Release Notes for Cisco Wireless LAN Controllers and Lightweight Access Points for Release 7.6.110.0

First Published: March 2014

Last Updated: July 16, 2014

OL-30342-02

These release notes describe what is new in this release, instructions to upgrade to this release, and open and resolved caveats for this release. Unless otherwise noted, all Cisco Wireless LAN Controllers are referred to as *Cisco WLCs*, and all Cisco lightweight access points are referred to as *access points* or *Cisco APs*.

Contents

These release notes contain the following sections:

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

Cisco Wireless LAN Controller and Access Point Platforms

The section contains the following subsections:

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

Supported Cisco Wireless LAN Controller Platforms

The following Cisco WLC platforms are supported in this release:

- Cisco 2500 Series Wireless LAN Controllers
- Cisco 5500 Series Wireless LAN Controllers
- Cisco Flex 7500 Series Wireless LAN Controllers
- Cisco 8500 Series Wireless LAN Controllers
- Cisco Virtual Wireless Controllers on Cisco Services-Ready Engine (SRE) or Cisco Wireless LAN Controller Module for Integrated Services Routers G2 (UCS-E)
- Cisco Wireless Controllers for high availability (HA Cisco WLCs) for the Cisco 2500 Series, 5500 Series, Wireless Services Module 2 (WiSM2), Flex 7500 Series, and 8500 Series WLCs
- Cisco WiSM2 for Catalyst 6500 Series Switches

Supported Access Point Platforms

The following access point platforms are supported in this release:

- Cisco 1040, 1130, 1140, 1240, 1250, 1260, 1600, 2600, 3500, 3500p, 3600, 3700, Cisco 600 Series OfficeExtend Access Points, 700 Series, AP801, and AP802
- Cisco Aironet 1530 Series outdoor 802.11n mesh access points, Cisco Aironet 1550 (1552) Series outdoor 802.11n mesh access points, Cisco Aironet 1520 (1522, 1524) Series outdoor mesh access points
- 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

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

Note Before you use an AP802 series lightweight access point with Cisco WLC software release 7.6.110.0, 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 LAN Controller Platforms

The following Cisco WLC platforms are not supported:

- Cisco 4400 Series Wireless LAN Controller
- Cisco 2100 Series Wireless LAN Controller
- Cisco Catalyst 3750G Integrated Wireless LAN Controller
- Cisco Wireless LAN 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 WiSM
- Cisco Wireless LAN Controller Module (NM/NME)

What's New in This Release

There are no new features or enhancements in this release. For information about features introduced in Release 7.6.100.0, see http://www.cisco.com/c/en/us/td/docs/wireless/controller/release/notes/crn76.html.

For more information about updates in this release, see the "Caveats" section on page 22.

Software Release Support for Access Points

Table 1 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 1 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	—
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	—
1140 Series	AIR-LAP1141N	5.2.157.0	—
	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	—
	AIR-LAP1242AG	3.1.59.24	—
1250 Series	AIR-LAP1250	4.2.61.0	—
	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
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	—
AP801		5.1.151.0	—
AP802		7.0.98.0	—
AP802H		7.3.101.0	—

Table 1 Software Support for Access Points (continued)

Access Points		First Support	Last Support
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	—
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	
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 7.2.103.0 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

Table 1 Software Support for Access Points (continued)

Access Points		First Support	Last Support
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]	—
1530	AIR-CAP1532I-x-K9	7.6	—
	AIR-CAP1532E-x-K9	7.6	—
1550	AIR-CAP1552I-x-K9	7.0.116.0	—
	AIR-CAP1552E-x-K9	7.0.116.0	—
	AIR-CAP1552C-x-K9	7.0.116.0	—
	AIR-CAP1552H-x-K9	7.0.116.0	—
	AIR-CAP1552CU-x-K9	7.3.101.0	—
	AIR-CAP1552EU-x-K9	7.3.101.0	—
1552S	AIR-CAP1552SA-x-K9	7.0.220.0	—
	AIR-CAP1552SD-x-K9	7.0.220.0	—

[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.

Software Release Types and Recommendations

This section contains the following topics:

- Types of Releases, page 7
- Software Release Recommendations, page 8
- Solution Compatibility Matrix, page 8

Types of Releases

Table 2 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 LAN 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 3 Software Release Recommendations

Type of Release	Deployed Release	Recommended Release
Maintenance Deployment (MD) release	7.0 MD release train	7.4 MD release train
Early Deployment (ED) releases for pre-802.11ac deployments	7.2 ED releases 7.3 ED releases	7.4 MD release train (7.4.121.0 is the minimum recommended release)
Early Deployment (ED) releases for 802.11ac deployments	7.5 ED release	7.6 ED release

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.pdf

Solution Compatibility Matrix

Table 4 Solution Compatibility Matrix

Software Release	ISE	Cisco Prime Infrastructure	Cisco MSE
7.0 (MD train)	1.2	2.0	7.6
7.4 (MD train)	1.2	2.0	7.6
7.6 (ED)	1.2	Update 1 for 1.4.0.45	7.6

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 7.6.110.0

Guidelines and Limitations

- When you are upgrading from a release that is prior to Release 7.6.X, Cisco lightweight access point (LAP) is unable to set up DTLS with Cisco WLC when LAP tries to join Cisco WLC using ap3g1-k9w8-tar.152-4.JB4.tar image. The workaround is as follows:
  1. Downgrade the Cisco WLC to 7.4.121.0.

     LAP would still not join the Cisco WLC as it is running the 7.6 image in it, which it once downloaded.
  2. Delete the 7.6 image from LAP CLI, so it boots from the rcvk image.

Booting from the rcvk image lets it form DTLS with out-of-order packet situation.

The rcvk image should not be 7.6 image. If it fails on rcvk image too, then probably we have 7.6 based rcvk image in it.

3. Download the 7.4 rcvk image in the AP, via archive download-sw /force /overwrite commands.

   LAP downloads the 7.4 code and boots using it. Using 7.4 code on both the ends, will get the DTLS session up, with out-of-order packets.

   Key point is to not use 7.6 image at either ends, LAP or WLC.

   Further Problem Description: LAP with MTU 1400 is unable to set up DTLS with Cisco WLC. The cert present by the AP, arrive on the Cisco WLC properly fragmented but out of order. According to Cisco WLC debug dtls, it fails with the following “debug dtls all enable” logs on Cisco WLC:

```
*spamApTask4: Apr 17 16:54:15.551: b0:c6:9a:c5:74:01 record=Handshake epoch=1
seq=0
*spamApTask4: Apr 17 16:54:15.551: b0:c6:9a:c5:74:01 msg=Unknown or Encrypted
*spamApTask4: Apr 17 16:54:15.551: openssl_shim_info_callback: SSL state = 0x2181;
where = 0x2002; ret = 0x0
*spamApTask4: Apr 17 16:54:15.551: openssl_shim_info_callback:
ret_type_string=unknown
*spamApTask4: Apr 17 16:54:15.551: openssl_shim_info_callback:
ret_desc_string=close notify
*spamApTask4: Apr 17 16:54:15.551: openssl_shim_info_callback:
SSL_state_string=SSLv3 read client certificate B
*spamApTask4: Apr 17 16:54:15.551: b0:c6:9a:c5:74:01 SSL_do_handshake:
SSL_ERROR_SYSCALL while communicating with 164.154.94.8 : (null)
```

- Cisco WLC Release 7.3.112.0, which is configured for new mobility, might revert to old mobility after upgrading to Release 7.6, even though Release 7.6 supports new mobility. This issue occurs when new mobility, which is compatible with the Cisco 5760 Wireless LAN Controller and the Cisco Catalyst 3850 Series Switch, are in use. However, old mobility is not affected.

  The workaround is as follows:

  a. Enter the following commands:

```
config boot backup
show boot

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

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

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

```
config boot primary
```

Note The epings are not available in 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, 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 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.
- 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 7.6.110.0, 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 7.6.110.0.
- When a client sends an HTTP request, the Cisco WLC intercepts it for redirection to the login page. If the HTTP request intercepted by the Cisco WLC is fragmented, the Cisco WLC drops the packet because the HTTP request does not contain enough information required for redirection.
- A client whose home page is an HTTPS (HTTP over SSL, port 443) one is not redirected by Web Auth to the web authentication dialog box. Therefore, it is not possible for such a client to get authenticated, and eventually, fails to connect to the network. The workaround is for the client to open an HTTP (port 80) web page.
- We recommend that you install Release 1.9.0.0 of Cisco Wireless LAN Controller Field Upgrade Software (FUS), which is a special AES package that contains several system-related component upgrades. These include the bootloader, field recovery image, and FPGA/MCU firmware. Installing the FUS image requires special attention because it installs some critical firmware. The FUS image is independent of the runtime image. For more information, see http://www.cisco.com/c/en/us/td/docs/wireless/controller/release/notes/fus_rn_OL-31390-01.html

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 Field Upgrade Software (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 ACLs 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 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 7.6.110.0 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 7.6.110.0. Table 5 shows the upgrade path that you must follow before downloading Release 7.6.110.0.

Table 5 Upgrade Path to Cisco WLC Software Release 7.6.110.0

Current Software Release	Upgrade Path to 7.6.110.0 Software
7.0.x releases	You can upgrade directly to 7.6.110.0. **Note** If you have VLAN support and VLAN mappings defined on H-REAP access points and are currently using a 7.0.x Cisco WLC software release that is prior to 7.0.240.0, we recommend that you upgrade to the 7.0.240.0 release and then upgrade to 7.6.110.0 to avoid losing those VLAN settings.
7.1.91.0	You can upgrade directly to 7.6.110.0.
7.2.x releases	You can upgrade directly to 7.6.110.0. **Note** If you have an 802.11u HotSpot configuration on the WLANs, we recommend that you first upgrade to the 7.3.101.0 Cisco WLC software release and then upgrade to the 7.6.110.0 Cisco WLC software release. You must downgrade from the 7.6.110.0 Cisco WLC software release to a 7.2.x Cisco WLC software release if you have an 802.11u HotSpot configuration on the WLANs that is not supported.
7.3.x releases	You can upgrade directly to 7.6.110.0.
7.4.x releases	You can upgrade directly to 7.6.110.0.
7.5.x releases	You can upgrade directly to 7.6.110.0.
7.6.100.0	You can upgrade directly to 7.6.110.0.

- 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.
- Cisco Prime Infrastructure 1.4.1 is needed to manage Cisco WLC software Release 7.6.110.0.
- 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.
- 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 7.6.110.0. 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 7.6.110.0 Cisco WLC software and your TFTP server does not support files of this size, the following error message appears:

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

  Bootloader menu for Cisco 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 control the address(es) are sent in the 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 APs, you must disable AP link latency (if enabled) before you use the disable option for the **config network ap-discovery nat-ip-only** command. To disable AP link latency, use the **config ap link-latency disable all** command.

- You can configure 802.1p tagging by using the **config qos dot1p-tag** {**bronze** | **silver** | **gold** | **platinum**} tag. For Release 7.2.103.0 and later releases, if you tag 802.1p packets, the tagging has impact only on wired packets. Wireless packets are impacted only by the maximum priority level set for QoS.
- You can reduce the network downtime using the following options:

  – You can predownload the AP image.

  – For FlexConnect access points, use the FlexConnect AP upgrade feature to reduce traffic between the Cisco WLC and the AP (main site and the branch). For more information about the FlexConnect AP upgrade feature, see the *Cisco Wireless LAN Controller FlexConnect Configuration Guide*.

Note Predownloading Release 7.6.110.0 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 7.6.110.0 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 7.6.110.0 (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 7.6.110.0 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 on 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 Disable the WLANs on the Cisco WLC.

Step 6 Choose **Commands** > **Download File** to open the Download File to Controller page.

Step 7 From the **File Type** drop-down list, choose **Code**.

Step 8 From the **Transfer Mode** drop-down list, choose **TFTP**, **FTP**, or **SFTP**.

Step 9 In the **IP Address** text box, enter the IP address of the TFTP, FTP, or SFTP server.

Step 10 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 11 In the **File Path** text box, enter the directory path of the software.

Step 12 In the **File Name** text box, enter the name of the software file (*filename*.aes).

Step 13 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 14 Click **Download** to download the software to the Cisco WLC.

A message appears indicating the status of the download.

Step 15 After the download is complete, click **Reboot**.

Step 16 If you are prompted to save your changes, click **Save and Reboot**.

Step 17 Click **OK** to confirm your decision to reboot the Cisco WLC.

Step 18 Re-enable the WLANs.

Step 19 For Cisco WiSM2 on the Catalyst switch, check the port channel and re-enable the port channel if necessary.

Step 20 If you have disabled the 802.11a/n and 802.11b/g/n networks in Step 4, re-enable them.

Step 21 To verify that the 7.6.110.0 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 Download the Cisco DTLS license.

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

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

b. On the Product License Registration page, choose **Get New > IPS, Crypto, Other Licenses**.

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

d. 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 21 detailed in the "Upgrading to Cisco WLC Software Release 7.6.110.0" section on page 8.

Interoperability With Other Clients in Release 7.6.110.0

This section describes the interoperability of Release 7.6.110.0 of the Cisco WLC software with other client devices.

Table 6 describes the configuration used for testing the clients.

Table 6 Test Bed Configuration for Interoperability

Hardware/Software Parameter	Hardware/Software Configuration Type
Release	7.6.110.0
Cisco WLC	Cisco 5500 Series Controller
Access points	1131, 1142, 1242, 1252, 3500e, 3500i, 3600, 3702
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 4.2, ACS 5.2
Types of tests	Connectivity, traffic, and roaming between two access points

Table 7 lists the client types on which the tests were conducted. The clients included laptops, handheld devices, phones, and printers.

Table 7 Client Types

Client Type and Name	Version
Laptop	
Intel 3945/4965	11.5.1.15 or 12.4.4.5, v13.4
Intel 5100/5300/6200/6300	v14.3.0.6
Intel 1000/1030/6205	v14.3.0.6
Intel 7260(11AC)	16.1.5.2
Broadcom 4360(11AC)	6.30.163.2005
Dell 1395/1397/Broadcom 4312HMG(L)	XP/Vista: 5.60.18.8 Win7: 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)	v5.100.235.12
Cisco CB21	v1.3.0.532
Atheros HB92/HB97	8.0.0.320
Atheros HB95	7.7.0.358
MacBook Pro (Broadcom)	5.10.91.26
MacBook Air	OSX 10.8.5, BCM43xx 1.0(6.30.223.154.45)
Handheld Devices	
Apple iPad	iOS 5.0.1
Apple iPad2	iOS 7.0.3(11B511)
Apple iPad3	iOS 7.0.3(11B511)
Asus Transformer	Android 4.0.3
Sony Tablet S	Android 3.2.1
Toshiba Thrive	Android 3.2.1
Samsung Galaxy Tab	Android 3.2
Motorola Xoom	Android 3.1
Intermec CK70	Windows Mobile 6.5 / 2.01.06.0355
Intermec CN50	Windows Mobile 6.1 / 2.01.06.0333
Symbol MC5590	Windows Mobile 6.5 / 3.00.0.0.051R
Symbol MC75	Windows Mobile 6.5 / 3.00.2.0.006R
Phones and Printers	
Cisco 7921G	1.4.2.LOADS
Cisco 7925G	1.4.2.LOADS
Ascom i75	1.8.0
Spectralink 8030	119.081/131.030/132.030
Vocera B1000A	4.1.0.2817

Table 7 Client Types (continued)

Client Type and Name	Version
Vocera B2000	4.0.0.345
Apple iPhone 4	iOS 7.0.3(11B511)
Apple iPhone 4S	iOS 7.0.3(11B511)
Apple iPhone 5	iOS 7.0.3(11B511)
Apple iPhone 5s	iOS 7.0.3(11B511)
Ascom i62	2.5.7
HTC One(11AC)	Android 4.2.2
Samsung Galaxy S4 - GT-I9500(11AC)	Android 4.3
HTC Sensation	Android 2.3.3
RIM Blackberry Pearl 9100	WLAN version 4.0
RIM Blackberry Bold 9700	WLAN version 2.7
Samsung Galaxy S II	Android 2.3.3
SpectraLink 8450	3.0.2.6098/5.0.0.8774
Samsung Galaxy Nexus	Android 4.0.2
Motorola Razr	Android 2.3.6

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

- Wired Guest Access
- Bandwidth Contract
- Service Port
- AppleTalk Bridging
- Right-to-Use licensing
- PMIPv6
- High Availability (1:1)
- Multicast-to-Unicast

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

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.

- L3 Roaming
- VideoStream
- 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 enable** command.

- Mesh
- 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
- 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.

- IPv6
- High Availability
- PMIPv6
- WGB
- VideoStream
- Outdoor mesh access points

Note Outdoor APs in the FlexConnect mode are supported.

- Indoor mesh access points
- Application Visibility and Control (AVC)
- Client downstream rate limiting for central switching

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

The following sections lists Open Caveats and Resolved Caveats for Cisco WLCs and lightweight access points for Release 7.6.110.0. To enable you to locate caveats in the Cisco Bug Toolkit, the caveat titles listed in this section are drawn directly from the Bug Toolkit database. These caveat titles are not intended to be read as complete sentences because the title field length is limited. In the caveat titles, some truncation of wording or punctuation might be necessary to provide the most complete and concise description. The only modifications made to these titles are as follows:

- Commands are in **boldface** type.
- Product names and acronyms might be standardized.
- Spelling errors and typos might be corrected.

If you need information about a specific caveat that does not appear in these release notes, you can use the Cisco Bug Toolkit to find caveats of any severity. Click this URL to browse to the Bug Toolkit:

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

Note If you request a defect that cannot be displayed, the defect number might not exist, the defect might not yet have a customer-visible description, or the defect might be marked Cisco Confidential.

Open Caveats

Table 8 lists the open caveats in the 7.6.110.0 Cisco WLC software release.

Table 8 Open Caveats

ID	Description

CSCuo35247	**Symptom**: Cisco lightweight access point (LAP) is unable to set up DTLS with Cisco WLC.
	Conditions: LAP trying to join Cisco WLC using ap3g1-k9w8-tar.152-4.JB4.tar image.
	Workaround:
	1. Downgrade the Cisco WLC to 7.4.121.0.
	LAP would still not join the Cisco WLC as it is running the 7.6 image in it, which it once downloaded.
	2. Delete the 7.6 image from LAP CLI, so it boots from the rcvk image.
	Booting from the rcvk image lets it form DTLS with out-of-order packet situation.
	The rcvk image should not be 7.6 image. If it fails on rcvk image too, then probably we have 7.6 based rcvk image in it.
	3. Download the 7.4 rcvk image in the AP, via archive download-sw /force /overwrite commands.
	LAP downloads the 7.4 code and boots using it. Using 7.4 code on both the ends, will get the DTLS session up, with out-of-order packets.
	Key point is to not use 7.6 image at either ends, LAP or WLC.
	Further Problem Description: LAP with MTU 1400 is unable to set up DTLS with Cisco WLC. The cert present by the AP, arrive on the Cisco WLC properly fragmented but out of order. According to Cisco WLC debug dtls, it fails with the following "debug dtls all enable" logs on Cisco WLC:
	`*spamApTask4: Apr 17 16:54:15.551: b0:c6:9a:c5:74:01 record=Handshake epoch=1 seq=0`
	`*spamApTask4: Apr 17 16:54:15.551: b0:c6:9a:c5:74:01 msg=Unknown or Encrypted`
	`*spamApTask4: Apr 17 16:54:15.551: openssl_shim_info_callback: SSL state = 0x2181; where = 0x2002; ret = 0x0`
	`*spamApTask4: Apr 17 16:54:15.551: openssl_shim_info_callback: ret_type_string=unknown`
	`*spamApTask4: Apr 17 16:54:15.551: openssl_shim_info_callback: ret_desc_string=close notify`
	`*spamApTask4: Apr 17 16:54:15.551: openssl_shim_info_callback: SSL_state_string=SSLv3 read client certificate B`
	`*spamApTask4: Apr 17 16:54:15.551: b0:c6:9a:c5:74:01 SSL_do_handshake: SSL_ERROR_SYSCALL while communicating with 164.154.94.8 : (null)`

CSCud68413	**Symptom**: A Cisco WLC functioning as a DHCP server with large DHCP scopes might stop servicing DHCP client requests. **Conditions**: Cisco WLC Release 7.2.110.0. **Workaround**: Reboot the Cisco WLC.
CSCue99119	**Symptom**: AP drops randomly and does not associate back. **Conditions**: Cisco WLCs running a large number of APs and clients. Debug indicates that CAPWAP queue is full during this time. **Workaround**: Reboot the Cisco WLC.

Table 8 Open Caveats (continued)

ID	Description
CSCug34700	**Symptom**: Cisco WLC sends active keep-alive as a wired packet instead of wireless. **Conditions**: When the Cisco WLC sends the keep-alive as a wired packet, the ISE drop it because of license issues. **Workaround**: Use passive keep-alive instead of active.
CSCuc78713	**Symptom**: Wireless clients cannot receive broadcast packets after broadcast key rotation. **Conditions**: Dynamic WEP; Release 7.0.235.0, 7.2.110.0, and 7.3.101.0. **Workaround**: Enter the **config advanced eap bcast-key-interval 86400** command in the middle of the night and then change security setting to WPA2.

CSCtx68870	**Symptom**: Cisco 5508 WLC stops responding every 3 hours with the following message:
	`************************************************************    *`
	`Start Cisco Crash Handler                *`
	`************************************************************ Sys Name:`
	`BHN_WLC1    Model:                 AIR-CT5508-K9    Version:`
	`7.0.116.0   Timestamp:      Fri Jan 27 19:24:37 2012   SystemUpTime:`
	`0 days 3 hrs 3 mins 41 secs    signal:                   11    pid:`
	`1053   TID:      952488784   Task Name:      spamApTask2   Reason:`
	`System Crash    si_signo:              11    si_errno:              0`
	`si_code:             1    si_addr:              0x0    timer tcb:`
	`0xa95    timer cb:              0x1009b228 ('apfCreateLbsEntry 1056')`
	`timer arg1:          0x3eef15f0    timer arg2:          0x3eef15f0`
	`Long time taken timer call back inforamtion:    Time Stamp:      Fri Jan`
	`27 19:24:37 2012    timer cb  :           0x1009b228 ('apfCreateLbsEntry`
	`1056')    Duration  : 539152 usecs  cbCount= 1`
	`------------------------------------------------------------    Analysis`
	`of Failure:               Software Failed on instruction at :    pc =`
	`0x1012f28c (apfMeshCACremoveMAP 584)  ra = 0x1012f270`
	`(apfMeshCACremoveMAP 584)                Software Failed while accessing`
	`the data located at :0x0`
	`------------------------------------------------------------    System`
	`Stack         Frame 0: 0x10012c38: create_crash_dump 7128    Frame 1:`
	`0x10011a4ccreate_crash_dump 2540    Frame 2: 0x100080c8: sigsegv_handler`
	`6120    Frame 3: 0x38c5c330: SHA1Final 661876928    Frame 4: 0x1012f28c:`
	`apfMeshCACremoveMAP 612    Frame 5: 0x10272030: spamDeleteLCBTemp 3696`
	`Frame 6: 0x102734b4: spamAllocateLCB 3092    Frame 7: 0x10a07318:`
	`acAddWtpToDatabase 120    Frame 8: 0x102ebc8c: acCapwapSmInit 25828`
	`Frame 9: 0x102e3e18: acPostDecodeConfigRequest 5448    Frame 10:`
	`0x102efad4: capwapAcStatemachine 532    Frame 11: 0x10a04d38:`
	`spamApReceiveTask 432    Frame 12: 0x10779f28: osapiTaskAppKeySelfSet 304`
	`Frame 13: 0x11685500: SHA1Final 1442448    Frame 14: 0x116eae6c: SHA1Final`
	`1858556`
	`------------------------------------------------------------    Semaphore`
	`and Mutex Usage    (Caller IP(instruction pointer of caller) Gives one`
	`more level    of depth in stack to track the Semaphore and Mutex`
	`operation)`
	Conditions: Cisco WLC comes back online after cycling.
	Workaround: None.

Table 8 Open Caveats (continued)

ID	Description
CSCuh20715	**Symptom**: Cisco 5500 Series WLC stopped responding on the Reaper Reset: Task "LDAP DB Task 2" missed software watchdog. **Conditions**: Reaper Reset: Task "LDAP DB Task 2" missed software watchdog. **Workaround**: None.
CSCuh39893	**Symptom**: Cisco WLC using Releases 7.3 and 7.4 fail authenticate One Time Password (OTP) users when attempting to authenticate to the Cisco WLC using TACACS+. The following debug output is displayed when the **debug aaa tacacs enable** command is entered on the WLC CLI: `TPLUS_AUTHEN_STATUS_GETPASS auth_cont get_pass reply: pkt_length=25 processTplusAuthResponse: Continue auth transaction No auth response from: <SERVER IP> retrying with next server Preparing message for retransmit. Decrypting first Forwarding request to <SERVER IP> port=4900 AUTH Socket closed underneath No auth response from: <SERVER IP> retrying with next server Preparing message for retransmit. Decrypting first Forwarding request to <SERVER IP> port=4900 AUTH Socket closed underneath Exhausted all available servers for Auth/Author packet` **Conditions**: Cisco WLC using Releases 7.3 and 7.4; TACACS+ used for Management User Authentication; OTP used for TACACS+ static passwords are not affected. **Workaround**: Extend the TACACS+ Management Server Timeout value by entering these commands: **config tacacs auth disable** *server-index* **config tacacs auth mgmt-server-timeout** *server-index* **config tacacs auth enable** *server-index*
CSCuh52238	**Symptom**: False DFS detections related to client activity. **Conditions**: Clients triggering DFS detections due to spurious emissions. **Workaround**: Use non-DFS channels. This issue is to track additional filtering for pulses generated by client activity.
CSCuh55653	**Symptom**: Cisco 5500 Series WLC experienced unexpected reboot using Release 7.4.100.0 software with the ""apfMsConnTask_5"" task suspended. **Conditions**: This issue occurs under normal condition without any hardware or software configuration changes or network topology changes. **Workaround**: None. **Issue Analysis**: The software failed on instruction at: pc = 0x1050c868 (mmAnchorExportSend 1116) ra = 0x10561d5c (mmAnchorExportSend 1116). Software failed while accessing the data located at:0xf3. This issue is observed only once in the network and the Cisco WLC is under monitoring.

Table 8 Open Caveats (continued)

ID	Description
CSCuc91441	**Symptom**: When more clients time out at the same time, for example more than 64, due to limitation of chunk memory allocation, some clients were not removed from Cisco WLC's database after user idle timer expired. **Conditions**: When 100 clients expire their user idle timeout simultaneously, only 64 or 65 deauthentications are sent and 36 or 37 clients were not removed from Cisco WLC's database. **Workaround**: Options: • Manually remove the stale clients • Reboot the AP that had these clients • Reboot Cisco WLC • Disable and enable WLAN. Resolution improved the client user idle timeout handling so that 128 clients are taken care of simultaneously.
CSCuh69558	**Symptom**: Default interface takes precedence over foreign VLAN mapping with AAA override. When both AAA override and foreign map are enabled in a guest anchor scenario. If AAA sends override VLAN, the system works as expected and this AAA VLAN takes precedence. If AAA is enabled but does not sent any override VLAN, the WLAN's VLAN takes precedence and not the foreign map. Effectively, foreign map feature stops working. **Conditions**: Configure a guest anchor solution; enable foreign Cisco WLC-interface mapping in the anchor; enable AAA override in the WLAN. If the AAA server does not send any interface details, the anchor Cisco WLC uses the default interface configuration for the WLAN to assign IP address to the client. The precedence should fall to the foreign Cisco WLC-interface mapping and then to the default interface in the WLAN. **Workaround**: None.
CSCuh86993	**Symptom**: Cisco AP, on receiving authentication request from a client whose database is about to be freed/deleted, should not respond with authentication response for a disabled BSSID. **Conditions**: Unknown. **Workaround**: None.

Table 8 Open Caveats (continued)

ID	Description
CSCuh92835	**Symptom**: The following error message is displayed: `WLAN with duplicate SSID and L2 security policy found.` **Conditions**: Cannot make change on any of the two similar WLANs using same L2/L3 security, that is, QoS bandselect, because it results in an error. **Workaround**: 1. Change the WLAN configuration using the CLI. 2. Disable both WLANs using the GUI, make all WLAN configuration changes and then enable WLANs. 3. Delete and recreate the other WLAN using the GUI. **Further Problem Description**: Fix the popup error. The error message should not pop up when making changes on WLAN configuration because two WLANs with similar SSID name and L2 security with WLAN ID2 and WLAN ID 20 are intentionally allowed.
CSCuh94366	**Symptom**: Clients are unable to connect and get DHCP. **Conditions**: After upgrading a Cisco Flex 7510 WLC to Release 7.4.100.60, clients on Cisco 1242 APs are unable to connect to a FlexConnect Local Switching WLAN that is mapped to some VLANs (301 is noted) in the AP's FlexConnect configuration. **Workaround**: Use other VLANs.
CSCui26077	**Symptom**: FT roam fails between FlexConnect APs. **Conditions**: FT client and FlexConnect APs advertising 802.11r FT PSK WLAN. **Workaround**: Use FT-802.1x or use 11i fast roam methods like OKC because normal roam occurs because FT roam fails.
CSCui37300	**Symptom**: Cisco WLC uses 0.0.0.0 as source IP for mDNS query or response when Cisco WLC has untagged interface. **Conditions**: WLAN attached with untagged interface; mDNS client associated with this WLAN client request for service using mDNS; when Cisco WLC responds, it uses 0.0.0.0 as source IP address so the service provider might or might not be seen on the client device. **Workaround**: Use VLAN interfaces on mDNS WLAN.
CSCui48379	**Symptom**: Dynamic environment - bsnMobileStationTable does not reflect correct number of clients. **Conditions**: Dynamic environment. **Workaround**: Use the **show client summary** command.
CSCui57980	**Symptom**: Cisco WLC unresponsive. **Conditions**: Not applicable at this time; however, this is a large campus deployment and it is possible that it might be related to a large influx of clients (2000-3000) connecting to the Cisco WLC. **Workaround**: None.

Table 8 Open Caveats (continued)

ID	Description
CSCui86670	**Symptom**: When supplying the DNS server IP address and domain name to an AP with static IP address configuration, the DNS server's IP address is written to run configuration immediately, but domain name is not. **Conditions**: Static IP configuration. **Workaround**: Reboot the AP.
CSCui90481	**Symptom**: SnmpOperationException table too large; possible agent loop CdpApNeighbors refresh configuration fails due to CDP-SNMP looping. **Conditions**: All Cisco WLCs. **Workaround**: Disable AP neighbor CDP on Cisco WLC.
CSCui94634	**Symptom**: Cisco APs in FlexConnect local switching mode with VLAN mappings dissociate from Cisco WLC when an ACL is applied to one of the VLANs. Once ACL is pushed, CAPWAP UDP processing become sluggish and retransmissions of packets from Cisco WLC result in errors with duplicate sequence number errors. Eventually, this state causes a DTLS timeout and reassociation process on the AP, which fails over and over with same issue. It appears that the issue is related to corruption of the CAPWAP private configuration because the actual content of the ACL does not matter. The issue occurs immediately at the point the ACL is pushed. **Conditions**: FlexConnect mode APs with VLAN mappings and FlexConnect ACL. **Workaround**: Do not apply ACL to the AP; use another enforcement point if required. Perform a reimage of the AP with 15.2 recovery image.
CSCui94702	**Symptom**: When using the Cisco 602I OEAP for the personal SSID and using DHCP, the OEAP acts as the DNS server for the DHCP subnet (there is no option to hard code other DNS servers or pass down the ISP DNS servers). Within 24 hours, the OEAP suddenly stops responding to DNS requests, making Internet access through name impossible for DHCP clients. The only workaround found so far was to disable DHCP on the OEAP (this immediately resolves the issue and the OEAP starts responding to DNS once again), and reenable DHCP. This works for about a day, but then stops working. **Conditions**: Every 24 hours. **Workaround**: Setting the Cisco 600 Series OEAP IP address to a static IP address or rebooting the AP.
CSCui95938	**Symptom**: Apple devices such as iPad, iPhone, and iPod are unable to switch transparently from a 802.1X WLAN to a WPA-WPA2(PSK) WLAN. **Conditions**: Cisco AP1142 is used with Cisco WLC using Release 7.5.102.0; FlexConnect local switching is used; two SSIDs are created—one with 802.1X authentication and the other with WPA-PSK. Switching from the 802.1X WLAN to the PSK one does not happen smoothly **Workaround**: Use another AP (tested with AP1262 and AP3501); or use a Cisco WLC release other than 7.5.102.0.
CSCuj05274	**Symptom**: Cisco WLC unresponsive. **Conditions**: Release 7.4.110.0. **Workaround**: None.

Table 8 Open Caveats (continued)

ID	Description
CSCuj15593	**Symptom**: Backed up Cisco WLC configuration with RF profile commands cannot be uploaded to another Cisco WLC. **Conditions**: Cisco WLC configuration with RF profile commands. **Workaround**: Open the configuration file in a text editor and find the commands related to RF profile This issue occurs when the commands for RF profile data rates, transmit power, and so on, occur before the command that actually creates the RF profile. For example, you may see something like this: **config rf-profile data-rates 802.11a mandatory 6 test** **config rf-profile data-rates 802.11a supported 9 test** **config rf-profile create 802.11a test**. Move the **create** command before any of the other commands related to the RF profile. Therefore, the above should be changed to the following: **config rf-profile create 802.11a test** **config rf-profile data-rates 802.11a mandatory 6 test** **config rf-profile data-rates 802.11a supported 9 test** Download the new configuration to the Cisco WLC. **Further Problem Description**: Cisco WLC Release 7.4.110.0. Create a configuration backup with RF profile configuration and then upload it to another Cisco WLC. The operation fails with the following message displayed: `*TransferTask: Sep 05 18:05:52.951: RESULT_STRING: Error: There cannot be multiple maps for the field 58.1.5.0 Config CLI:config rf-profile data-rates 802.11a disabled 6 test123”`
CSCuj17683	**Symptom**: 802.11r Roaming—AP might sometimes send deauthentication with reason code 7. **Conditions**: AP roam in a bad RF environment. Clients fail to hear ACK for reassociation request from AP and continues to send reassociation request and following a data packet. **Workaround**: After the deauthentication, complete roam occurs and the clients can join again. **Further Problem Description**: This issue is seen very rarely and only with Samsung I565 phones.
CSCuj35236	**Symptom**: Changing a parameter on an SSID causes issue in FlexConnect APs if another SSID exists with a different profile. **Conditions**: FlexConnect multiple WLANs with the same SSID. **Workaround**: None.

Table 8 Open Caveats (continued)

ID	Description
CSCuj45983	**Symptom**: When the Cisco WLC gets a CoA (Change of Authorization) RADIUS message, for example from ISE, the Cisco WLC sends a deauthentication to the client and move the client to DHCP_REQ state. Unless "DHCP Required" is disabled on the WLAN, this means that the client will then be disconnected unless it performs a new DHCP request. With "debug client" in effect on the Cisco WLC, the following message will be seen: `DHCP_REQD (7) DHCP Policy timeout. Number of DHCP request 0 from client` **Conditions**: Cisco WLC is using CoA from RADIUS and has DHCP Required on the WLAN. Client is one that does not reliably re-DHCP upon 802.11 deauthentication; some Windows 7 and Mac OS X systems have been seen to have this problem. **Workaround**: For a single VLAN system (same VLAN before and after CoA), disable DHCP Required. For some client types, you might be able to reconfigure them to make sure that they re-DHCP as needed. For example, on a Windows 7 system, perform the following: **1.** In the HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces registry path, create a DWORD value named as ?UseNetworkHint? and set it to ?0?. **2.** Restart the DHCP client service by executing the following commands from elevated command prompt: **net stop dhcp** **net start dhcp** An alternative might be to use two VLANs, one a pre-CoA and the other a post-CoA. The DHCP leases for the pre-CoA scope might be set with very short lease durations such as 30 seconds. This should trigger a more timely DHCP lease renewal from the client so that it can regain access to the network after the CoA event.
CSCuj58556	**Symptom**: Cisco AP disconnects from the primary WLC and moves to the secondary WLC due to memory allocation. **Conditions**: Unknown. **Workaround**: Reboot AP.
CSCuj58625	**Symptom**: Cisco WLC unresponsive with local EAP-FAST in use. **Conditions**: Cisco WLC is performing local EAP-FAST. **Workaround**: Use an external RADIUS server.
CSCuj61455	**Symptom**: Clients get disconnected from FlexConnect AP. 802.11 deauthentication with Reason Code 1 (Unspecified) WLC "debug client" output shows "Sent Deauthenticate to mobile on BSSID 00:3a:98:8a:70:a0 slot 0 (caller 1x_bcastkey.c:951)". **Conditions**: Cisco Flex 7510 WLC using Release 7.4.110.0; Cisco AP 1602 in FlexConnect mode; WLAN = WPA2 AES PSK, Central Authentication, Local Switching. **Workaround**: None.

Table 8 Open Caveats (continued)

ID	Description

CSCuj70166	**Symptom**: AP dissociates from Cisco WLC when %DOT11-2-NO_CHAN_AVAIL_CTR occurs.
	`Log details:`
	`DOT11-2-NO_CHAN_AVAIL_CTRL: Interface Dot11Radio1  no channel available.`
	`DTLS_CLIENT_EVENT: local_in_addr_comp: Client and server addresses of 2`
	`nodes are AC190D09  BDAF  AC190C01  147E : AC190D09  BDAF  AC190C01  147E`
	`DTLS_CLIENT_EVENT: dtls_disconnect: Disconnecting DTLS connection`
	`0x4369A0C  DTLS_CLIENT_EVENT: dtls_connectionDB_del_connection: Connection`
	`deleted AC190D09  BDAF  AC190C01  147E -----`
	Conditions: %DOT11-2-NO_CHAN_AVAIL_CTR occurs after DFS detects.
	Workaround: None.

CSCuj74920	**Symptom**: A client roam between two Cisco WLCs can fail intermittently making the client to be part of the VLAN originally mapped to the WLAN; for example two Cisco WLC serving clients, WLAN mapped to VLAN x, RADIUS assigned to VLAN y; intermittently, client can be put on VLAN x during roams between WLC1 to WLC2.
	Conditions: When a client roams between two Cisco WLCs.
	Workaround: None.
	Further Problem Description: Debug example:
	`pemReceiveTask: Oct 09 15:58:40.382: 60:fe:c5:69:ef:50 Set symmetric`
	`mobility tunnel for 60:fe:c5:69:ef:50 as in Foreign role *pemReceiveTask:`
	`Oct 09 15:58:40.382: 60:fe:c5:69:ef:50 167.73.161.198 Added NPU entry of`
	`type 1  dtlFlags 0x1 *pemReceiveTask: Oct 09 15:58:40.382:`
	`60:fe:c5:69:ef:50 Skip Foreign / Export Foreign Client IP 167.73.161.198`
	`plumbing in FP SCB *bcastReceiveTask: Oct 09 15:58:40.389: Sending MLD`
	`query First Time to  0C:85:25:C6:71:90  ap for mgid 15`
	`*bcastReceiveTask: Oct 09 15:58:40.389: Entry for ap  0C:85:25:C6:71:90`
	`MLD query packet not queued for mgid 15... Enquing the Query packet...`
	`*DHCP Socket Task: Oct 09 15:58:41.520: 60:fe:c5:69:ef:50 DHCP received op`
	`BOOTREQUEST (1) (len 308 vlan 0  port 13  encap 0xec03) *DHCP Socket Task:`
	`Oct 09 15:58:41.520: 60:fe:c5:69:ef:50 DHCP processing DHCP DISCOVER (1)`
	`*DHCP Socket Task: Oct 09 15:58:41.520: 60:fe:c5:69:ef:50 DHCP   op:`
	`BOOTREQUEST  htype: Ethernet  hlen: 6  hops: 0 *DHCP Socket Task: Oct 09`
	`15:58:41.520: 60:fe:c5:69:ef:50 DHCP   xid: 0x75555ccb (1968528587)  secs:`
	`43  flags: 0 *DHCP Socket Task: Oct 09 15:58:41.520: 60:fe:c5:69:ef:50`
	`DHCP   chaddr: 60:fe:c5:69:ef:50 *DHCP Socket Task: Oct 09 15:58:41.520:`
	`60:fe:c5:69:ef:50 DHCP   ciaddr: 0.0.0.0   yiaddr: 0.0.0.0 *DHCP Socket`
	`Task: Oct 09 15:58:41.520: 60:fe:c5:69:ef:50 DHCP   siaddr: 0.0.0.0`
	`giaddr: 0.0.0.0 *DHCP Socket Task: Oct 09 15:58:41.520: 60:fe:c5:69:ef:50`
	`DHCP successfully bridged packet to EoIP tunnel`

CSCuj84256	**Symptom**: When using a WLAN on the Cisco WLC that has WMM marked to disable some clients that try to connect to this WLAN through a Cisco 602 OfficeExtend Access Point (OEAP) cannot get an IP address. **Conditions**: WPA2 with 802.1X security; Cisco WLC Release 7.3 and 7.4. **Workaround**: Two options: • Set WMM field to “Allowed” or “Required” • Use PSK security on the SSID. **Further Problem Description**: Cisco 602 OEAP does not process DHCP correctly with WMM disabled on an 802.1X enabled WLAN.

Table 8 Open Caveats (continued)

ID	Description
CSCuj85183	**Symptom**: The status of the fans becomes OK even if it is not present. **Conditions**: Multiple PS is used for Cisco WLC. Remove the fan tray first and then turn off one of two PS. **Workaround**: None.
CSCuj89799	**Symptom**: Cannot apply more than 7 RF profiles to AP group. **Conditions**: Cisco WiSM2 using Release 7.4.100.60. **Workaround**: None.
CSCuj91950	**Symptom**: For some VHT MCS rate configurations, the driver might be programmed with rates that are different from those specified in the CLI and GUI. It might appear that the 802.11ac client is associating at MCS rates that are greater than those configured for the 802.11ac interface. **Conditions**: The issue might be encountered if the VHT MCS rates are configured to some values that are other than the default value. **Workaround**: Avoid invalid MCS rate configurations. **Further Problem Description**: The problem exists because the HT rate configuration interface was extended to allow VHT rate configuration leading to ambiguous configurations in some cases. The fix is to create a separate VHT MCS configuration interface as described in the bug description.
CSCuj93777	**Symptom**: In very rare situations, there is a racing condition that data packets are sent before switchport receiving BPDU packets from the wireless side cause MAC address flapping. **Conditions**: STP to break network loop mesh AP reboot or moving between RAPs intensive packets flooding in network to cause packets are sent before BPDUs are propagated. **Workaround**: None.

CSCuj96172	**Symptom**: bsnDot11StationAssociate varbinds order is different than what is defined in AIRESPACE-WIRELESS-MIB.
	Conditions: Trap are received with varbinds in the following order:
	`{ V2Trap(205) R=92318642    .1.3.6.1.2.1.1.3.0=211747500 <-- sysUpTime`
	`.1.3.6.1.6.3.1.1.4.1.0=.1.3.6.1.4.1.14179.2.6.3.53 <--snmpTrapOID`
	`.1.3.6.1.4.1.14179.2.6.2.35.0=24_b6_57_b4_60_30 <-- bsnStationAPMacAddr`
	`.1.3.6.1.4.1.14179.2.6.2.36.0=1 <--bsnStationAPIfSlotId`
	`.1.3.6.1.4.1.14179.2.6.2.34.0=90_72_40_9f_e8_eb <-- bsnStationMacAddress`
	`.1.3.6.1.4.1.14179.2.6.2.43.0=10.227.145.12 <--bsnUserIpAddress`
	`.1.3.6.1.4.1.14179.2.2.1.1.3.0=””AP1140-6cb147”” <--bsnAPName`
	`.1.3.6.1.4.1.14179.2.6.2.39.0=””xxk840”” <--bsnStationUserName    } }`
	`This is what defined in the MIB: bsnDot11StationAssociate`
	`NOTIFICATION-TYPE     OBJECTS         {`
	`bsnStationAPMacAddr                 bsnStationAPIfSlotId`
	`bsnUserIpAddress                   bsnStationMacAddress`
	`bsnStationUserName                           bsnAPName`
	`}  Seems that bsnUserIpAddress  bsnStationMacAddress are in different`
	`order  and bsnStationUserName and bsnAPName are in different order`
	Workaround: None.

Table 8 Open Caveats (continued)

ID	Description
CSCuj97293	**Symptom**: Cisco WLC stops responding when the **show local-auth certificates** commands is entered. **Conditions**: Unknown. **Workaround**: None.
CSCuj97899	**Symptom**: The time difference on the Cisco Prime Infrastructure alarms can go higher than the actual wIPS security alert. But the alarm will be off by a value less than 24 hours. **Conditions**: Cisco WLC is not configured on UTC time. **Workaround**: Time zone needs to be in UTC for the Cisco WLC when used with MSE wIPS. We recommend MSE to be in the same time zone as Cisco WLC, and the MSE needs to be in UTC time. Cisco Prime Infrastructure need not be in UTC time. You can choose Cisco Prime Infrastructure to be in the time zone of your choice. Cisco Prime Infrastructure will change the UTC time from MSE to the time zone that is configured on Cisco Prime Infrastructure.
CSCul03672	**Symptom**: Cisco 5500 Series WLC lost some setting after restoring the configuration file. **Conditions**: AIR-CT5508-K9 using Release 7.5.102.0. **Workaround**: None.
CSCul04029	**Symptom**: Cisco WLC unresponsive on task name ‘emWeb’. **Conditions**: Cisco 5508 WLC using Release 7.3.112.0 with a mobility setup. **Workaround**: None.
CSCul04090	**Symptom**: Cisco WLC unexpectedly reboots with Reaper Reset. System Stack indicates tsmClientStatsDataLock. **Conditions**: Unknown. **Workaround**: None.
CSCul10779	**Symptom**: Cisco WLC stopped responding. **Conditions**: Cisco 5508 WLC using Release 7.5.102.0. **Workaround**: None.
CSCul11549	**Symptom**: Services leak from one mDNS profile to another. **Conditions**: This issue can be reproduced by using dynamic VLAN assignment. **Workaround**: None.

Table 8 Open Caveats (continued)

ID	Description
CSCul15555	**Symptom**: A CCKM client associated with a FlexConnect AP using Cisco WLC Release 7.4.110.0 (local switching/central authentication) might lose IP connectivity soon after a successful CCKM roaming while remaining associated with the AP. On Cisco WLAN phone, the symptom is often seen as a two-way voice outage, phone stuck in “requesting DHCP” state. On the AP side, a radio level debugging shows decryption errors. **Conditions**: Cisco WLC/AP using Release 7.4.110.0; FlexConnect local switching and central authentication; frequent CCKM roaming events including interband roaming. **Workaround**: The issue recovers soon after the client roams to another AP. **Further Problem Description**: This is not a persistent issue; normally, the client can then roam back to the AP without any issues.

CSCtj06944	**Symptom**: A Cisco 5508 WLC or Cisco WiSM2 might stop responding with messages similar to the following displayed on the console log:
	`Kernel panic - not syncing: Failed to allocate skb for hardware pool 0`
	`LKCD: Dumping from interrupt handler! 262144 pages of RAM 0 pages of`
	`HIGHMEM 10968 reserved pages 5010 pages shared 0 pages swap cached`
	`swapper: page allocation failure. order:0  mode:0x20 Call Trace:`
	`[<ffffffff81126b28>] dump_stack 0x8/0x48 [<ffffffff81196de4>]`
	`__alloc_pages 0x32c/0x3c0 [<ffffffff811b56a8>] cache_alloc_refill`
	`0x398/0x6e8 [<ffffffff811b5b50>] __kmalloc 0x158/0x168`
	`[<c0000000003f758c>] ssh_kernel_alloc 0x5c/0x1b0 [sshquicksec]`
	`[<c0000000003faaec>] ssh_interceptor_packet_alloc_header 0x64c/0x708`
	`[sshquicksec] [<c0000000004947e0>] ssh_interceptor_packet_in 0xe8/0x750`
	`[sshquicksec]`
	Conditions: The service port on the Cisco WLC is plugged into a VLAN, which is also present on one of the Cisco WLC’s uplink interfaces.
	Workaround: Unplug the service port or connect it to a VLAN, which is not switched to one of the Cisco WLC’s uplink interfaces.
	Further Problem Description: The service port, if connected to the switched network, must be put into a VLAN, which is not connected to the WLC’s distribution ports. It is not a valid configuration to have the service port in a VLAN, which is in use by the WLC’s management AP Manager or dynamic interfaces.

CSCuh25790	**Symptom**: HA enabled Cisco 5508 WLC setup with 430 real Cisco APs. A predownload on the 430 APs was started. The predownload completed, but cannot reset the system after the predownload. It complains that the AP software upgrade is in progress and the system becomes unresponsive.
	The following command was entered and the output is as shown below:
	`(Cisco Controller) >reset system`
	
	`AP software being upgraded  please try again later.`
	Conditions: High AP count failed predownlaod.
	Workaround: Initiate a Cisco WLC reboot with the **reset system forced** command.

Table 8 Open Caveats (continued)

ID	Description
CSCuj04921	**Symptom**: At close range, clients such as S4 Linksys and Macbook Air are not able to reach the m8/m9 data rates and this affects the throughput. The A-MPDU details with BCMDBG enabled for S4 and Linksys 3x3 are collected. **Conditions**: Unknown. **Workaround**: None.
CSCug80814	**Symptom**: The foreign Cisco WLC does not respond to ARP from foreign export client to a local client being on the same VLAN. **Conditions**: • Client1 associates with WLC1 (local) • Client1 does L3 roam to WLC2 (WLC2: foreign / WLC1: anchor) • Client2 associates with WLC2 (local) • Initiate traffic, that is ping from Client1 to Client2 **Workaround**: None.
CSCui27642	**Symptom**: Public safety status mismatch in active and standby Cisco WLCs. **Conditions**: HA setup with public safety configuration. **Workaround**: None.
CSCsz82878	**Symptom**: Cisco WLCs using Release 4.2.130.181M (mesh) stop responding with Task Name: reaperWatcher. **Conditions**: Multiple Cisco WiSMs using Release 4.2.130.181M with numerous Cisco AP1510s associated. **Workaround**: If such a behavior and subsequent issue occurs in any deployment, use the following command to disable the dynamic CAC tree updates: **config mesh cac disable'** To return the CAC tree to normal behavior, use the following command: **config mesh cac enable** **Further Problem Description**: At present, the issue appears to be due to a problem with the dynamic building of the mesh CAC tree. The issue is present even when CAC is not enabled for voice or video.

Table 8 Open Caveats (continued)

ID	Description

CSCuc68995	**Symptom**: A wireless web authentication client might be unable to authenticate to the network. When the client opens a browser window, a blank page is displayed.
	With the **debug web-auth redirect** command in effect, messages similar to the following might be displayed:
	`*webauthRedirect: Oct 15 18:43:19.470: #EMWEB-6-REQUEST_IS_NOT_GET_ERROR:`
	`webauth_redirect.c:1055 Invalid request not GET on client socket 72`
	or
	`*webauthRedirect: Oct 10 16:36:30.715: %EMWEB-3-PARSE_ERROR: parse error after`
	`reading. bytes parsed = 0 and bytes read = 189`
	Conditions: The HTTP GET from the client arrives at the Cisco WLC in multiple TCP segments.
	Workaround: Reconfigure the TCP/IP stack of your network and the client to ensure that the HTTP GET arrives in a single segment. One example of client software that is known to introduce TCP segmentation behavior that triggers this issue is AnyConnect Web Security 3.0.3054.
	This issue is a regression that was introduced in Release 7.2.

CSCud57046	**Symptom**: Client entry is seen on multiple Cisco WLCs even when it is not anchored to a Cisco WLC or part of its mobility group. **Conditions**: Unknown. **Workaround**: None.
CSCud69426	**Symptom**: AAA overridden ACL is not applied. **Conditions**: After a session timeout, the Cisco WLC clears the AAA Override cache and puts the wireless client in default VLAN. **Workaround**: None.

Table 8 Open Caveats (continued)

ID	Description

CSCuf77488	**Symptom**: The FT and LT detection time for an alarm is ahead or later than the AP clock. This causes a delay in Cisco NCS to detect the alarm.
	`LCAVIAX014-2AD1#show capwap am alarm 54`
	`capwap_am_show_alarm = 54`
	
	`<A id='139266813'>`
	`<AT>54</AT>`
	`<FT>2013/03/12 23:37:44</FT>`
	`<LT>2013/03/12 23:38:07</LT>`
	`<DT>2013/03/01 21:59:47</DT>`
	`<SM>D0:57:4C:08:FB:B2-g</SM> <SNT>1</SNT>`
	` <CH>1</CH>`
	` <FID>0</FID>`
	` pAlarm.bPendingUpload = 0`
	`LCAVIAX014-2AD1#`
	`LCAVIAX014-2AD1#show clock`
	`*21:59:18.983 UTC Tue Mar 12 2013`
	In Cisco NCS, the alarm is not seen until the actual AP time matches the time reported in the FT.
	Conditions:
	• Cisco 5500 Series WLC using Release 7.0.235.3
	• Cisco AP3500 in wIPS ELM mode
	• MSE 3350 using Release 7.0.201.204
	Workaround: None.

CSCug19563	**Symptom**: Cisco WiSM2 secondary WLC DP crashed due to deadlock in HA configuration while it booted and synchronized with the primary WLC. **Conditions**: This might occur rarely when there are multiple reboots of Cisco WLC in HA configuration. The Cisco WLC recovers after the reboot. **Workaround**: None.
CSCug25043	**Symptom**: The **config flexconnect group** "*flex group*" **multicast overridden-interface enable** command is required to enable multicast on AAA overridden interfaces. The command works if there are no spaces in the FlexConnect group name and then you do not have to use quotes in the command syntax. When you have a FlexConnect group name with spaces in it, the command syntax needs to use quotes to enclose the group name. The command does not work when quotes are used thereby leaving the command unusable for FlexConnect group names with spaces in them. **Conditions**: Unknown. **Workaround**: Use FlexConnect group name without spaces.

Table 8 Open Caveats (continued)

ID	Description
CSCug29840	**Symptom**: Sometimes error message is displayed on the console of the Cisco AP1140 during a radio failure detection and recovery. After a radio failure is detected, the radio resets. Between the time radio is nonoperational and operational, the error message is displayed a few times. **Conditions**: These debug messages are displayed due to radio failure detection and recovery. This issue is seen in 7.4.100.0 and 7.4.110.0 releases. **Workaround**: None.
CSCug34802	**Symptom**: Rogue containment fails on a 5-GHz radio. **Conditions**: Rogue on 5-GHz radio. **Workaround**: None.
CSCug38140	**Symptom**: Message displayed on Cisco WLC: `SNMPTask: Central Switch = TRUE` **Conditions**: Debugging is enabled on the client MAC for 802.11 mobile. **Workaround**: Disable SNMP polling from manager.
CSCug38888	**Symptom**: Disabled SSID is broadcast by a 2.4-GHz radio. **Conditions**: SSID was created and disabled previously. This is a very rare occurrence, and only seen once; never reproduced in the lab, **Workaround**: Reconfigure the Cisco AP.

CSCug57545	**Symptom**: Clients are unable to connect to SNMP NAC SSID. The following error message is displayed:
	`Unable to process out-of-band login request from <MAC and IP Addr>`
	`[device-filter]. Cause: OOB client<MAC and IP Addr> not found.`
	Conditions: Upgrade from Release 7.4.
	Workaround: Enable NAC Alert Client Trap.

CSCug73845	**Symptom**: Cisco WLC NAS ID override takes system name instead of the NAS ID that is configured on an AP group, WLAN, or an interface. **Conditions**: Configure a NAS ID for an AP group, WLAN, or an interface. **Workaround**: Unknown.

CSCuh12796	**Symptom**: Consecutive SNMP 'set' commands for same MIB variable on Cisco WLC fails.
	Conditions: When we set a MIB object on Cisco WLC using SNMP 'set' command, it works at the first attempt. However, if you repeat the same command, the following error message is displayed:
	`Error in packet.`
	`Reason: noCreation (That table does not support row creation or that`
	`object can not ever be created)`
	Workaround: Perform SNMP 'get' before doing 'set'.

Table 8 Open Caveats (continued)

ID	Description
CSCuh16842	**Symptom**: Client gets IPv6 address from a different VLAN. **Conditions**: This is a combination of the following factors: • Interface group • Client sends traffic from either a static IP address or a previously allocated IP address. • Client traffic does not match the assigned VLAN that was initially received. The following system message is displayed when this occurs: `Overriding interface of client from 'vlan20' to 'vlan30' within interface group 'vlan20-30'` **Workaround**: Use DHCP Required.
CSCuh42398	**Symptom**: Logs show the following: `#NIM-3-CANT_DISABLE_MCAST: nim.c:4542 Cannot disable multicast state` **Conditions**: Unknown. **Workaround**: None.
CSCuh42665	**Symptom**: Cisco WLC sends incorrect information for Rogue AP detection through traps. **Conditions**: Only with Release 7.4. **Workaround**: None.

CSCuh16870	**Symptom**: Client with static IP address loses connectivity on session timeouts.
	Conditions: This occurs only if the following conditions are met:
	Interface that the client would get from an interface group does not match the interface corresponding to the static IP address.
	Client gets VLAN overridden and the following message is displayed:
	`apfReceiveTask: May 28 12:48:28.066: 00:1a:70:a5:2f:bd Overriding interface of client from 'vlan20' to 'vlan30' within interface group 'vlan20-30'`
	`*apfReceiveTask: May 28 12:48:28.066: 00:1a:70:a5:2f:bd Applying Interface policy on Mobile, role Local. Ms NAC State 2 Quarantine Vlan 0 Access Vlan 20`
	This overriding is lost when PMK expires, and a new authentication occurs. This occurs even if the client continuously sends traffic.
	Workaround: Either disable interface groups or enable DHCP required.

Table 8 Open Caveats (continued)

ID	Description
CSCuh26716	**Symptom**: The **show redundancy summary** command shows the following line regardless of its real SKU: `Unit = Secondary - HA SKU` **Conditions**: Enter the **show redundancy summary** command on the following: Secondary Cisco WLC which is converted from the primary Cisco WLC. HA-SKU Cisco WLC. **Workaround**: None.

CSCuh46442	**Symptom**: Cisco lightweight access point displays %CAPWAP-3-ERRORLOG messages when AP associates with the Cisco WLC:
	`%CAPWAP-3-ERRORLOG: Invalid event 10 & state 5 combination.`
	` %CAPWAP-3-ERRORLOG: CAPWAP SM handler: Failed to process message type 10 state 5.`
	` %CAPWAP-3-ERRORLOG: Failed to handle capwap control message from controller`
	` %CAPWAP-3-ERRORLOG: Failed to process encrypted capwap packet from 172.22.170.1`
	Conditions: AP join process.
	Workaround: Unknown.

CSCuh52238	**Symptom**: False DFS detections related to client activity. **Conditions**: Clients trigger DFS detections due to spurious emissions. This commit tracks additional filtering Cisco can do from their side to help with DFS falsing. The commit as per customer site information helps with DFS falsing about 30 percent of the time. Broadcom is simultaneously working on a fix from their side as well to address the root issue. **Workaround**: Use non-DFS channels.
CSCuh72474	**Symptom**: Cisco WLC assigns an interface inside a group to Dirty list. This is observed when some clients insist on requesting an IP address outside of their connected interface range in a flood (more than 100 DHCP request in the same second). The DHCP server begins to slow down the responses as a result of this flood. Since the dirty marking is based on requests without responses, the interface is marked as Dirty. **Conditions**: Clients request an IP address outside of their range in a flood way. **Workaround**: None.
CSCui22330	**Symptom**: This issue is to track and discuss default QoS values for L2 and L3 QoS priority markings. **Conditions**: None. **Workaround**: You can map each priority on its switch/router between Cisco WLC and AP. In Release 7.5, the default value of DSCP is 18 (010 010), which is IP Precedence 2 and it belongs to Class 2.

Table 8 Open Caveats (continued)

ID	Description
CSCui71605	**Symptom**: The running configuration taken with transfer upload is incomplete and therefore cannot be used for analysis. **Conditions**: Using transfer upload versus **sh run** command. **Workaround**: Use the **sh run-config** command.
CSCui73764	**Symptom**: Cisco AP1242: DHCP does not work with FlexConnect if VLAN Native is 2. **Conditions**: • FlexConnect local switching • Cisco AP1242 • Release 7.4.100.60 • VLAN Native is 2 • User unable to get IP address and to connect to the network **Workaround**: Change the native VLAN or use Release 7.4.100.0.
CSCui90116	**Symptom**: 802.11r roaming failure. **Conditions**: Client sends retry packet for FT-AUTH request. Original packet and then following a retry, packet with same SN. **Workaround**: Use a non-802.11r SSID/clients. **Further Problem Description**: AP does not detect the second retry packet as a duplicate packet and forwards both packets to Cisco WLC. Therefore, there are two FT-Auth responses with different Announce numbers and (FT-AUTH responses from Cisco WLC). Client uses the Announce received in the first FT-AUTH but Cisco WLC has the last updated Announce (which is sent for retry packet). This results in MIC failure.

CSCui99062	**Symptom**: Cisco WLC accepts the SysRq Magic key on the console. This allows even an unauthenticated user who has access to the serial console to unconditionally reboot the Cisco WLC from the SysRq menu.
	Following is the SysRq menu that pops up when you enter the magic key:
	`SysRq : HELP : loglevel0-8 reBoot Crashdump tErm Full kIll Dump showMem`
	`Nice showPc show-all-timers(Q) Sync showTasks Unmount shoW-blocked-tasks`
	Conditions:
	All released images
	SysRq magic key given from the serial console
	Workaround: Return key exits from the SysRq menu and returns to the console. Cisco WLC will still function normally while in the SysRq menu or even after exiting.

CSCuj15647	**Symptom**: APs report neighbors to be at abnormally high dBm. **Conditions**: Cisco AP2600 and AP3600. One AP on UNI 1 versus UNI 3. **Workaround**: None.

Table 8 Open Caveats (continued)

ID	Description
CSCuj28495	**Symptom**: clmgmtLicenseUsageCountRemaining task does not return the remaining AP count. **Conditions**: • Hardware: Cisco 5500 Series WLC • Software: Release 7.3.x **Workaround**: None.
CSCuj32157	**Symptom**: lb._dns-sd._udp.<domain-name> service is not supported by Cisco WLC. **Conditions**: When clients query for services of the nature mdns:lb._dns-sd._udp.<domain-name>, the Cisco WLC does not process the request because it is not listed in the master service database. Therefore, the service provider might or might not see the service provider. **Workaround**: Remove the domain name setting in the DHCP and on the clients (iPads, iPhones, and so on) from the server setting.
CSCuj32257	**Symptom**: AP secures CAC bandwidth for SIP phone in case of inter-Cisco WLC roaming even though the phone does not have any active SIP call. **Conditions**: SIP phone is roaming inter-Cisco WLC. Occurs only in case of a 32-byte call ID. **Workaround**: Use call ID, which is less than 32 bytes.
CSCuj53861	**Symptom**: The **config advanced statistics** command cannot be applied in Cisco WLC. **Conditions**: All Cisco WLC releases. **Workaround**: None.
CSCug34802	**Symptom**: Rogue containment fails on the 5-GHz radio. **Conditions**: Rogue on the 5-GHz radio. **Workaround**: None.
CSCuj36599	**Symptom**: On an 802.1X WLAN that has local switching in enabled state and where P2P blocking is in enabled state, if two clients are associated with the same AP, P2P blocking between them does not work as designed. However, for SSID with OPEN authentication, it works as expected. **Conditions**: • 802.1X WLAN with local switching enabled and P2P blocking enabled. • Release 7.4.110.0. **Workaround**: Remove VLAN override from AAA.

Table 8 Open Caveats (continued)

ID	Description
CSCui75794	**Symptom**: The foreign Cisco WLC does not respond to ARP from foreign export client to a local client being on the same VLAN. **Conditions**: • Client1 associates to Cisco WLC1 (local) • Client1 does an L3 roam to Cisco WLC2 (Cisco WLC2 is foreign and Cisco WLC1 is the anchor) • Client2 associates with Cisco WLC2 (local) • Initiate traffic, that is ping from Client1 to Client2 **Workaround**: None.
CSCuj66912	**Symptom**: SNMP get for Cisco WiSM2 reports that Cisco WiSM2 has secondary power supply. **Conditions**: Cisco WiSM2 using Release 7.0.235.3. **Workaround**: None.
CSCuj78942	**Symptom**: Trunk VLAN ID is not saved for Cisco AP1240. The VLAN ID is set in the **Advanced** tab. The Cisco AP reboots, but the VLAN ID is not displayed. **Conditions**: Not applicable. **Workaround**: None. **Further Problem Description**: http://www.cisco.com/c/en/us/td/docs/wireless/controller/7-4/configuration/guides/consolidated/b_cg74_CONSOLIDATED/b_cg74_CONSOLIDATED_chapter_01101110.html#task_43A307F686B3487F931FA496571987CA Issue is not seen on other AP platforms such as Cisco AP3600 or AP1140.
CSCuj95892	**Symptom**: When a port in a LAG goes down and then comes back up, the Cisco WLC does not send 'interface up' message to syslog server. **Conditions**: This issue is seen when distribution ports are configured in a LAG, and syslog server is configured. **Workaround**: Look in the message logs in the Cisco WLC GUI.
CSCul16911	**Symptom**: Cisco APs disconnect from the Cisco WLC due to DTLS errors. **Conditions**: Cisco AP disconnects. **Workaround**: None.

Table 8 Open Caveats (continued)

ID	Description
CSCuj83637	**Symptom**: Following an HA failover, the service port on the active Cisco WLC that is configured to get its IP address through DHCP loses connectivity after the DHCP lease expires (or the DHCP renew is forced through the **config interface dhcp service-port** {**enable** | **disable**} command). In case of Cisco WiSM2, this connectivity issue might cause the Cisco WLC and Catalyst 6000 to fail to exchange WCP keep-alives. Thus, the **show wism status** command shows the active module to be not operational. **Conditions**: • Cisco WLC or Cisco WiSM2 using Release 7.4.110.x or Release 7.5.102.0 in an HA environment • The service port is configured for DHCP • The issue is seen after the following events happen in the specified order: • HA failover • Service port DHCP lease expiry **Workaround**: Configure a static IP address for the service ports on both peers and force an HA switchover. From the active Cisco WLC, enter the following commands: **config interface dhcp service-port disable** **config interface address service-port** *addr1 netmask* **config redundancy interface address peer-service-port** *addr2 netmask* **redundancy force-switchover** Forcing a switchover might disconnect all the clients and any mesh APs in Release 7.4.X. Therefore, we recommend that you perform this workaround during a maintenance window.
CSCul16796	**Symptom**: Client is using PEAP; the EAP handshake fails when the Cisco vWLC needs to send the server certificate. **Conditions**: Using a Cisco vWLC and an EAP method that requires certificates. The path MTU between the Cisco vWLC and the Cisco AP is 1200 bytes or less. **Workaround**: Increase the path MTU. **Further Problem Description**: This is a regression; the issue was not observed in Release 7.4.X.
CSCua52205	**Symptom**: WGB wired client does not get IP address while changing VLAN on a switchport. **Conditions**: Unknown. **Workaround**: After changing VLAN for a WGB wired client, in an autonomous setup, clear the bridge table on WGB. In a unified setup, shut down the Ethernet interface, clear the bridge table on WGB, wait for a couple of seconds, unshut the Ethernet interface.

Table 8 Open Caveats (continued)

ID	Description
CSCul25617	**Symptom**: When you try to enable AP Management on dynamic interface, the "Failed to Add MDNS profile" message is displayed. **Conditions**: Not applicable. **Workaround**: None.
CSCul25679	**Symptom**: Unmapped physical interface to VLAN forwarding native VLAN traffic and also not helpful for TFTP code upgrade on AP. **Conditions**: Not applicable. **Workaround**: None.
CSCul31732	**Symptom**: FlexConnect VLAN mode was changed to disabled after a power cycle. **Conditions**: Unknown. **Workaround**: Reconfigure the FlexConnect VLAN mode.
CSCul43921	**Symptom**: wIPS treat regular Cisco APs as rogues. **Conditions**: MSE Release 7.4 with wIPS; Cisco Prime Infrastructure Release 1.3 and 2.0. **Workaround**: None.

CSCul82557	**Symptom**: When there is a large deployment with Cisco Flex 7500 and Cisco 8500 Series WLCs with over 2000 Cisco APs associating with the Cisco WLC that has FlexConnect groups with a large number of clients at the same time. This might occur due to network outage or might be while testing different scenarios of pre-deployment.
	When the FlexConnect APs try to associate with the Cisco WLC, the Cisco WLC tries to send the PMK cache to the FlexConnect APs. This increases the CPU by increasing SPAMRECEIVETASK, messages queued into the queue which is handled by the spamReceiveTask.
	`spamReceiveTask at near 100 percent CPU`
	`Cisco APs associating and dissociating`
	`Queue overflows in spamAP Queues`
	Conditions: FlexConnect APs using FlexConnect groups associating with the Cisco WLC at the same time and when the Cisco WLC is sending the PMK to the FlexConnect APs.
	Workaround: Use the **test pmk cache delete all** command. This command deletes the PMK, which clears the queue and the Cisco APs associate again.

CSCuj21407	**Symptom**: Cisco AP3700 does not use 802.11ac rates for mesh backhaul, uses only 802.11n rates. **Conditions**: Cisco AP3700 in mesh mode. **Workaround**: None. **Further Problem Description**: Mesh protocol needs to be extended to handle 802.11ac capability and VHT rates.

Table 8 Open Caveats (continued)

ID	Description
CSCun12965	**Symptom**: Lightweight AP might send CAPWAP packets whose size is larger than 1500 bytes to test maximum path MTU. These large CAPWAP packets cause errors on a directly connected switch, if the switch cannot enable jumbo frame support. Because AireOS based Cisco WLC does not support jumbo frame, this behavior should not be enabled by default. **Conditions**: This symptom may be observed by using Lightweight AP IOS Release 15.2(4)JB or later releases, which support jumbo frames. **Workaround**: None. **Further Problem Description**: The errors on the neighboring switch does not affect client traffic because the error is caused by CAPWAP path MTU test packets.
CSCun27153	**Symptom**: L3 MGID gets created for ff02::2:ffxx:xxxx/104 groups. All 100 MGIDs per VLAN are occupied with these groups. Any new group cannot be created and multicast (v4/v6) does not work for the new group. **Conditions**: Apple MacBook with iOS 10.9.1 seems to generate MLD join for ff02::2:ffxx:xxxx/104 as per RFC 4620. **Workaround**: Disable MLD snooping.
CSCui01948	**Symptom**: On Cisco Prime Infrastructure 1.3, when monitoring APs, the following error message is displayed. `SNMP operation to Device failed Table too large, possible agent loop` **Conditions**: When the SSID is set to FlexConnect Local Switching and the AP is set to Local AP Mode and when a client is attached to the AP, an error in Cisco Prime Infrastructure is observed when trying to view AP or client attached to the AP. **Workaround**: None.
CSCul45107	**Symptom**: Cisco WLC on Release 7.5.102.0 stops responding silently in an HA topology. No crash file or core file. **Conditions**: • HA topology • No back-to-back redundancy port is used. • Using L2 network for keepalives. • High Availability enhancements: Redundancy ports can operate over a Layer 2 connection (multiple intermediate switches or routers). Therefore, a direct connection is not required. **Workaround**: None.
CSCum46098	**Symptom**: HA false switchover due to keepalive loss possibly in the kernel stack. **Conditions**: Possibly heavy load. **Workaround**: None.

Table 8 Open Caveats (continued)

ID	Description
CSCum66202	**Symptom**: FlexConnect local switching + Web-Auth + per-user ACL: Upon successful web authentication, the per-user ACL is correctly applied, but the web authentication page is unresponsive, with the redirect to the success/logout page pending. Explicitly permitting traffic to the virtual IP address does not help. **Conditions**: • FlexConnect local switching + Web-Auth + per-user ACL • Cisco AP3600 using Cisco WLC Release 7.5.102.0 or Release 7.6.100.0. **Workaround**: The same scenario works correctly if the following workarounds are applied: • No ACL is pushed • The pushed ACL is either empty or "permit IP any any"
CSCui38822	**Symptom**: When editing the WLCs in the HA tab of the AP, the GUI does not allow a secondary WLC to be moved up to the primary position. The following error message is displayed `Primary Controller: Unable to set controller name and IP address` **Conditions**: Swapping primary to secondary WLC roles. **Workaround**: This forces the user to delete the secondary WLC from the list, apply those changes, then edit the primary WLC field to the former secondary WLC name/IP and apply those changes.
CSCuc72713	**Symptom**: Static IP on clients working with interface group VLAN select feature gets assigned to an incorrect interface. **Conditions**: Though the static IP subnet exists as a valid interface, it does not get overridden to the correct subnet interface and gets marked into mac-hash interface and the client is unable to pass traffic. **Workaround**: Enter the **config ipv6 disable** command.

Resolved Caveats

Table 9 lists the caveats that have been resolved in Release 7.6.110.0.

Table 9 Resolved Caveats

ID	Title
CSCun37799	VideoStream failed with Release 7.6 on WPA2 SSID
CSCum68243	Cisco AP1530: dot11 ant-band-mode command was missing in Autonomous image
CSCuj17283	Cisco AP3700 used 8 replay counters with clients that support only one (ARP failed).
CSCum16566	When 1532I in the C, E, H, M and S domains, is powered with 802.3at PoE+ or AIR-PWRINJ4 power injector, one 2.4-GHz Tx was disabled
CSCum53468	DNS resolver enabled on AP

Table 9 Resolved Caveats (continued)

ID	Title
CSCum17989	After DFS RM3000AC-Q and AP3702I-Q show illegal channel 144 in CBW80 use
CSCum49200	Broadcom client connectivity problems if WMM is enabled with Cisco AP3600 in use
CSCun02785	Cisco AP1530: 7.6 D-domain 5G CTL update

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

You can access these documents at this URL: http://www.cisco.com/c/en/us/support/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.

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.