Release Notes for Cisco Wireless LAN Controllers and Lightweight Access Points for Release 8.0.110.0

First Published: December 22, 2014

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*.

Revision History

Table 1 ***Revision History***

Modification Date	Modification Details
November 10, 2017	• Open Caveats, page 27 – Added CSCvc65568
October 10, 2017	• Features Not Supported on Cisco Virtual WLCs, page 25 – Added Wired Guest and FlexConnect central switching.

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

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 (no AP SSO support), 5500 Series, Wireless Services Module 2 (WiSM2), Flex 7500 Series, and 8500 Series WLCs
- Cisco WiSM2 for Catalyst 6500 Series Switches

For information about features that are not supported on the Cisco WLC platforms, see Features Not Supported on Cisco WLC Platforms, page 23.

Supported Access Point Platforms

The following access point platforms are supported in this release:

- Cisco Aironet 1040, 1130, 1140, 1240, 1250, 1260, 1600, 1700, 2600, 2700, 3500, 3500p, 3600, 3700, Cisco 600 Series OfficeExtend, 702, 702W, AP801, and AP802 Series indoor access points
- Cisco Aironet 1520 (1522, 1524), 1530, 1550 (1552), 1570 Series outdoor access points

For information about features that are not supported on some access point platforms, see Features Not Supported on Access Point Platforms, page 26.

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

- AP860:

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

- AP880:

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

  http://www.cisco.com/c/en/us/products/collateral/routers/800-series-routers/data_sheet_c78-613481.html

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

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

- AP890:

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

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

  Before you use an AP802 series lightweight access point with Cisco WLC software release 8.0.110.0, 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

- "Enhancements to Cisco WLAN Express Setup for Cisco 2500 Series Wireless LAN Controller Feature" section on page 5
- "Change in Behavior with SSLv3 in Disabled State" section on page 6

Note If you have Cisco AP3700Ps, do not upgrade to Release 8.0.110.0; please contact TAC for software support. This does not apply to 3700i/3700e models. For more information, see https://tools.cisco.com/bugsearch/bug/CSCus35411.

For other updates in this release, see the "Caveats" section on page 27.

Note For an overview of features introduced in Release 8.0.100.0, see *Release Notes for Cisco Wireless LAN Controllers and Lightweight Access Points for Release 8.0.100.0*.

Support for Cisco Aironet 1570 Series Access Points

Support for Cisco Aironet 1570 Series Access Points is introduced. For more information, see http://www.cisco.com/c/en/us/products/wireless/aironet-1570-series/index.html.

The following GUI updates are made in Cisco WLC for the Cisco Aironet 1570 Series APs:

- The GPS Location information is moved to **Wireless > Access Points > All APs > AP Name > General** tab. In the earlier releases, this information was present in the **Mesh** tab.
- The **General** tab also shows the following new information: **Internal Temperature**, **Temperature State**, and **PoE Out State**.
- The **Internal Temperature** of the AP is displayed in both Celsius and Fahrenheit.
- The **Temperature State** is shown to be in one of three states: GREEN, YELLOW, or RED. The GREEN state indicates that the AP is functioning normally and the internal temperature is at an optimal operating temperature; the YELLOW state indicates that the AP state is in transition to either GREEN or RED state; if the AP is in RED state, it means that the internal temperature of the AP has increased and the number of antennas that are used for transmission will be reduced.
- The **PoE Out State** shows the status of the Power over Ethernet output port from the AP. The PoE Out State can be in OFF or ON state depending on the input power source for the AP.
- For Cisco 1570AP with a cable modem, the WLC GUI on **Wireless > Access Points > All APs > AP Name > General** tab has a link to the Statistics report, which shows information about the AP and lists the event logs.

Cisco Aironet Universal AP Priming and Cisco AirProvision

Priming a universal access point sets the regulatory domain and country configurations for the access point. Cisco AirProvision helps you set the unique regulatory domain and country configurations for a universal Cisco Aironet access point, based on the its geographical location. The regulatory domain and country configurations for your access point define the valid set of channels and allowed power levels for the country where the AP is installed. For more information, see *Cisco Aironet Universal AP Priming and Cisco AirProvision User Guide*.

Note Also see *Universal AP Regulatory Domain Deployment Guide*.

Enhancements to Cisco WLAN Express Setup for Cisco 2500 Series Wireless LAN Controller Feature

Connect to any Port

The Cisco WLAN Express Setup for Cisco 2500 Series Wireless Controller feature is enhanced so that you can now connect a client device to any port on the Cisco 2500 Series WLC and access the GUI configuration wizard to run Cisco WLAN Express Setup. Previously, you were required to connect the client device to only port 2.

Wireless Support to run Cisco WLAN Express Setup

You can connect an AP to any of the ports on the Cisco 2500 Series WLC, associate a client device with the AP, and run Cisco WLAN Express Setup. When the AP is associated with the Cisco 2500 Series WLC, only 802.11b and 802.11g radios are enabled; the 802.11a radio is disabled. The AP broadcasts an SSID named "CiscoAirProvision," which is of WPA2-PSK type with the key being "password." After a client device associates with this SSID, the client device automatically gets an IP address in the 192.168.x.x range. On the web browser of the client device, go to http://192.168.1.1 to open the GUI configuration wizard.

This feature is supported only on the following web browsers:

- Microsoft Internet Explorer 10 and later versions
- Mozilla Firefox 32 and later versions
- Google Chrome 38.X and later versions
- Apple Safari 7 and later versions

Note This feature is not supported on mobile devices such as smartphones and tablet computers.

Preparing Cisco 2500 Series WLC to use Cisco WLAN Express Setup (Wireless)

Step 1 Plug in a Cisco AP to any one of the ports of Cisco 2500 Series WLC. If you do not have a separate power supply for the AP, you can use Port 3 or Port 4, which supports PoE.

Step 2 After the AP boots up, the AP associates with the WLC and downloads the WLC software.

Step 3 The AP starts provisioning a WPA2-PSK SSID "CiscoAirProvision" with the key "password."

Step 4 Associate a client device to the "CiscoAirProvision" SSID.

The client device is assigned an IP address in the 192.168.x.x range.

Step 5 On the web browser of the client device, go to http://192.168.1.1 to open the GUI configuration wizard, which you can use to run Cisco WLAN Express Setup.

Note From Release 8.0.110.0 onwards, the Autoinstall feature is not supported on Cisco 2504 WLC.

Change in Behavior with SSLv3 in Disabled State

Because of CSCur27551, Cisco WLC has a new behavior where SSLv3 is disabled by default. Older browsers, for example Microsoft Internet Explorer 8, might fail to connect over HTTPS because of compatibility issues. In such cases, you can explicitly enable SSLv3 by entering the **config network secureweb sslv3 enable** command.

Software Release Support for Access Points

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

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

Table 2 Software Support for Access Points

Access Points		First Support	Last Support
700 Series	AIR-CAP702I-x-K9	7.5.102.0	—
	AIR-CAP702I-xK910	7.5.102.0	—
700W Series	AIR-CAP702Wx-K9	7.6.120.0	—
	AIR-CAP702W-xK910	7.6.120.0	—
1000 Series	AIR-AP1010	3.0.100.0	4.2.209.0
	AIR-AP1020	3.0.100.0	4.2.209.0
	AIR-AP1030	3.0.100.0	4.2.209.0
	Airespace AS1200	—	4.0
	AIR-LAP1041N	7.0.98.0	—
	AIR-LAP1042N	7.0.98.0	—
1100 Series	AIR-LAP1121	4.0.155.0	7.0.x
1130 Series	AIR-LAP1131	3.1.59.24	—
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	—

Table 2 Software Support for Access Points (continued)

Access Points		First Support	Last Support
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	—
1700 Series	AIR-CAP1702I-x-K9	8.0.100.0	—
	AIR-CAP1702I-xK910	8.0.100.0	—
AP801		5.1.151.0	—
AP802		7.0.98.0	—
AP802H		7.3.101.0	—
2600 Series	AIR-CAP2602I-x-K9	7.2.110.0	—
	AIR-CAP2602I-xK910	7.2.110.0	—
	AIR-SAP2602I-x-K9	7.2.110.0	—
	AIR-SAP2602I-x-K95	7.2.110.0	—
	AIR-CAP2602E-x-K9	7.2.110.0	—
	AIR-CAP2602E-xK910	7.2.110.0	—
	AIR-SAP2602E-x-K9	7.2.110.0	—
	AIR-SAP2602E-x-K95	7.2.110.0	—
2700 Series	AIR-CAP2702I-x-K9	7.6.120.0	—
	AIR-CAP2702I-xK910	7.6.120.0	—
	AIR-CAP2702E-x-K9	7.6.120.0	—
	AIR-CAP2702E-xK910	7.6.120.0	—
	AIR-AP2702I-UXK9	8.0.110.0	—
3500 Series	AIR-CAP3501E	7.0.98.0	—
	AIR-CAP3501I	7.0.98.0	—
	AIR-CAP3502E	7.0.98.0	—
	AIR-CAP3502I	7.0.98.0	—
	AIR-CAP3502P	7.0.116.0	—

Table 2 Software Support for Access Points (continued)

Access Points		First Support	Last Support
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 7.2.115.2 or a later release.			
1500 Mesh Series	AIR-LAP-150	3.1.59.24	4.2.207.54M
	AIR-LAP-1510	3.1.59.24	4.2.207.54M

Table 2 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-CAP1552C-x-K9	7.0.116.0	—
	AIR-CAP1552E-x-K9	7.0.116.0	—
	AIR-CAP1552H-x-K9	7.0.116.0	—
	AIR-CAP1552I-x-K9	7.0.116.0	—
	AIR-CAP1552EU-x-K9	7.3.101.0	—
	AIR-CAP1552CU-x-K9	7.3.101.0	—
	AIR-CAP1552WU-x-K9	8.0.100.0	—

Table 2 Software Support for Access Points (continued)

Access Points		First Support	Last Support
1552S	AIR-CAP1552SA-x-K9	7.0.220.0	—
	AIR-CAP1552SD-x-K9	7.0.220.0	—
1570	AIR-AP1572EAC-x-K9	8.0.110.0	
	AIR-AP1572ICy[2]-x-K9	8.0.110.0	
	AIR-AP1572ECy-x-K9	8.0.110.0	

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

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

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

Software Release Types and Recommendations

This section contains the following topics:

Types of Releases

Table 3 Types of Releases

Type of Release	Description	Benefit
Maintenance Deployment (MD) releases	Software releases that provide bug-fix support and ongoing software maintenance. These releases are categorized as Maintenance Deployment (MD) and may be part of the AssureWave program.[1] These are long-lived releases with ongoing software maintenance.	Provides you with a software release that offers stability and long support duration with periodic maintenance releases (MRs).
Early Deployment (ED) releases	Software releases that provide new features and new hardware platform support in addition to bug fixes. These releases are categorized as Early Deployment (ED). These are short-lived releases.	Allows you to deploy the latest features and new hardware platforms or modules.

1. AssureWave is a Cisco program that focuses on satisfying customer quality requirements in key industry segments in the mobility space. This program links and expands on product testing conducted within development engineering, regression testing, and system test groups within Cisco. The AssureWave program has established partnerships with major device and application vendors to help ensure broader interoperability with our new release. The AssureWave certification marks the successful completion of extensive wireless 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 4 Software Release Recommendations

Type of Release	Deployed Release	Recommended Release
Maintenance Deployment (MD) release	7.0 MD release train (latest release: 7.0.250.0)	7.4 MD release train (7.4.121.0 is the MD release)
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 MD release)
Early Deployment (ED) releases for 802.11ac deployments	7.5 ED release 7.6 ED release	7.6 ED release (7.6.130.0 is MR3 on 7.6 release train)

For detailed release recommendations, see the software release bulletin:

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

Solution Compatibility Matrix

Table 5 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
8.0 (MD train)	1.3	2.1.1	8.0

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

Upgrading to Cisco WLC Software Release 8.0.110.0

Note If you have Cisco AP3700Ps, do not upgrade to Release 8.0.110.0; please contact TAC for software support. This does not apply to 3700i/3700e models. For more information, see https://tools.cisco.com/bugsearch/bug/CSCus35411.

Guidelines and Limitations

- Cisco WLCs validate client IP address at the time of learning, using the dynamic interface IP address as per the VLAN assigned to the client. Ensure that the clients and the dynamic interface VLAN of the clients are on the same subnet, even if DHCP proxy is disabled at the Cisco WLC.
- 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 downgrade from Release 8.0.110.0 to a 7.x release, the trap configuration is lost and must be reconfigured.
- If you have ACL configurations in the Cisco WLC and downgrade from a 7.4 or a later release to a 7.3 or an earlier release, you might experience XML errors on rebooting the Cisco WLC. However, these errors do not have any impact on any functionality or configurations.

- If you are upgrading from a 7.4.X or an earlier release to a later release, the Called Station ID type information is mapped to the RADIUS Accounting Called Station ID type; the RADIUS Authentication Called Station ID type, by default, is set to apradio-mac-ssid. You can configure the RADIUS Authentication Called Station ID type information by using the **config radius auth callStationIdType** command.
- When FlexConnect access points (known as H-REAP access points in the 7.0.x releases) that are associated with a Cisco WLC that has all the 7.0.x software releases prior to Release 7.0.240.0 upgrade to Release 8.0.110.0, 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 8.0.110.0.
- 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.
- 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 8.0.110.0 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 8.0.110.0. Table 6 shows the upgrade path that you must follow before downloading Release 8.0.110.0.

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

Table 6 Upgrade Path to Cisco WLC Software Release 8.0.110.0

Current Software Release	Upgrade Path to 8.0.110.0 Software
7.0.x releases	You can upgrade directly to 8.0.110.0. **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 8.0.110.0 to avoid losing those VLAN settings.
7.1.91.0	You can upgrade directly to 8.0.110.0.
7.2.x releases	You can upgrade directly to 8.0.110.0. **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 8.0.110.0 Cisco WLC software release. You must downgrade from the 8.0.110.0 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 8.0.110.0.
7.4.x releases	You can upgrade directly to 8.0.110.0.
7.5.x releases	You can upgrade directly to 8.0.110.0.
7.6.100.0	You can upgrade directly to 8.0.110.0.
8.0.100.0	You can upgrade directly to 8.0.110.0.

- 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.
- 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.
- We recommend that you insert Interoperability test for RADIUS to show Cisco ISE.

- When you upgrade to the latest software release, the software on the access points associated with the Cisco WLC is also automatically upgraded. When an access point is loading software, each of its LEDs blinks in succession.
- We recommend that you access the Cisco WLC GUI using Microsoft Internet Explorer 9 or a later version or Mozilla Firefox 17 or a later version.

Note Older browsers, for example Microsoft Internet Explorer 8, might fail to connect over HTTPS because of compatibility issues. In such cases, you can explicitly enable SSLv3 by entering the **config network secureweb sslv3 enable** command.

- Cisco WLCs support standard SNMP Management Information Base (MIB) files. MIBs can be downloaded from the Software Center on Cisco.com.
- The Cisco WLC software is factory installed on your Cisco WLC and is automatically downloaded to the access points after a release upgrade and whenever an access point joins a Cisco WLC. We recommend that you install the latest software version available for maximum operational benefit.
- Ensure that you have a TFTP, FTP, or SFTP server available for the software upgrade. Follow these guidelines when setting up a server:
  - Ensure that your TFTP server supports files that are larger than the size of Cisco WLC software Release 8.0.110.0. 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 8.0.110.0 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 8.0.110.0 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 8.0.110.0 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 8.0.110.0 (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 8.0.110.0 Cisco WLC software:

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

http://www.cisco.com/cisco/software/navigator.html

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

c. Click **Wireless LAN Controllers**.

The following options are 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 Choose **Commands** > **Download File** to open the Download File to Controller page.

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

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

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

Step 9 If you are using a TFTP server, the default values of 10 retries for the **Maximum Retries** text field, and 6 seconds for the Timeout text field should work correctly without any adjustment. However, you can change these values if desired. To do so, enter the maximum number of times that the TFTP server attempts to download the software in the Maximum Retries text box and the amount of time (in seconds) that the TFTP server attempts to download the software, in the **Timeout** text box.

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

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

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

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

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

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

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

A message appears indicating the status of the download.

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

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

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

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

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

Step 19 To verify that the 8.0.110.0 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 19 detailed in the "Upgrading to Cisco WLC Software Release 8.0.110.0" section on page 12.

Interoperability With Other Clients in Release 8.0.110.0

This section describes the interoperability of Release 8.0.110.0 of the Cisco WLC software with other client devices.

Table 7 describes the configuration used for testing the clients.

Table 7 Test Bed Configuration for Interoperability

Hardware/Software Parameter	Hardware/Software Configuration Type
Release	8.0.110.0
Cisco WLC	Cisco 5500 Series Controller

Table 7 Test Bed Configuration for Interoperability (continued)

Access points	1142, 3500e, 3500i, 3600, 2602, 3702, 2702, 702W
Radio	802.11ac, 802.11a, 802.11g, 802.11n2, 802.11n5
Security	Open, WEP, PSK (WPA and WPA2), 802.1X (WPA-TKIP and WPA2-AES) (LEAP, PEAP, EAP-FAST, EAP-TLS)
RADIUS	ACS 4.2, ACS 5.2
Types of tests	Connectivity, traffic, and roaming between two access points

Table 8 lists the client types on which the tests were conducted. The clients included laptops, handheld devices, phones, and printers.

Table 8 Client Types

Client Type and Name	Version
Laptop	
Intel 4965	v13.4
Intel 5100/5300/6200	v14.3.2.1
Intel 6300	v15.11.0.7
Intel 1000/1030/6205	v14.3.0.6
Intel 7260 (11AC)	17.1
Intel 3160 (11AC)	17.1
Broadcom 4360 (11AC)	6.30.163.2005
Linksys AE6000 (USB 11AC)	5.0.7.0
Netgear A6200 (USB 11AC)	6.30.145.30
D-Link DWA-182 (USB 11AC)	6.30.145.30
Dell 1395/1397/Broadcom 4312HMG(L)	5.30.21.0
Dell 1501 (Broadcom BCM4313)	v5.60.48.35/v5.60.350.11
Dell 1505/1510/Broadcom 4321MCAG/4322HM	5.60.18.8
Dell 1515(Atheros)	8.0.0.239
Dell 1520/Broadcom 43224HMS	5.60.48.18
Dell 1530 (Broadcom BCM4359)	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)	10.10
MacBook Air	OSX 10.10
Macbook Pro with Retina Display 2013	OSX 10.10
Tablets	
Apple iPad2	iOS 8.1.2(12B440)
Apple iPad3	iOS 8.1.2(12B440)

Table 8 Client Types (continued)

Client Type and Name	Version
Apple iPad mini with Retina display	iOS 8.1.2(12B440)
Apple iPad Air	iOS 8.1.2(12B440)
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
Samsung Galaxy Tab 10.1- 2014 SM-P600 (11AC)	Android 4.4.2
Samsung Galaxy Note 3 SM-N900(11AC)	Android 4.4.2
Microsoft Surface Pro 3 Tablet (11AC)	Windows 8.1 Driver: 15.68.3044.85
Microsoft Surface Pro 2	Windows 8.1 Driver: 14.69.24039.134
Motorola Xoom	Android 3.1
Nexus 7 2nd Gen	Android 4.4.2
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	1.4.5.3.LOADS
Cisco 7925G	1.4.5.3.LOADS
Ascom i75	1.8.0
Spectralink 8030	119.081/131.030/132.030
Apple iPhone 4S	iOS 8.1.2(12B440)
Apple iPhone 5	iOS 8.1.2(12B440)
Apple iPhone 5s	iOS 8.1.2(12B440)
Apple iPhone 5c	iOS 8.1.2(12B440)
Apple iPhone 6	iOS 8.1.2(12B440)
Apple iPhone 6 Plus	iOS 8.1.2(12B440)
HTC One(11AC)	Android 4.2.2
Samsung Galaxy S4 GT-I9500 (11AC)	Android 4.3
Sony Xperia Z Ultra(11AC)	Android 4.3
Nokia Lumia 1520 (11AC)	Windows Phone 8.1
Google Nexus 5 (11AC)	Android 4.4.3
Samsung Galaxy S5-SM-G900A (11AC)	Android 4.4.2
HTC Sensation	Android 2.3.3

Table 8 Client Types (continued)

Client Type and Name	Version
Samsung Galaxy S III	Android 4.3
SpectraLink 8450	3.0.2.6098/5.0.0.8774
Samsung Galaxy Nexus GTI9200	Android 4.2.2
Sony Xperia Z Ultra (11AC)	Android 4.4.2
Samsung Galaxy Mega SM900 (11AC)	Android 4.4.2

Features Not Supported on Cisco WLC Platforms

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

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

Features Not Supported on Cisco 2500 Series WLCs

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

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

- 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 (use Flex + Bridge mode for mesh enabled FlexConnect deployments)
- Spanning Tree Protocol (STP)
- Cisco Flex 7500 Series WLC cannot be configured as a guest anchor Cisco WLC. However, it can be configured as a foreign Cisco WLC to tunnel guest traffic to a guest anchor Cisco WLC in a DMZ.
- Multicast

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

- PMIPv6

Features Not Supported on Cisco 8500 WLCs

- TrustSec SXP
- Internal DHCP Server

Features Not Supported on Cisco Virtual WLCs

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

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

- FlexConnect central switching

Note FlexConnect local switching is supported.

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

Note Outdoor APs in the FlexConnect mode are supported.

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

Features Not Supported on 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

Features Not Supported on Access Point Platforms

Features Not Supported on 1130 and 1240 APs

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

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

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

- PPPoE
- PMIPv6

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

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

Caveats

Cisco Bug Search Tool

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

To view the details of a caveat listed in this document:

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

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

Open Caveats

Use the BST to view the details of a caveat listed in this section. For more information about the BST, see the "Cisco Bug Search Tool" section on page 27.

Table 9 Open Caveats

ID	Headline
CSCus45806	Enable CDP Spare pair TLV for 1570 and 1530 series access points
CSCsv54436	SSH to WLC is sometimes denied "Sorry, Telnet is not allowed on..."
CSCuc78713	dWEP client cannot receive broadcast after broadcast key rotation
CSCuh20715	"WLC 5508 crashed on 7.3.101.0 Reaper Reset: Task "LDAP DB Task 2"
CSCui57047	Cisco WLC stopped working with taskname SXP SOCK
CSCuj60872	WLC crash due to reaper reset for apfMsConnTask_6
CSCuj93777	Mesh AP should block data packets before BPDU packets are handled
CSCul40203	Interface is not marked as dirty because of dual stack clients
CSCul53090	IPv6 stopped to be forwarded through WLC BCast queue full
CSCum25947	PPPoE configurations are still retained after write erase on AP
CSCun20584	AP replicates broadcast packets to the default gateway
CSCun34295	WiSM2 crash on task radiusTransportThread
CSCun59052	Page error occurs after applying the configuration on the VLAN mapping page
CSCun83393	Cannot compile CISCO-LWAPP-DOT11-CLIENT-MIB by MG-Soft

Table 9 Open Caveats (continued)

ID	Headline
CSCun96815	OEAP ACLs and network lists are deleted after upload/download of the configuration
CSCuo05142	EAP-AKA Client Unable to Reauth Using Fast Re-Auth Id & Mult Auth Server
CSCuo19677	Cisco WLC does not update AP with new bandwidth setting
CSCuo43002	Enabling IP Protocol 119 from GUI does not display on show-run
CSCuo48442	Stale old DTLS data_encryption session histories are left on WLC
CSCuo70310	Flex+bridge with PPPoE mode AP not associating with Cisco WLC
CSCuo96366	WLC sends RADIUS packets with same ID without doing RADIUS ID check
CSCup00196	Local auth EAP-FAST not working for Flex AP Auth users on AP1240
CSCup02792	CLI configuration issues regarding enabling or disabling of rogue traps
CSCup29095	Mesh: PI not showing the neighbor details in mesh links page of Parent
CSCup31640	Changing channel to Auto does not set maximum bandwidth for FlexConnect APs
CSCup46302	Virtual WLC: RSSI missing from Monitor mode AP
CSCup49763	RRM: All channel scan option does not work in AP702 and AP702w
CSCup50512	Webauth Redirect Loops with guest user role
CSCup54560	AP2600 in mesh mode dissociates from Cisco WLC
CSCup57457	WS-SVC-WISM2-K9 unable to change Rogue state
CSCup60282	Ping generated from WLC seen as incorrect ICMP type
CSCup64468	WLC device sends invalid format “#” in front of syslog message
CSCup71136	MAC filter: MAC delimiter does not change in accounting message
CSCup72502	Cisco 5500 Series WLC using Release 7.6 does not deauthenticate the client when FlexConnect ACL is not present on the Cisco AP
CSCup77631	IPv6 queue full and continuous IPv6 message logs
CSCup80403	Low iMac throughput; supported rate IE in association response has zero length
CSCup81511	Incorrect WMM UP to DSCP markings on AP1131 and AP1242
CSCup85896	Interference profile failure for secondary40 channel
CSCup86941	GUI: Policy type for “Static WEP” clients is showing as N/A
CSCup88910	630937505 - AP impersonation flood of events on WLC 8510-SR14-00512
CSCup92480	802.11ac crash due to PCI reset
CSCup96492	IPv6 route with /128 prefix removes after reboot
CSCup97263	Flex 7500 WLC: System Crash Dot1x_NW_MsgTask_2
CSCup98731	https-redirect command is missing in the uploaded config file
CSCuq05410	vWLC/SRE: Boot option 3 to change active boot image is not working
CSCuq08623	WLC crash due to Double free in cdpFreeCacheTable()
CSCuq09859	APs sending GARP and ARP requests approximately every 2 seconds
CSCuq14231	7500 WLC: Efficient upgrade IPv6—slaves cannot download new image
CSCuq20950	AVC profile not able to block BitTorrent traffic

Table 9 Open Caveats (continued)

ID	Headline
CSCuq21626	IP address reversed in duplicate IP trap in 8500 WLC
CSCuq21999	CAPWAPv6 DTLS sessions tear down when data DTLS is enabled
CSCuq26793	PPPoE: Beacons stuck RLDP_STOP payload not received AP after RLDP_START
CSCuq28038	Hop2—multiple attempts to rejoin WLC in very-fast convergence
CSCuq28973	8500 WLC crashed on “IPv6_Msg_Task”
CSCuq32731	WLC stopped working on mmRemoveHbMbr while peering with new mobility
CSCuq36265	802.11ac: Surface client not associating on 802.11ac if SSID is not broadcast
CSCuq48800	Low throughput due to UAPSD for Intel 7260 Wi-Fi chipset
CSCuq50069	SHA1 key cipher not working between WLC 8.0 and MSE 8.0 releases.
CSCuq54548	5508 WLC Silent crash on 7.6.120.x
CSCuq56829	Flex+Bridge MAPs drop after association; failed to receive data keep-alive
CSCuq60042	Memory leak on WLC when using PMIPv6 clients pem_api.c
CSCuq61208	RADIUS + Webauth + Anchoring + Accounting is causing webauth loop
CSCuq63642	Internal web page appears after successful redirect to external webauth
CSCuq66684	802.11ac capable MacBook 2014 unable to get ARP response from LAP
CSCuq68753	5500 anchor running 7.6.x.x crashed on osapiBsnTimer
CSCuq71068	AP traffic issue causing client to lose layer 3 connectivity
CSCuq72285	Unable to insert line break in Internal Web-Auth message window
CSCuq73072	Mesh Convergence list includes incorrect channel
CSCuq73590	WLC adds incorrect class attribute in accounting stop
CSCuq74491	WLC 8.0.100.0 crashes due to Task Name: apfRogueTask_0
CSCuq86252	DFS false detection on manufacturing plant
CSCuq86263	DFS on AP1600
CSCuq86269	DFS detection due to Broadcom spurious emissions
CSCuq86274	AP1530 DFS detection across all channels
CSCuq88333	FlexConnect AP2700 5-GHz radio stops accepting clients
CSCuq88748	Rogue APs wrong classification from malicious to unclassified
CSCuq90632	AP3702 crashed with a traceback
CSCuq91056	Interface Dot11Radio1 flapping on AP3702
CSCuq94678	WiSM2 not responding to ARP requests
CSCuq96986	WLC 2504 crash on upgrade to 8.0
CSCuq97914	PI 1.4 cannot finish auditing WLC
CSCuq98802	WLC 7.6 memory leak on aaaqueuereader
CSCur02514	Release 8.0.100.0: SNMP trap is not sent out on HA switchover
CSCur07086	AP1142 Config loss after cold reboot
CSCur10713	Wireless controller returns a null value using SNMP for memory usage

Table 9 Open Caveats (continued)

ID	Headline
CSCur10853	Several APs crashes on Release 8.0.100.0
CSCur11060	False positive on honeypot alert with multiple SSIDs
CSCur19331	Clients cannot complete DHCP and are deauthenticated from vWLC
CSCur20154	HA SSO pair memory leak
CSCur23915	WLC Reaper Reset during AP image predownload
CSCur24512	AP3602i crash at dot11_driver_ie_find
CSCur30074	AP802- Radio Reset Mode - Code 71
CSCur31693	AP1570: 9 Mbps Link Test fails. 100% packet loss
CSCur32475	New Mobility Web Auth on MAC Filter Failure always send client to web auth
CSCur33320	SC1/SC2/SC3 Radio reset w/ FW stuck in macenb (Cont. of CSCuo27106)
CSCur37475	WiSM2 system crash - at client stats AVL corruption
CSCur38682	FlexConnect AP—Local switch/local auth sends deauth 802.1x on PSK WLAN
CSCur40312	AVC does not mark YouTube traffic from Android devices in Release 8.0.100.0
CSCur40950	FlexConnect Clients with AAA override randomly default to management VLAN
CSCur45862	APs cannot discover WLC through option 43 in Release 8.0.100.0
CSCur46884	Bouncing power to WiSM2 causes second 10-GHz link to stop forwarding data
CSCur49165	WiSM2 system crash radiusTransportThread aaaRadiusAuth
CSCur52246	PMIPv6 GRE key database gets full during scale testing
CSCur54531	Interface Dot11Radio1 resets on AP3702 causing operational down state
CSCur92472	PMIPv6: Roaming WLC1->WLC2 does not work; wrong handoff indicator
CSCuq45110	M1 is sometimes encrypted leading to M1 refusal on station side
CSCuq55962	Non-WMM Client outer CAPWAP DSCP is not marked as per WLAN QoS profile
CSCuq91181	Client does not regain IP connectivity after roaming
CSCur00288	Release 8.0.100.0 client is shown with “IP address unknown” and “DHCP required”
CSCur10487	External webauth redirect not working properly for https://<virtual-ip>
CSCur19519	MAP stuck on 802.1x after error condition + roaming
CSCur22714	AP3602 trying to contain its own RM3000AC module
CSCur47745	Client unable to join WLAN with FlexConnect Central DHCP processing
CSCur48944	Problem in Client Stats Reports and Optimized Roaming
CSCur54332	Failed to parse RADIUS AVP XML file in standby WLC
CSCur54681	GUI: Flex+Bridge Parent inherited Flex VLAN mappings not reflected on MAP
CSCur56576	WLC does not support 802.11a for Qatar
CSCur63456	Delay on Apple iOS devices to show connection
CSCur71427	“Flex: Client roaming fails “not processing DOT1X_4WAY_COMPLETED_AT_AP”
CSCur86600	ap3g2 recovery image sends BPDU to the network
CSCur91376	Memory corruption on Rogue task for Release 8.0

Table 9 Open Caveats (continued)

ID	Headline
CSCus00818	Some BlackBerry Z10 devices reported as Android device
CSCus06920	Preauth bit set in RSN IE when WLAN is wpa2AES
CSCvc65568	Cisco Wireless IP Phone 8821 fails 802.11r FT roam with 'Invalid FTIE MIC'

Resolved Caveats

Use the BST to view the details of a caveat listed in this section. For more information about the BST, see the "Cisco Bug Search Tool" section on page 27.

Table 10 Resolved Caveats

ID	Headline
CSCuq63783	Second AP radio will not be up with third-party switch
CSCub75472	Rogue AP detection on wire fails if radio MAC is 1 of Ethernet MAC (AP1130/AP1240)
CSCug34802	Rogue detector AP fails to correlate and contain wired rogues on 5 GHz (AP1130/AP1240)
CSCup43052	WLC crashes after starting client roaming
CSCup46986	The first DHCP client needs to be kicked off after detected duplicate IP
CSCup47579	AP Core Dump check box disabled (GUI); AP mode change from Flex to Local
CSCup55898	IPv6 DTLS negotiation failure in Local and FlexConnect modes
CSCup59877	%DOT11-2-NO_CHAN_AVAIL_CTRL: Interface Dot11Radio2 no channel available
CSCup66509	#OSAPI-0-INVALID_TIMER_HANDLE: [SA] timerlib_mempool (TRCBK)
CSCup84060	Radio interface down with rcore on 1130 and 1240 APs
CSCup92277	Controller responds to SYN-FIN scans
CSCup94796	QoS bandwidth contracts not cleared with fast-ssid-switching
CSCup96353	HA enabled Controller crash Task: NFV9_Task
CSCuq04522	OEAP access points lose config after power cycle
CSCuq14453	Memory leak on WLC when using PMIPv6 clients
CSCuq18402	Slave AP not connecting over daisy chain
CSCuq27304	Apple iOS7 devices not able to pass traffic in 11v+FTDot1x WLAN
CSCuq33165	Loss of jumbo state config on upgrade from 7.6 to 8.0
CSCuq34493	Unable to queue 802.11a AP PLM message
CSCuq40682	Optimized Roaming does not work
CSCuq41792	802.11ac: iPhone6/Samsung 802.11ac clients deauthe'd on 802.11r roam reassoc request
CSCuq42751	WLC not sending all the Client attributes to PI
CSCuq49638	Pre-auth Flex-ACL cannot be applied on AP when AP joined the WLC

Table 10 Resolved Caveats (continued)

ID	Headline
CSCuq50181	OpenSSL issues August 2014 - WLC
CSCuq55372	8.0 - WLC crash with Flex AP and Local Switching Enabled
CSCuq57637	15.3(3)JA AP IOS crash loop with Release image validation failure
CSCuq61451	Wrong cert while accessing WLC by IPv6 address and HTTPS
CSCuq61753	Lobby admin broken on 8.0.100.0 on WLC 2500
CSCuq61876	%DOT11-2-NO_CHAN_AVAIL_CTRL: Interface Dot11Radio2 no channel available
CSCuq73119	Need knob to suppress all RADIUS Interim Acct Updates per WLAN
CSCuq73468	RADIUS AP users not synchronizes after standalone-Connected transition
CSCuq79572	8.0.100.1- 5500 crashing continuously -ipv6socetTask
CSCuq81885	DHCP fails FlexConnect Local Switching MAC Filtering RADIUS VLAN assign
CSCuq82202	WLC hung - No free Mbufs (ARP Fllod) available
CSCuq86750	NDP packets on 3700 abnormally low TX power
CSCuq89707	IOS AP OpenSSL August 2014 vulnerabilities
CSCuq89956	AP in local mode 1550 crashes on show mesh forwarding port-state
CSCuq90997	PMIPv6 crash WLC 7.6 Reaper Reset: PMIPV6_Thread taking too much cpu
CSCuq92650	WLC memory leak on 7.6 post PIMPV6 implementation
CSCuq94967	WLC: iPhone 6 displays as an Nortel-Phone for Device-Type
CSCuq96360	702W: LED not working for the LAN ports in autonomous mode
CSCuq97267	Anchor clients not able to see custom webauth page; SSL to WLC GUI fails
CSCur00985	Local Policy created from GUI gives an error if the day is Sunday
CSCur09386	FlexConnect VLAN mode changed to Disabled after power cycle (AP1242/AP1131)
CSCur12358	AP1532 channel announce on DFS not working
CSCur13703	Central Webauth with HTTPS redirect fails
CSCur15784	Flex-Bridge fails to maintain MAP & client connectivity
CSCur16761	Outdoor APs going to Local mode with clear capwap privateconfig command
CSCur21198	Coverage hole detection not working as expected
CSCur21984	Memory Usage Increasing on Bonjour Services While Running 8.0.100.0
CSCur23139	vWLC: Client cannot access network after reconnect
CSCur27399	AP702W LAN port wired client traffic gets disturbed
CSCur27551	SSLv3 Poodle attack against HTTPS in WLC CVE-2014??-3566
CSCur42201	Crash on WLC apf_rogue_rule.c:2415
CSCur43050	APs mfg in September/October 2014 unable to join an AireOS controller
CSCur44620	Radio reset after Flex+Bridge AP recovers from standalone
CSCur46621	OEAP600:radCfg config get lost after upgrade due to CSCuq04522
CSCur48600	AP1530 crashes after radio failure
CSCur56103	WiSM2 Active Silent crash

Table 10 Resolved Caveats (continued)

ID	Headline
CSCur88408	LAP does not send discovery request to WLC IP discovered by DNS resolution
CSCur97205	AP1242: AP can not be converted from Mesh Mode to Local Mode
CSCuq97965	WLC crash with AVC enabled

Installation Notes

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

Warnings

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

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

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

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

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

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

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

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

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

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

Safety Information

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

FCC Safety Compliance Statement

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

Safety Precautions

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

1. If you are installing an antenna for the first time, for your own safety as well as others, seek professional assistance. Your Cisco sales representative can explain which mounting method to use for the size and type of antenna you are about to install.
2. Select your installation site with safety as well as performance in mind. Electric power lines and phone lines look alike. For your safety, assume that any overhead line can kill you.
3. Call your electric power company. Tell them your plans and ask them to come look at your proposed installation. This is a small inconvenience considering your life is at stake.
4. Plan your installation carefully and completely before you begin. Successfully raising a mast or tower is largely a matter of coordination. Each person should be assigned to a specific task and should know what to do and when to do it. One person should be in charge of the operation to issue instructions and watch for signs of trouble.

5. When installing an antenna, remember:
   a. Do not use a metal ladder.
   b. Do not work on a wet or windy day.
   c. Do dress properly—shoes with rubber soles and heels, rubber gloves, long-sleeved shirt or jacket.
6. If the assembly starts to drop, get away from it and let it fall. Remember that the antenna, mast, cable, and metal guy wires are all excellent conductors of electrical current. Even the slightest touch of any of these parts to a power line completes an electrical path through the antenna and the installer: **you!**
7. If any part of an antenna system should come in contact with a power line, do not touch it or try to remove it yourself. Call your local power company. They will remove it safely.
8. If an accident should occur with the power lines, call for qualified emergency help immediately.

Installation Instructions

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

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

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

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

Service and Support

Troubleshooting

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

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

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

Related Documentation

For more information about the Cisco WLCs, lightweight access points, and mesh access points, see these documents:

- The quick start guide or installation guide for your particular Cisco WLC or access point

- *Cisco Wireless 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.