP impersonation appearing for Cisco 1530 AP(s)
CSCur53809	Cisco 2702AP sometimes unable to receive packets or ACK from STA with 20MHz wide channel
CSCur68316	Cisco 802 AP in FlexConnect mode are losing VLAN mapping after power cycle
CSCur80841	Apple remote app not working with MDNS snooping enabled
CSCur94843	External web authentication URL goes through loop and never gets the login page
CSCus06589	Cisco 2700 AP flooding AP sourced packets out of Aux Gig 1 port
CSCus46848	Cisco WLC hangs on RF-profile page if too many RF-profiles are created
CSCus49607	Cisco 5500 Series WLC HA reloads unexpectedly with taskname:tosapiReaper
CSCus50404	AP Name is mismatched between controller and AP
CSCus52826	Cisco 8.1 release: rogue client detection on serving channel on wIPS enabled non monitor APs
CSCus52828	SNMPv3 rw user credentials not working if key length is more than 32
CSCus55192	Cisco 8500 WLC reloads unexpectedly during removing SNMP Communities
CSCus58120	Traplog is wrong about temperature status
CSCus58468	Multicast Address set issue using SNMP
CSCus61679	Problem in client statistics reports
CSCus68363	Rogue policies are not applied correctly
CSCus71140	Bonjour service learnt via MDNS AP is being forwarded to wired
CSCus79056	Cisco 5508 WLC- management frames are not marked with CS6
CSCus80562	Power client does not work
CSCut10131	WLC fails to resend ciscoLwappDot11ClientMovedToRunState traps
CSCut10668	Cisco 1570 AP: RADIO_OVER_TEMPERATURE, Cisco WLC still shows AP radio is up
CSCut12606	Remove auto-containment from high security level setting
CSCut27312	AP group VLAN not overridden on client when AAA override is enabled on the WLAN
CSCut35315	Negative rogue count reported in show rogue ap summary - GUI changes
CSCut40765	Cisco WLC reporting incorrect “”remote address”” to TACACS+ sever
CSCut44986	Cisco WLC is throwing error when accounting is disabled on WLAN

Table 11 Resolved Caveats (continued)

Caveat ID Number	Headline
CSCut55043	FlexConnect Group with space in name renders terminal session unusable
CSCut60058	Cisco WLC does not deauthenticate client when AAA Flex-ACL is not present on AP
CSCut61668	AID errors on the controller for FlexConnect APs
CSCut63868	Cisco 8500 WLC reloads unexpectedly on Taskname emWeb
CSCut64180	AP holds bandwidth after call when WLC HA SO happens during call setup
CSCut76824	Anchor WLC will not forward DHCP request to the DHCP server
CSCut88319	FF08:/16 range of organization-local IPv6 multicast addresses
CSCut91086	Client associated to MAP does not get AAA override in Flex+Bridge mode
CSCut92934	Cisco vWLC - AP with expire mic not able to join with ignore mic settings
CSCut96691	TFTP address for AP core dump is goofed up after HA switchover
CSCuu07744	Interface is not created when we have both ACL and WLAN-VLAN mapping
CSCuu08012	Cisco 2700 AP: CleanAir sensor died (src/dspm_main.c:389) - slot 0
CSCuu13860	’autoconvert flexconnect’ is stored as ‘disable’ on startup-commands
CSCuu16052	Do not set DF bit for non-capwap traffic from WLC such as RADIUS
CSCuu17338	Cisco 1142 AP configuration loss after cold reboot
CSCuu21625	Session not cleared on Cisco 5508 WLC anchor with Cisco 3850 foreign causing authentication issues
CSCuu33740	Cisco WLC reloads unexpectedly onwhile editing SNMP community - waFormSubmit_snmp_comm_list
CSCuu42378	RxSOP threshold not working correctly
CSCuu52409	SNMP: Providing MIBS support for out-of-box feature
CSCuu59340	SNR alarms for mesh APs have invalid content, not working as expected
CSCuu60475	Cisco 3702 AP in CI reloads unexpectedly in Process: Net Background
CSCuu83548	Traceback observed in export-foreign standby WLC while disassociating client
CSCuu89294	Primary AP in Flex Group not saved in WLC configuration nor in commands backup
CSCuu91943	Cisco 8510 WLC reloads unexpectedly while accessing the controller crash file information through GUI
CSCuu97320	Flex+Bridge&SE-Connect filtering back to uncheck after Change Filter
CSCuv03380	During Mesh Roam sec error gateway not reachable leading to CAPWAP restart
CSCuv03937	Unexpected WLC reload with RLDP enabled
CSCuv16756	Cisco 5500 WLC reloads unexpectedly on coredump spamApTask4 spamSendConfigRequestInfo
CSCuv16895	MAP count shown wrongly in “show mesh ap summary” command in WLC CLI
CSCuv29025	Mobility domain name displayed as junk if created in UTF-8 character

Table 11 Resolved Caveats (continued)

Caveat ID Number	Headline
CSCuv33255	AP CDP neighbor information is missing or outdated
CSCuv34176	Transmitter Stop Radio reset due DTIM Multicast Pak stuck
CSCuv36306	AP sensord_crashFile No CleanAir measurements
CSCuv40794	AP Impersonator alarm for Cisco 3602i AP
CSCuv43125	mdnsQueryDelayHandler tracebacks in Cisco Release 8.0 WLC flooding syslog server
CSCuv43466	Garbage character are shown in CLI show run-config startup-command
CSCuv62540	Adding -S domain support for Hong Kong; Macau; Thailand and Vietnam
CSCuv86345	Upgrade WiSM2 WLC from 8.1 to 8.2 releases and performing SSO changes mobility MAC
CSCuv97132	Show ap image all output will not fetch spamPreDownLoadInProgress
CSCuv99415	AP should bootup even if CAPWAP IOS download was corrupted
CSCuv99434	Roams using PMF + OKC not working correctly
CSCuw02258	Severity Filter for Monitoring CleanAir interferes does not work
CSCuw03318	GUI does not pop up an error when a duplicated PSK key is provisioned
CSCuw10445	SNMP optimization for the client and AP MIBS
CSCuw18306	Cisco Mesh AP 5-GHz channel on non-configured channel in DCA list on WLC
CSCuw21213	Downstream: QoS Bronze Profile not marking traffic to AF11 on Cisco FlexConnect
CSCuw23023	Cisco 3700 AP Sniffer Mode not capturing on 5-GHz radio with Rx-SOP set
CSCuw29539	Cisco 1552E series AP running lightweight IOS will not discover WLC using DNS
CSCuw30129	Debugging logging quickly falls behind real-time
CSCuw30644	Cisco 702W AP 2.4GHz radio showing low to no throughput at random times
CSCuw34565	Cisco 7500 WLC reloads unexpectedly after deleting AP crash logs from GUI
CSCuw36069	Threshold MIBs incorrectly set for WSSI modules
CSCuw38795	Cisco 5508 WLC reloads unexpectedly upon pushing RF calibration template from PI
CSCuw41092	AP not send traffic indication in beacon for power-save client after FT
CSCuw61132	Need Cisco 5508 WLC to support sleeping client as single anchor with NGWC
CSCuw61901	Local authentication EAP-FAST is not working for Flex AP user authentication with Cisco AnyConnect
CSCuw62172	System reloads unexpectedly on HA standby while setting authentication priority order from PI in 7.6 release
CSCuw65933	Client statistics mismatch in client roaming scenarios
CSCuw66299	Cisco WLC msglog showing NMSP transmit failure even when there is no MSE
CSCuw80470	Controller reloads unexpectedly on radiusTransportThread

Table 11 Resolved Caveats (continued)

Caveat ID Number	Headline
CSCuw81352	Unwanted debug messages : Wired client head is NULL
CSCuw86320	AP had multiple issues with reason ‘offchannel request stuck’
CSCuw95126	Optimized Roaming Rejection function does not work
CSCux00803	New Mobility clients stuck in DHCP_REQD state with NAT IP on Foreign
CSCux08557	Reaper reset because of SNMPTASK : VALIDATE_GUEST_SESSION_FAILED
CSCux23003	8dBm max power for -Z, -T domain APs in channels 36 through 64
CSCux24575	Release 8.2.15.5 - MAPs are unstable if convergence is standard
CSCux25143	WLC: SNMP task memory leak in 8.3 in k_mib_cisco_lwapp_ap
CSCux28775	WLC per-WLAN client traffic stats accuracy enhancements
CSCux32328	Token Bucket leak with QoS Roles and with WebAuth on 8.0.120.2
CSCux34439	802.11ac module: 802.11ac clients can not connect to Cisco 3600 AP radio slot2
CSCux45077	Cisco 3500 AP reloads unexpectedly due to LWAPP CLIENT process
CSCux51833	Client fails on RAP with AAA Override ACL when AP is in Flex+Bridge mode
CSCux53607	WLC SNMP for cLAPGroups802dot11bgRFProfileName returns wrong value
CSCux57925	Controller entering yellow zone at 1.6 GB with Teredo traffic
CSCux58427	Clients cannot connect, drops and high latency pings to Cisco WLC management interface
CSCux58953	Cannot set channel from web interface
CSCux59359	Cisco 8510 WLC behind NAT on New mobility and client stuck in DHCP_REQD state
CSCux59592	Wrong message in message log about ACL
CSCux60012	With New Mobility-Mobility members do not survive reload
CSCux62529	Lightweight AP reloads unexpectedly at disc_client_txq_dump
CSCux62936	IPv6 address delete in MSCB failing when client hops between WLANs
CSCux63218	Upgrade to 8.0 moved APs to EAP-MD5 authentication on wired 802.1x
CSCux63449	WLC running 8.0.120.0 release reloads unexpectedly on TransferMsgPeerSend
CSCux69221	HP printer not seen by iOS devices after returning from sleep mode
CSCux73555	8.0MR3: Make 802.11v DMS on WLAN configurable using Web UI
CSCux74970	MAG with PMIPv6 does not assign secondary DNS to clients via DHCP
CSCux78389	RADIUS failover should failover both authentication account server on WLAN
CSCux78464	WLC reloads unexpectedly running Process Bonjour_Process_Task
CSCux82955	Anchor WLC not forward DHCP request to server as VLAN is set as 0
CSCux85357	WLC sends GARP for flex local switching clients after HA switch-over

Table 11 Resolved Caveats (continued)

Caveat ID Number	Headline
CSCux90031	Intermittent multiple packet and ping drop between RAP and Cisco 1572 mesh AP
CSCux91996	Rogue containment not starting if no client info on best RSSI AP
CSCux95662	PMIPv6 client fails to get an IP if there is no DHCP server configured
CSCux96500	WiSM2 reloads unexpectedly on bcastReceiveTask
CSCux96731	Data plane reloads unexpectedly on Cisco 8500 WLC
CSCuy02774	PMIPv6 client binding clean up issues
CSCuy02853	DNS-ACL: debug profiling events and error print junk characters in AP console
CSCuy04572	Wrong time stamp sent on rogue traps when delta value set on controller
CSCuy08305	Client deleted because of Intra AP Roam event
CSCuy11885	Cisco 3500 AP reloads unexpectedly due to Pid 128: Process CAPWAP CLIENT
CSCuy12943	WLC running 8.1 release: Unknown emWeb error message
CSCuy13549	Flex group push eap-md5 supplicant config to APs
CSCuy13829	Cisco 2602I AP reloads unexpectedly on dot11_pmkid_timeout
CSCuy14547	HA configuration sync failed
CSCuy20175	Windows clients machine and user authentication failing when doing inter-WLC roaming
CSCuy31302	AVC profile on a local policy not removed on recreation of the policy
CSCuy31962	APs detect different WPA Support value from Rogue AP
CSCuy33247	AP send disassociation frames twice and optimized roaming go wrong
CSCuy34975	WLC 5508 running 8.0.120.0 release reloads unexpectedly when adding SSID to friendly rule
CSCuy37694	Cisco WLC reloads unexpectedly on running 8.0.120.0 at task apfRogueTask_1
CSCuy41330	Error in setting trap port number on SNMP system summary page
CSCuy42458	FlexConnect ACL allows ACL names with spaces in CLI
CSCuy47407	Client leak at anchor controller
CSCuy48983	Cisco 2702 AP radio reset due to encryption engine stuck BZ738[BZ1180].
CSCuy52607	Data Plane reloads unexpectedly on cvmcs_StaToDS
CSCuy52757	GUI does not display any rogue APs information
CSCuy53556	RADIUS deactivated message should define authentication or accounting
CSCuy53596	Cisco CleanAir fatal error and radio reset on Flex+Bridge AP
CSCuy53775	Device reloads unexpectedly in osapiReaper (fatal condition at broffu_fp_dapi_cmd.c)
CSCuy54406	Flex SSID going to centrally switched WLANs list
CSCuy57627	Universal AP admin security risk

Table 11 Resolved Caveats (continued)

Caveat ID Number	Headline
CSCuy57687	No RF-group membership information when RF-gr member is MA
CSCuy58091	Evaluation of WLC for OpenSSL March 2016
CSCuy60049	Observed Cisco AP non responsive in local mode
CSCuy61463	PM4:%AAA-3-CALLED_STATION_ATTRIBUTE_GET_FA: aaa.c:3021
CSCuy63671	Not able to edit mobility group member with edit all option from web GUI
CSCuy64520	Access Points (AP) sending CDP packets to the wireless clients
CSCuy65492	Clean-air details not showing up on GUI On Mobility controller
CSCuy70474	Missing device information in local profiling device statistics
CSCuy70671	Client's mobility role becomes local during F-F roaming in GA web authentication
CSCuy73622	Time sync failure for mmMsg_HandoffComplete on MC not printed on debugs
CSCuy73979	WLC Data Plane reloads unexpectedly
CSCuy75241	Cisco 5508 system reloads unexpectedly with task mmMobility
CSCuy76410	Unwanted logs are coming in debug aaa events and MSK gets printed
CSCuy78583	Invalid AID reported by standby for client joining in Flex AP
CSCuy82754	Cisco 5508 WLC: process queue. enqueue failed. due to local authentication failures
CSCuy82849	Memory leak found@mm_heartbeat module on guest anchor WLC
CSCuy83690	Backup controller configuration fails to sync to standby
CSCuy83951	HA: configuration sync failure in mDNS profile
CSCuy84467	Cisco FlexConnect: AP specific WLAN - VLAN change is not pushed to the AP
CSCuy86428	New mobility: Able to configure same multicast for MC and SPG
CSCuy86827	SNMP community, IPSec PSK configuration with HEX is not working
CSCuy87117	Not able to add the MIC with certificate type as MIC under AP policy
CSCuy87337	FT and adaptive option disappears in GUI with L2 security as WPA+WPA2
CSCuy92423	Central Web Authentication (CWA) broken in beta 8.0.122.50 release image
CSCuy92693	Cisco FlexConnect: ACL returned from AAA is not synced to standby
CSCuy94534	Cisco 2700 and 3700 APs on DFS do not see Cisco 2700 or 3700 APs as neighbor when RxSOP is set at High/Med/Low
CSCuy95327	802.1x frames are not marked with DSCP CS4
CSCuy98783	AP reloads unexpectedly in a loop after upgrade on 8.3 release and 8.0mr3 release
CSCuz02387	Mobility tunnel does not come up after changing the mobility group
CSCuz02871	Web authenticated ACL is not pushed from Flexgroup when a new WLAN is added to AP
CSCuz03657	New mobility: ** LOCK ASSERT ** (mmMaListen) !! reloads unexpectedly on Cisco WiSM2 GA WLC

Table 11 Resolved Caveats (continued)

Caveat ID Number	Headline
CSCuz05437	System reloads unexpectedly with task name: sshpmMainTask
CSCuz11663	Cisco 8.2 MR1 Longevity - Cisco 5508 WLC primary reloads unexpectedly on taskname - aaaQueueReader
CSCuz15763	Flex Data DTLS enabled AP gets stranded with WAN link flap
CSCuz16883	Address registration issues for mobility scenarios
CSCuz17680	Cisco Flex 7510 WLC reloads unexpectedly after enabling the enhanced client traps
CSCuz18014	GA Hardening: Enhancement of mobility msg(EA/EF msg) - phase1
CSCuz18040	GA Hardening: Enhancement of mobility msg(HC/client del msg) - phase2
CSCuz18317	WiSM2 does not provide all respective license OIDs in SNMP response
CSCuz18811	FlexConnect: Local Switching WLAN is changing to Central Switching WLAN on add
CSCuz18869	Cisco WLC picking up the unicast DHCP for unknown destination
CSCuz18914	Cisco 8.0 MR4 release: FT Over-the-air roam does not work
CSCuz22367	Cisco 3502 AP reloads unexpectedly in LWAPP RM Receive process
CSCuz22387	New mobility: NAT public IP change and reverting bring down control path
CSCuz23501	WiMAX register changes for Channel 153 for issues with Broadcom and QCA client
CSCuz23758	Local profiling not sorting correctly, not corrected on 8.0.132 release
CSCuz24121	Bonjour and mDNS incorrectly disabled on Cisco 2500 WLC platforms
CSCuz24258	Memory leak due to OpenSSL debug infra
CSCuz26426	UI: Adding URL domain to ACL is throwing error
CSCuz26463	New mobility: switch peer group multicast IP address is not shown
CSCuz26773	FlexConnect: split ACLs cannot be pushed to the AP
CSCuz28501	Cisco FlexConnect APs fail to join WLC after Fault tolerance
CSCuz28853	Background scanning enabled in 8.0 release
CSCuz29259	Traceback is seen when message queue RLDP-Q is nearing full
CSCuz31305	Random blank field in rogue summary > active rogue ap > detail page
CSCuz33087	GUI does not allow config of SSID with beginning space in Rogue rule
CSCuz33818	Profiler: double free issue
CSCuz33933	Configuration upload and download with mobility, configuration shows group error
CSCuz34485	Rogue AP entry page showing incorrect no of rogue entry range
CSCuz34615	FlexConnect: External web authenticated ACL plumbed in AP incorrectly
CSCuz35221	Mobility handoff fails in new mobility 802.1x CWA client reconnect
CSCuz38059	Anchor WLC does not free Client Sessions - client entries stale
CSCuz39340	CAPWAP payload aggregation while join of APs

Table 11 Resolved Caveats (continued)

Caveat ID Number	Headline
CSCuz39368	NOS module sometime showing as interface no:2(unknown type), in trap msg
CSCuz39417	WLC reloads unexpectedly with SHOW LICENSE FILE command
CSCuz40055	Actual AP doing containment is more than manually set containment level
CSCuz40066	Guest Anchor: Foreign to Foreign roam fails on GA scenario
CSCuz40263	Cisco wIPS reloads unexpectedly on memory corruption during fuzz testing
CSCuz40970	Cisco 8510 WLC anchor reloads unexpectedly on task osapiBsnTimer
CSCuz42595	Debug mac addr <ap-mac>' broken in 8.0 release unable to get per AP CAPWAP logs
CSCuz44066	AAA shared secret is shown in clear text on flex AP
CSCuz45298	Enhance the CLI for client summary to include akmtypes
CSCuz45831	Adhoc rogue classified as friendly internal is not shown sh adhoc rogue
CSCuz47732	WLC reloads unexpectedly on task name "radiusTransportThread"
CSCuz47786	FlexConnect AP sending IGMP report to WLC for local switching WLAN
CSCuz47863	SHA256 self-signed certificate for WLC web admin
CSCuz48979	AP: radio reset and core dump: FW: cmd=0x2C seq=6, @7601422F,s@76013F12
CSCuz49333	Time zone index was changed
CSCuz49482	FlexConnect: WLAN config stays in ap-specific on moving from one AP group to another
CSCuz49616	WLAN-VLAN mapping incorrect when AP moves across AP-Groups of different WLANs
CSCuz49801	Active configurations not syncing to standby when rogue detection security high
CSCuz49802	Band select fails for Client RSSI field > 8.0 WLC
CSCuz49968	Cisco WLC running 8.0 MR4 release reloads unexpectedly during SNMP set operation
CSCuz52435	Evaluation of Cisco WLC for OpenSSL May 2016
CSCuz53350	DNS update of RADIUS servers fails with IPv4 and IPv6 records
CSCuz53866	RF group is not formed. Group member is not added to static leader
CSCuz56009	Client reassociation not happening when central DHCP is enabled
CSCuz56479	Cisco WLC cLReapApVlanInheritance object not taking WLAN specific value
CSCuz57472	IPv6 not getting disabled on Cisco 8510 WLC running 8.0.120.0 release causing mcast Q full
CSCuz58011	FlexConnect: WLAN is not removed from the AP
CSCuz59734	Cisco 1572 AP: proper support for -B domain- VID:02 FCC requirements
CSCuz62013	WLC sends system name as NASID in accounting stop instead of WLAN NASID
CSCuz63274	mDNS snooping drops IPv6 mDNS traffic

Table 11 Resolved Caveats (continued)

Caveat ID Number	Headline
CSCuz63877	F to F roam failed with L3 roam Cisco 8510 WLC anchor with Cisco 5508 WLC foreign behind NAT
CSCuz64702	Cisco 5520 WLC running 8.3 release reloads unexpectedly on task-ApfGuest TB apfGuestTask&apfRemove...WiredClientList
CSCuz64820	Cisco 2702 AP reloads unexpectedly running 'LWAPP REAP PROCESS'
CSCuz65797	New mobility: Guest anchor controller reloads unexpectedly at mmMaListen
CSCuz70131	GUI not show rogue AP or clients till we hit show rogue summary from CLI
CSCuz70197	Authentication fails junk characters seep clients in GA and session timeout issues
CSCuz71587	Not able to push the FlexConnect template from Prime Infrastructure to WLC
CSCuz72994	FT clients reassociation denied leading to full association
CSCuz73971	Sleeping client entry deletion for AAA reject
CSCuz74146	Cannot edit dynamic interface if WLAN is enabled and mapped to management
CSCuz75862	Disabling sleeping client on the WLAN should clear the cached credential
CSCuz77747	FlexConnect: AP 1602 loses native VLAN configuration on reload
CSCuz77859	FlexConnect: AP specific DHCP-NAT-PAT config does not apply in the WLC
CSCuz78359	Guest anchor CWA: Client may lose IP while moving to RUN state
CSCuz78555	Bulk sync status "In-progress" after standby boots up
CSCuz79869	Cisco 8510 WLC reloads unexpectedly
CSCuz81415	1msec delay in processing IGMP packets causing roadcast queue to remain full
CSCuz83936	Cisco 1572 AP does not list the newer -B channels
CSCuz86679	Cisco WLC reloads unexpectedly on SNMPTask
CSCuz91317	Foreign not exporting client information to anchor
CSCuz96264	Rogue Client detect is showing 0, there is rogue client on Rogue AP
CSCva03376	UX-AP3702i After primed carrier set 5GHz only allowing four UNII3 channels
CSCva08662	Sleeping client entry on session timeout
CSCva08694	FlexConnect: WLC reloads unexpectedly while adding Central DHCP in FlexGroup
CSCva14667	GET on AP groups table after set - response missing
CSCva15190	WLC CCX client location calibration shows low cLD11ClientCalibSamplesCollected
CSCva17630	WLC sends warm-start trap instead of cold-start during autoprovisioning
CSCva26821	Auto Anchor Deployment: scheduling deletion of mobile station fails
CSCva28652	ICMP tracker message
CSCva32509	Layer 3 client roam fails on controller running Cisco 8.0.134.26 release
CSCva33212	Reintroduce auto provisioning feature on WLC 2504 running 8.0

Table 11 Resolved Caveats (continued)

Caveat ID Number	Headline
CSCva41482	Autonomous AP does not forward ARP requests to client on tag VLAN
CSCva47891	WLC reloads unexpectedly at task 'EAP_Framework_0'
CSCva49651	Flex Data DTLS enabled, WLC to flush old data DTLS sessions on WAN flap
CSCva55011	System reloads unexpectedly on Task Name redXmlTransferMain running with HA SSO
CSCva76317	WLC reloads unexpectedly with taskname TransferTask
CSCva86353	Cisco 5508 WLC reloads unexpectedly on 'apfMsConnTask_7' on 8.0.132.0 code
CSCva87295	Flex AP radio reset during FT with Central DHCP and Nat-pat enabled

Installation Notes

This section contains important information to keep in mind when installing Cisco WLCs and access points.

Warnings

Warning **This warning means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device.** Statement 1071

Warning **Only trained and qualified personnel should be allowed to install, replace, or service this equipment.** Statement 1030

Warning **Do not locate the antenna near overhead power lines or other electric light or power circuits, or where it can come into contact with such circuits. When installing the antenna, take extreme care not to come into contact with such circuits, as they may cause serious injury or death. For proper installation and grounding of the antenna, please refer to national and local codes (e.g. U.S.: NFPA 70, National Electrical Code, Article 810, Canada: Canadian Electrical Code, Section 54).** Statement 280

Warning **This product relies on the building's installation for short-circuit (overcurrent) protection. Ensure that a fuse or circuit breaker no larger than 120 VAC, 15A U.S. (240 VAC, 10A international) is used on the phase conductors (all current-carrying conductors).** Statement 13

Warning **This equipment must be grounded. Never defeat the ground conductor or operate the equipment in the absence of a suitably installed ground connector. Contact the appropriate electrical inspection authority or an electrician if you are uncertain that suitable grounding is available.** Statement 1024

Warning **Read the installation instructions before you connect the system to its power source.** Statement 10

Warning **Do not work on the system or connect or disconnect any cables (Ethernet, cable, or power) during periods of lightning activity. The possibility of serious physical injury exists if lightning should strike and travel through those cables. In addition, the equipment could be damaged by the higher levels of static electricity present in the atmosphere.** Statement 276

Warning **Do not operate the unit near unshielded blasting caps or in an explosive environment unless the device has been modified to be especially qualified for such use.** Statement 364

Warning **In order to comply with radio frequency (RF) exposure limits, the antennas for this product should be positioned no less than 6.56 ft. (2 m) from your body or nearby persons.** Statement 339

Warning **This unit is intended for installation in restricted access areas. A restricted access area can be accessed only through the use of a special tool, lock and key, or other means of security.** Statement 1017

Safety Information

Follow the guidelines in this section to ensure proper operation and safe use of the Cisco WLCs and access points.

FCC Safety Compliance Statement

FCC Compliance with its action in ET Docket 96-8, has adopted a safety standard for human exposure to RF electromagnetic energy emitted by FCC-certified equipment. When used with approved Cisco Aironet antennas, Cisco Aironet products meet the uncontrolled environmental limits found in OET-65 and ANSI C95.1, 1991. Proper operation of this radio device according to the instructions in this publication results in user exposure substantially below the FCC recommended limits.

Safety Precautions

For your safety, and to help you achieve a good installation, read and follow these safety precautions. They might save your life!

1. If you are installing an antenna for the first time, for your own safety as well as others, seek professional assistance. Your Cisco sales representative can explain which mounting method to use for the size and type of antenna you are about to install.
2. Select your installation site with safety as well as performance in mind. Electric power lines and phone lines look alike. For your safety, assume that any overhead line can kill you.
3. Call your electric power company. Tell them your plans and ask them to come look at your proposed installation. This is a small inconvenience considering your life is at stake.
4. Plan your installation carefully and completely before you begin. Successfully raising a mast or tower is largely a matter of coordination. Each person should be assigned to a specific task and should know what to do and when to do it. One person should be in charge of the operation to issue instructions and watch for signs of trouble.
5. When installing an antenna, remember:
   a. Do not use a metal ladder.
   b. Do not work on a wet or windy day.
   c. Do dress properly—shoes with rubber soles and heels, rubber gloves, long-sleeved shirt or jacket.
6. If the assembly starts to drop, get away from it and let it fall. Remember that the antenna, mast, cable, and metal guy wires are all excellent conductors of electrical current. Even the slightest touch of any of these parts to a power line completes an electrical path through the antenna and the installer: **you!**
7. If any part of an antenna system should come in contact with a power line, do not touch it or try to remove it yourself. Call your local power company. They will remove it safely.
8. If an accident should occur with the power lines, call for qualified emergency help immediately.

Installation Instructions

See the appropriate quick start guide or hardware installation guide for instructions on installing Cisco WLCs and access points.

Note To meet regulatory restrictions, all external antenna configurations must be installed by experts.

Personnel installing the Cisco WLCs and access points must understand wireless techniques and grounding methods. Access points with internal antennas can be installed by an experienced IT professional.

The Cisco WLC must be installed by a network administrator or qualified IT professional, and the proper country code must be selected. Following installation, access to the Cisco WLC should be password protected by the installer to maintain compliance with regulatory requirements and ensure proper unit functionality.

Service and Support

Troubleshooting

For the most up-to-date, detailed troubleshooting information, see the Cisco TAC website at this URL:

http://www.cisco.com/c/en/us/support/index.html

Click **Product Support** > **Wireless**. Then choose your product and **Troubleshooting** to find information on the problem you are experiencing.

Related Documentation

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 Controller Configuration Guide*
- *Cisco Wireless Controller Command Reference*
- *Cisco Wireless Controller System Message Guide*
- *Cisco Wireless Mesh Access Points, Design and Deployment Guide*

You can access these documents at:

http://www.cisco.com/c/en/us/support/index.html

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), 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 delivers content directly to your desktop using a reader application. The RSS feeds are a free service.

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.