Release Notes for Cisco Wireless Controllers and Lightweight Access Points, Cisco Wireless Releases 8.0.120.0 and 8.0.121.0

First Published: October 26, 2015

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 Controllers are referred to as *Cisco WLCs*, and all Cisco lightweight access points are referred to as *access points* or *Cisco APs*.

Revision History

Table 1 Revision History

Modification Date	Modification Details
November 10, 2017	• Open Caveats, page 24 – Added CSCvc65568
October 10, 2017	• Features Not Supported on Cisco Virtual WLCs, page 22 – Added Wired Guest and FlexConnect central switching.
August 19, 2016	• Guidelines and Limitations, page 9 – Added information about CSCva84464.
February 17, 2016	• What's New in Release 8.0.121.0, page 3 – Added information about CSCuw06153 • Resolved Caveats, page 30 – Added a note about CSCuw06153 in the Resolved Caveats list

Cisco Wireless Controller and Access Point Platforms

The section contains the following subsections:

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

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

Supported Cisco Wireless Controller Platforms

The following Cisco WLC platforms are supported in this release:

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

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

Supported Access Point Platforms

The following access point platforms are supported in this release:

- Cisco Aironet 1040, 1130, 1140, 1240, 1250, 1260, 1600, 1700, 2600, 2700, 3500, 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, and Industrial Wireless 3700 Series outdoor and industrial wireless access points

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

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 8.0.12x.0, you must upgrade the software in the Next Generation Cisco 880 Series ISRs to Cisco IOS 15.1(4)M or later releases.

Unsupported Cisco Wireless Controller Platforms

The following Cisco WLC platforms are not supported:

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

What's New in Release 8.0.121.0

The Cisco Wireless Release 8.0.121.0 is a respost of the Cisco Wireless Release 8.0.120.0 to address CSCuu82607 and CSCuw06153. There are no other updates in this release.

What's New in Release 8.0.120.0

- The Cisco Industrial Wireless 3702 (IW3702) Series access points are IP67 rated and suitable for outdoor use cases such as trackside and on-board rail, mining, intelligent transportation systems, and City Wi-Fi applications. These access points are IEEE 802.11a/b/g/n/ac compliant with external antennas and designed to withstand extremes in temperature, vibration, and shock common in industrial environments. For more information, see www.cisco.com/go/iw3702-docs.
- Cisco Lightweight Access Points that were manufactured over 10 years ago may fail to create a CAPWAP or LWAPP connection due to certificate expiration. You may allow the Access Points with Manufactured Installed Certificates (MICs) or Self-signed Certificates (SSCs) beyond their expiration date to associate with Cisco WLC.

  On Cisco WLCs, the AP lifetime-check parameter is enabled by default. After upgrading, we recommend that you configure the Cisco WLC to ignore the expiration date on the APs' MICs and SSCs by entering this command:

  ```
  (Cisco Controller) >config ap cert-expiry-ignore {mic | ssc} enable
  ```

When the **config ap cert-expiry-ignore** {**mic** | **ssc**} **enable** command is entered, Cisco WLC ignores the expiration date on the APs' MICs or SSCs, allowing APs or Cisco WLCs with certificates that are more than 10 years old to connect with each other. The AP lifetime-check parameter must remain enabled as long as APs with expired MICs or SSCs are managed by this Cisco WLC.

You can see the configuration state by entering this command:

```
(Cisco Controller) >show certificate summary

    Web Administration Certificate.................. 3rd Party
    Web Authentication Certificate.................. Locally Generated
    Certificate compatibility mode:................. off
    Lifetime Check for MIC ......................... Enable
    Lifetime Check for SSC ......................... Enable
```

For more information, see http://www.cisco.com/c/en/us/support/docs/field-notices/639/fn63942.html.

- For other updates in this release, see the "Caveats" section on page 24.

Note For an overview of features/enhancements introduced in Release 8.0.x, see http://www.cisco.com/c/en/us/support/wireless/wireless-lan-controller-software/products-release-notes-list.html.

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

Table 2 Software Support for Access Points (continued)

Access Points		First Support	Last Support
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	—
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	—

Table 2 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	—
2700 Series	AIR-CAP2702I-x-K9	7.6.120.0	—
	AIR-CAP2702I-xK910	7.6.120.0	—
	AIR-CAP2702E-x-K9	7.6.120.0	—
	AIR-CAP2702E-xK910	7.6.120.0	—
	AIR-AP2702I-UXK9	8.0.110.0	—
3500 Series	AIR-CAP3501E	7.0.98.0	—
	AIR-CAP3501I	7.0.98.0	—
	AIR-CAP3502E	7.0.98.0	—
	AIR-CAP3502I	7.0.98.0	—
	AIR-CAP3502P	7.0.116.0	—
3600 Series	AIR-CAP3602I-x-K9	7.1.91.0	—
	AIR-CAP3602I-xK910	7.1.91.0	—
	AIR-CAP3602E-x-K9	7.1.91.0	—
	AIR-CAP3602E-xK910	7.1.91.0	—
	USC5101-AI-AIR-K9	7.6	
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	—
IW3700	IW3702-2E-UXK9	8.0.120.0	—
	IW3702-4E-UXK9	8.0.120.0	—

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

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

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

Software Release Types and Recommendations

This section contains the following topics:

- Types of Releases, page 8
- Software Release Recommendations, page 9

Types of Releases

Table 3 Types of Releases

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

1. AssureWave is a Cisco program that focuses on satisfying customer quality requirements in key industry segments in the mobility space. This program links and expands on product testing conducted within development engineering, regression testing, and system test groups within Cisco. The AssureWave program has established partnerships with major device and application vendors to help ensure broader interoperability with our new release. The AssureWave certification marks the successful completion of extensive wireless controller and access point testing in real-world use cases with a variety of mobile client devices applicable in a specific industry.

Software Release Recommendations

Table 4 Software Release Recommendations

Type of Release	Deployed Release	Recommended Release
Maintenance Deployment (MD) release	7.0 MD release train (latest 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

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 8.0.12x.0

Guidelines and Limitations

- When you change the WLAN profile name, then FlexConnect APs (using AP-specific VLAN mapping) will become WLAN-specific. If FlexConnect Groups are properly configured, the VLAN mapping will become Group-specific.
- 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 or later, even though Release 7.6 supports new mobility. This issue occurs when new mobility, which is compatible with the Cisco 5760 Wireless Controller and the Cisco Catalyst 3850 Series Switch, are in use. However, old mobility is not affected.

  The workaround is as follows:

  a. Enter the following commands:

```
config boot backup
show boot

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

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

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

```
config boot primary
```

Note 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 8.0.12x.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 8.0.12x.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 8.0.12x.0.
- We recommend that you install Release 1.9.0.0 of Cisco Wireless Controller Field Upgrade Software (FUS), which is a special AES package that contains several system-related component upgrades. These include the bootloader, field recovery image, and FPGA/MCU firmware. Installing the FUS image requires special attention because it installs some critical firmware. The FUS image is independent of the runtime image. For more information, see http://www.cisco.com/c/en/us/td/docs/wireless/controller/release/notes/fus_rn_OL-31390-01.html

Note The FUS image installation process reboots the Cisco WLC several times and reboots the runtime image. The entire process takes approximately 30 minutes. We recommend that you install the FUS image in a planned outage window.

Note If you are using a Cisco 2500 Series controller and you intend to use the Application Visibility and Control (AVC) and NetFlow protocol features, you must install Release 1.9.0.0 of Cisco Wireless Controller Field Upgrade Software (FUS). This is not required if you are using other controller hardware models.

- 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 8.0.12x.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 8.0.12x.0. Table 5 shows the upgrade path that you must follow before downloading Release 8.0.12x.0.

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

Table 5 Upgrade Path to Cisco WLC Software Release 8.0.12x.0

Current Software Release	Upgrade Path to 8.0.12x.0 Software
7.4.x releases	You can upgrade directly to 8.0.12x.0.
7.6.x releases	You can upgrade directly to 8.0.12x.0.
8.0.100.0 8.0.110.0	You can upgrade directly to 8.0.12x.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.

- 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 8.0.12x.0. Some TFTP servers that support files of this size are tftpd32and the TFTP server within the Prime Infrastructure. If you attempt to download the 8.0.12x.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 Controller FlexConnect Configuration Guide*.

Note Predownloading Release 8.0.12x.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 8.0.12x.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 8.0.12x.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 8.0.12x.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 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 8.0.12x.0 Cisco WLC software is installed on your Cisco WLC, click **Monitor** on the Cisco WLC GUI and view the Software Version field under Controller Summary.

Special Notes for Licensed Data Payload Encryption on Cisco Wireless Controllers

Datagram Transport Layer Security (DTLS) is required for all Cisco 600 Series OfficeExtend Access Point deployments to encrypt data plane traffic between the APs and the Cisco WLC. You can purchase Cisco Wireless Controllers with either DTLS that is enabled (non-LDPE) or disabled (LDPE). If DTLS is disabled, you must install a DTLS license to enable DTLS encryption. The DTLS license is available for download on Cisco.com.

Important Note for Customers in Russia

If you plan to install a Cisco Wireless Controller in Russia, you must get a Paper PAK, and not download the license from Cisco.com. The DTLS Paper PAK license is for customers who purchase a Cisco WLC with DTLS that is disabled due to import restrictions, but have authorization from local regulators to add DTLS support after the initial purchase. Refer to your local government regulations to ensure that DTLS encryption is permitted.

Note Paper PAKs and electronic licenses that are available are outlined in the respective Cisco WLC platform data sheets.

Downloading and Installing a DTLS License for an LDPE Cisco WLC

Step 1 Download the Cisco DTLS license.

a. Go to the Cisco 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 8.0.12x.0" section on page 9.

Interoperability With Other Clients in Release 8.0.12x.0

This section describes the interoperability of Release 8.0.12x.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	8.0.12x.0
Cisco WLC	Cisco 5500 Series Controller

Table 6 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 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 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 7 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 7 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 Access Point Platforms

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

Features Not Supported on 1130 and 1240 APs

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

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

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

- PPPoE
- PMIPv6

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

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

Features Not Supported on Mesh Networks

- Multi-country support
- Load-based CAC (mesh networks support only bandwidth-based CAC or static CAC)
- High availability (fast heartbeat and primary discovery join timer)
- AP acting as supplicant with EAP-FASTv1 and 802.1X authentication
- Access point join priority (mesh access points have a fixed priority)

- Location-based services

Caveats

Cisco Bug Search Tool

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/search
2. Enter the bug ID in the **Search For:** field.

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

Open Caveats

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

Bug ID	Headline
CSCuh20715	Cisco 5508 WLC running 7.3.101.0 release unexpectedly reloads on Reaper Reset: Task LDAP DB Task 2
CSCui57047	Cisco WLC stopped working while executing the SXP SOCK task
CSCuj60872	Cisco WLC reloads unexpectedly due to reaper reset for apfMsConnTask_6
CSCuj93777	Mesh AP should block data packets and then handle the BPDU packets
CSCul40203	Interface is not marked as dirty because of dual stack clients
CSCul94524	On a WLAN running on 7.4 release, web authentication, FlexConnect Local Switching, and Anchor functions are affected
CSCum25947	PPPoE configurations are still retained after a write erase on the Cisco AP
CSCum86031	Roaming Cisco 5508 WLC to Cisco 5760 WLC applies wrong QoS policy on configuring AAA-override
CSCun20584	Cisco AP replicates broadcast packets to the default gateway
CSCun34295	Cisco WiSM2 unexpectedly reloads on radiusTransportThread task

Bug ID	Headline
CSCun59052	Page error occurs after applying configuration on the VLAN mapping page
CSCun96815	After upload or download of the configuration, the Cisco OEAP ACLs and network lists are deleted
CSCuo05142	The EAP-AKA client is unable to reauthenticate using fast reauthentication ID and multiple authentication servers
CSCuo19677	Cisco WLC does not update the AP with the new bandwidth setting
CSCuo43002	Enabling IP Protocol 119 from GUI does not display on show-run
CSCuo48442	Stale DTLS data_encryption sessions history are left on the Cisco WLC
CSCuo70310	Flex+Bridge with PPPoE mode AP does not associate with the Cisco WLC
CSCuo96366	Cisco WLC sends RADIUS packets with the same ID without doing the RADIUS ID check
CSCup00196	Local authentication EAP-FAST not working for Cisco FlexConnect AP authentication users on Cisco AP1240
CSCup02792	CLI configuration issues regarding enabling or disabling of rogue traps
CSCup29095	Mesh—PI does not show the neighbor details in the Parent's mesh links page
CSCup31640	Changing channel to Auto does not set the maximum bandwidth for FlexConnect APs
CSCup46302	In Cisco vWLC, the RSSI is missing from the Monitor mode AP
CSCup57457	WS-SVC-WISM2-K9 is unable to change Rogue state
CSCup60282	The Cisco WLC generated ping is seen as an incorrect type of ICMP ping
CSCup64468	Cisco WLC device sends invalid format '#' in front of syslog message
CSCup68372	When the session times out, the statistics are carried over
CSCup71136	MAC delimiter does not change in the accounting message
CSCup72165	Cisco 1522 AP unable to join 801.11ac parent; DHCP ACK sent as WEP
CSCup72502	Cisco 5508 WLC running 7.6 release does not deauthenticate client when FlexConnect ACL is not present on AP
CSCup75446	Default interface takes precedence over foreign VLAN mapping with CWA
CSCup77631	IPv6 queue is full and messages are continuously logged
CSCup80403	In low iMac throughput, the supported IE rate in association response has zero length
CSCup81511	Incorrect WMM UP to DSCP markings on Cisco AP1131 and Cisco AP1242
CSCup85896	Interference profile fails on secondary40 channel
CSCup86941	Cisco WLC GUI—Policy type for 'Static WEP' clients shows as N/A
CSCup88910	630937505—Cisco AP impersonation flood of events on Cisco WLC 8510-SR14-00512
CSCup92480	802.11ac unexpectedly reloads due to PCI reset
CSCup96492	IPv6 route with /128 prefix removes after reboot
CSCup97263	Cisco Flex 7510 WLC—Dot1x_NW_MsgTask_2 System reloads
CSCup98731	The HTTPS-redirect command is missing in the uploaded config file

Bug ID	Headline
CSCuq05410	Cisco vWLC/SRE—Boot option 3 to Change active boot image is not working
CSCuq08623	Cisco WLC unexpectedly reloads due to double free in cdpFreeCacheTable()
CSCuq14231	Cisco Flex 7510 WLC—Efficient upgrade IPv6: subordinates cannot download the new image
CSCuq20950	AVC profile not able to block the BitTorrent traffic
CSCuq27359	Flash write process is not getting completed even after many hours
CSCuq28038	Hop2—multiple attempts are made in very-fast convergence to rejoin Cisco WLC
CSCuq28973	Cisco 8510 WLC unexpectedly reloads on 'IPv6_Msg_Task' task
CSCuq32731	Cisco 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
CSCuq45110	M1 is sometimes encrypted leading to M1 refusal on station side
CSCuq50069	SHA1 key cipher is not working between Cisco WLC 8.0 and Cisco MSE 8.0 releases
CSCuq56669	Cisco WLC SSID is not backing up properly in config file
CSCuq56829	Flex+Bridge MAPs drop after association; failed to receive data keep-alive packets
CSCuq59501	Show tech not showing **show run-config** command's output
CSCuq68753	Cisco 5508 anchor WLC running Release 7.6.x.x unexpectedly reloads on 'osapiBsnTimer' task
CSCuq71068	Cisco AP traffic issue causes client to lose Layer 3 connectivity
CSCuq72285	Unable to insert line break in the Internal Web-Authentication message window
CSCuq73072	Mesh Convergence list includes incorrect channel
CSCuq73590	Cisco WLC adds incorrect class attribute in accounting stop
CSCuq79645	Cisco IOS-XE Release 3.7: Catalyst 3650 Switch to Cisco 5508 WLC mobility tunnel takes more than 1 hour to come up
CSCuq86263	DFS on Cisco AP1600
CSCuq86274	Cisco AP1530 DFS detection across all channels
CSCuq88748	Rogue APs wrongly classified as unclassified instead of malicious
CSCuq91181	Client does not regain IP connectivity after roaming
CSCuq94678	Cisco WiSM2 not responding to ARP requests
CSCuq96986	Cisco 2504 WLC unexpectedly reloads after upgrading to 8.0 release
CSCur02514	Cisco WLC 8.0.100.0—SNMP trap is not sent out on HA switchover
CSCur07086	Cisco AP1142 Config loss after cold reboot
CSCur10713	Cisco WLC returns a null value using SNMP for memory usage
CSCur11060	False positive on honeypot alert with multiple SSIDs
CSCur13400	DHCP Option 82 and Sub Option 5 issue in Cisco WLC 8.0
CSCur19331	Clients cannot complete DHCP and are deauthenticated from Cisco vWLC
CSCur19519	MAP stuck on 802.1x after error condition and roaming

Bug ID	Headline
CSCur23915	Cisco WLC Reaper Reset during AP image predownload
CSCur24512	Cisco AP 3602i unexpectedly reloads at dot11_driver_ie_find task
CSCur25239	Cisco WLC unexpectedly reloads on mping command over Telnet/SSH
CSCur31693	Cisco AP1570: 9-Mbps Link Test fails; 100 percent packet loss
CSCur32475	New Mobility Web authentication—MAC Filter failure always sends client to web authentication
CSCur33320	SC1/SC2/SC3 radio reset with FW stuck in macenb (Cont. of CSCuo27106)
CSCur38682	AP FlexConnect—Local switch/local authentication sends deauthentication 802.1x on PSK WLAN
CSCur42476	Cisco 8510/7510 WLC—SNMP IP Address configs reversed on downgrade from 7.6 to 7.4 release
CSCur43124	WSSI module stops working after upgrade from 7.4.121.0 to 7.6.130.0 release
CSCur46376	Cisco Flex 7510 WLC unexpectedly reloads with task “webauthredirect”
CSCur46884	Bouncing power to Cisco WiSM2 causes second 10-GHz link to stop forwarding data
CSCur47745	Client unable to join WLAN with FlexConnect Central DHCP processing
CSCur48612	Cisco WLC running 8.1 release emWeb unexpectedly reloads when adding devices to mDNS policy
CSCur48944	Problem in Client Stats Reports and Optimized Roaming
CSCur49165	Cisco WiSM2 system unexpectedly reloads on radiusTransportThread aaaRadiusAuth
CSCur54332	Failed to parse RADIUS AVP XML file in standby Cisco WLC
CSCur54681	Cisco WLC GUI: Flex+Bridge Parent inherited FlexConnect VLAN mappings are not reflected on MAP
CSCur63456	Delay on Apple iOS devices to show connection
CSCur66836	FlexConnect AP occasionally sends a RADIUS request with no username
CSCur71315	Cisco AP1552 bridge Transmit voice queue stuck leading to out of Tx buffers
CSCur74208	Name/OID: cLMobilityExtMgrAddress.0; Returning in IP in Reverse Order
CSCur80841	Apple remote app not working with snooping enabled mDNS
CSCur80935	8.0.100.0—AAA overridden ACL is not applied on Guest access Cisco WLC
CSCur88307	AP name unknown in dissociation messages (Intermittent)
CSCur89551	LWAPP-3-INVALID_AID: message observed for Cisco 1240 APs in FlexConnect mode
CSCur90555	Cisco WLC 8.0 keeps ghost client entry
CSCur91936	mDNS discovery issue with Cisco WLC 8.0.100
CSCur93964	PMIPv6 web-authenticated client is not able to get past authentication
CSCur95365	Cisco WLC unexpectedly reloads when the **show ap config general** command is entered.
CSCus02070	FlexConnect AP losing VLAN mapping and falling on native VLAN
CSCus03406	Cisco 8510 WLC running 7.6 release unexpectedly reloads on Data plane

Bug ID	Headline
CSCus03487	Cisco AP3700 sends wrong TLV during power level negotiation
CSCus04169	AID leak on 8.0.100.0 FlexConnect local switching scene
CSCus07013	Adding MAC filter check when client is changing SSID for web authentication
CSCus20868	Cisco WLC ignoring SNMP requests on ports 12225, 5246, or 5247
CSCus20991	Radius NAC Client authentication issues for 7.6.130.0 release
CSCus30429	Cisco 600 OEAP not giving IP address on remote LAN port in 8.0 release
CSCus33759	Local Policies not working after OUI Update
CSCus39396	Release 8.0.100.0—QoS Bronze Profile not marking traffic to AF11 on FlexConnect
CSCus50199	Default route to BVI is present on Central DHCP NAT FlexConnect scenario
CSCus56713	Cisco 5508 WLC HA: Frequent Switchovers with Release 8.0.110.0
CSCus61445	DNS ACL on Cisco WLC does not work; AP does not send DTLS to Cisco WLC
CSCus61679	Problem in Client Stats Reports —Follow up CDETS
CSCus64550	Mobility client IP Address as 0.0.0.0 in foreign Cisco WLC
CSCus68363	Rogue Policies are not applied correctly
CSCus73932	Multicast configuration issue on Cisco 8510 WLC running 8.0.110.x release
CSCus74299	New mobility: Client not deleted on Cisco 5508 WLC when it roams at webauthentication state
CSCus79046	CAPWAP AP does NOT fallback to IPv6 if ACL blocks IPv4 CAPWAP packets
CSCus79056	Cisco 5508 WLC —management frames are not marked with CS6
CSCus81385	msglog flooded with validation of SPAM_VENDOR_SPECIFIC_PAYLOAD(185)
CSCus83638	[BZ1043] 3702 AP 5 -GHz radio beaconing but not accepting any client association
CSCus85455	First client association does not create NVI int on central DHCP FlexConnect mode
CSCus89468	Need to add Cisco 802 AP to the list of APs that support Flex+Bridge mode
CSCus90178	Cisco AIR-OEAP602I has TCP port 5162 open
CSCus91214	”AP802 15.3(3)JAB unexpectedly reloads on issuing “”dir all-filesystems”” ISR C881W”
CSCus92667	GET on AP groups Table after set - response missing
CSCus97953	WLC 8510 silently reloads; NMI received for unknown reason 2d
CSCut02524	Default NAS-ID value at the AP-Groups should be empty or none
CSCut04924	Long delay between frame retransmissions on 1532; packet drops
CSCut06502	WLC unexpectedly reloads due to RRM-CLNT-5_0 task
CSCut09821	Unused Data DTLS session is remained on WLC running 7.6.130.x release
CSCut11821	WLC: ad-hoc containment does not stop
CSCut14459	Session ID changes for an intercontroller client roam using EAPFAST
CSCut16170	Mobility tunnel down after switchover to 7.6 release

Bug ID	Headline
CSCut22092	Client Disassociated due to inactivity ReasonCode: 4
CSCut24276	Unexpected PMKID count field in beacon’s RSN IE
CSCut39118	Cisco WLC 8510 failure to collect feature MobilityExtGroupMember on PI 2.2
CSCut42926	Cisco WLC unexpectedly reloads on SNMP task after doing config audit from PI
CSCut46811	Cisco 3702 AP not accepting clients on 5 GHz when WIPs Submode enabled
CSCut48172	LSC AP provisioning happening after MAP is disconnected for a long time
CSCut57957	1602 APs in FlexConnect mode do not maintain VLAN 1 configuration after reload
CSCut62319	Broadcast Key Rotation won’t occur after MAC Filtering enabled
CSCut70403	Cisco WiSM2 unexpectedly reloads on ‘HAConfigSyncTask’ task
CSCut74263	MAG on AP:AP does not clear bindings after session/user timeout & deauthentication
CSCut76481	Cisco WLC sends 1499 bytes MTU switchover
CSCut87326	Cisco WLC generates SNMP traps to PI 2.2 for AIR-3702 PoE+ getting low power
CSCut91086	Client associated to MAP doesn’t get AAA override in Flex+Bridge mode
CSCut97683	WLC unexpectedly reloads on spamApTask2 in 8.0.110.0 release
CSCut98006	DFS detections due to high energy profile signature
CSCut99150	Cisco 2702 AP requesting as a Type 1 power device instead of Type 2
CSCuu04464	License command causes WLC to unexpectedly reload (possible buffer size overwrite)
CSCuu12944	Increase WPA handshake timeout for FlexConnect local authentication
CSCuu15866	Unexpected Local EAP authentication termination.
CSCuu36176	If the PoE+ input is used as the power source, the lowest supported operating temperature on Cisco IW3702 will be –20°C (–4°F)
CSCuu42378	Rx-SOP threshold not working correctly
CSCuu44155	RAP takes 15 minutes to use wired connection if there are wireless peers available
CSCuu49291	7925 decrypt errors with Cisco AP 1131 running 8.0 release
CSCuu68490	Duplicate RADIUS-Accounting update message sent while roaming
CSCuu81792	Cisco AP1242 Ethernet Bridging does not pass VLANs other than the native VLANs
CSCuu98792	Cisco AP1570 antenna enable config is lost on reboot
CSCuu99222	Cisco AP 1530 MAP mode radio restarts due Tx in progress
CSCuu99344	Cisco WLC unexpectedly reloads—DHCP packet content while on new mobility
CSCuw91763	The AES Key Wrap feature does not work.
CSCvc65568	Cisco Wireless IP Phone 8821 fails 802.11r FT roam with 'Invalid FTIE MIC'

Resolved Caveats

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

Table 8 Resolved Caveats

Bug ID	Headline
CSCuu82607	Evaluation of all for OpenSSL June 2015 **Note** This bug is fixed in the 8.0.121.0 release.
CSCut83556	Reaper Reset Locked by apfReceiveTask
CSCuu37077	Cisco 3600AP limited channels/power similar to CSCus35411
CSCuu20683	RAP might lose the Native VLAN configuration on downgrade from 8.1 release
CSCuu20256	Traffic drop on Cisco WLCs with 7.6.130.x release and PMIPv6
CSCut05252	Cisco OEAP: Authentication rejected because of challenge failure Reason Code:15
CSCut47761	PMIPv6 Client stopped working with 802.1x authentication when user name have colon ':'
CSCun56310	#LWAPP-3-VENDOR_PLD_VALIDATE_ERR: SPAM_VENDOR_SPECIFIC_PAYLOAD(185)
CSCus44831	Cisco AP1702 reports power error with 802.3af power source
CSCus25256	Cisco AP1130 in FlexConnect mode sometimes lose bridge-group configuration
CSCuq97914	PI 1.4 cannot finish auditing Cisco WLC
CSCus26067	HA failing after upgrade to 8.0 release due to gateway ARP source mac
CSCus72994	Cisco WLC unexpectedly reloaded on Task Name: DHCP Socket Task
CSCus94968	osapiMalloc accepting negative size buffers
CSCut98741	Cisco WLC Monitor page needs to support session timeout
CSCut14210	Cisco FlexConnect arp-cache enabled—AP is not responding on behalf of client
CSCus30769	BSSID containing itself and also adding itself to client exclusion list.
CSCuq86269	DFS detection due to Broadcom spurious emissions
CSCus48787	AP: radio d1 reset: FW: vec=36 pc=10FC4 irq/mac stat=20000/80
CSCur53041	Datagram Transport Layer Security (DTLS) connection failure.
CSCus39358	Apple and Android not connecting to WPA2-AES on Cisco OEAP600 8.0.110
CSCus44802	WLAN NAS-id is not applied when AP Group NAS-id is changed
CSCus06920	Pre-authentication bit set in RSN IE when WLAN is WPA2-AES
CSCut96026	Security Group Tag (SGT) remains for client when moving between WLANs with Fast SSID change
CSCuq48218	Cisco WLC cannot process multiple sub-attributes in single RADIUS VSA
CSCur45862	APs cannot discover WLC through option 43 on 8.0.100 release
CSCuq09859	APs sending Generic Attribute Registration Protocol (GARP) and ARP requests approx every 2 seconds

Table 8 Resolved Caveats (continued)

Bug ID	Headline
CSCuq48800	Low throughput due to Unscheduled Automatic Power Save Delivery (UAPSD) for Intel 7260 Wi-Fi chipset
CSCuo09947	RADIUS AVP #44 (Acct-Session-ID) to be sent in RADIUS authentication messages
CSCuq48218	Cisco WLC cannot process multiple sub-attributes in single RADIUS VSA
CSCur45453	Cisco 8510 WLC GUI new mobility support and Switch Peer Group (SPG) configuration to be blocked
CSCur56576	Cisco WLC does not support 802.11a for Qatar
CSCur92472	PMIPv6: Roaming WLC1->WLC2 does not work, wrong handoff indicator
CSCus31292	Oct 2014 OpenSSL vulnerabilities
CSCus85767	Cisco FlexConnect local switch clients local DHCP are trying to do central DHCP
CSCut45950	MARCH 2015 OpenSSL Vulnerabilities
CSCus45806	Enable CDP Spare pair TLV for Cisco 1570 AP and Cisco 1530 AP series access points
CSCur22714	Cisco 3602 AP trying to contain its own RM3000AC module
CSCut26137	Cisco 3702 AP — Voice Queue stuck with no new clients able to associate
CSCur37475	Cisco WiSM2 system unexpectedly reloaded— client stats AVL corruption
CSCus13594	Slow in getting the DHCP address in the Cisco 2700 AP
CSCur78697	1st Hop MAP CAPWAP Restart Due to race condition when seeking RAP2
CSCur72287	EAPOL Security error seen when 1st HOP MAP Roams from RAP1 to RAP2
CSCus48452	MAPs do not return to configured channel along with RAP 30 after DFS
CSCus49126	Cisco 3702 AP floods RTS frames @ 8000pps to departed client
CSCuq99230	AP syslog fails due to default setting 'logging server-arp'
CSCus85337	CAPWAP Restart and Gateway not reachable when MAP roams From RAP1 to RAP2
CSCuq48043	IPv6 forwarding halts; broadcast queue full
CSCur52246	PMIPv6 GRE key database gets full during scale testing
CSCur71427	"FlexConnect: Client roaming fails" "not processing DOT1X_4WAY_COMPLETED_AT_AP"
CSCur74954	Central authentication + local switching: clients are in idle state always
CSCus80059	WLC always send authentication packet to aaa server even no any client in WLC
CSCut31679	Kernel panic—Unhandled kernel unaligned access
CSCuq60042	Memory leak on WLC when using PMIPv6 clients pem_api.c
CSCuq63642	Internal webpage appears after successful redirect to external web authentication
CSCur00288	8.0.100.0 client is shown with "ip address unknown" and "dhcp required" states
CSCur30298	Cisco 8510 WLC—New mobility support for guest anchor and block SPG config
CSCur50819	Browser Exploit Against SSL/TLS (BEAST) vulnerability not properly resolved in Cisco WLCs

Table 8 Resolved Caveats (continued)

Bug ID	Headline
CSCur67701	Cisco Flex 7510/ 8510 WLC—Image download errors for CAPWAP
CSCus39461	Radius DNS adds both Network and Management Authentication + Account = Enabled
CSCus46861	LIZARD attack: Denial of Service
CSCus64073	Cisco 1700/2700 APs native VLAN field missing in FlexConnect tab
CSCut07617	Signal 11 issue at PMIPV6_Thread_1
CSCut26403	Cisco AP1242 does not forward SIP INVITE when SIP-CAC is enabled
CSCus87673	Cisco AP3700 5-GHz radio reset
CSCur88864	Cisco 3600 APs with 802.11ac module shows 100 percentage Rx utilization on slot-2
CSCur23656	Cisco IOS and IOSd in IOS-XE: evaluation of SSLv3 POODLE vulnerability
CSCuq19142	Cisco AP/ Cisco WLC MIC lifetime expiration causes DTLS failure
CSCuq54548	Anchor Memory Leak when Sleeping Client Feature is enabled
CSCuq74491	Cisco WLC Release 8.0.100.0 unexpectedly reloads due to Task Name: apfRogueTask_0
CSCur20154	HA SSO pair memory leak
CSCur96221	Standby Cisco WLC unexpectedly reloads at haSSOServiceTask6
CSCus21276	Kernel panic on Cisco WiSM2
CSCus38268	Memory Leak on Cisco WiSM2 due to SNMPTask on 7.4.121.0 release
CSCus42727	JANUARY 2015 OpenSSL Vulnerabilities
CSCus55004	Cisco 2504 WLC on 8.0.110.0 release: Kernel panic with pre-authentication ACL and external web-redirect
CSCuw06153	Unauthorized configuration change for web management. **Note** This bug is fixed in Release 8.0.121.0

Installation Notes

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

Warnings

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

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

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

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

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

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

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

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

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

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

Safety Information

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

FCC Safety Compliance Statement

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

Safety Precautions

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

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

Installation Instructions

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

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

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

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

Service and Support

Troubleshooting

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

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

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

Related Documentation

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

- The quick start guide or installation guide for your particular Cisco WLC or access point
- *Cisco Wireless Controller Configuration Guide*
- *Cisco Wireless Controller Command Reference*
- *Cisco Wireless Controller System Message Guide*
- *Cisco Wireless Mesh Access Points, Design and Deployment Guide*

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

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.

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.