



Release Notes for Cisco Wireless Controllers and Cisco Lightweight Access Points, Cisco Wireless Releases 8.0.132.0, 8.0.133.0, and 8.0.135.0

First Published: April 02, 2016

This document describes what is new in 8.0.13x.0 release, instructions to upgrade to this release, and information about the open and resolved caveats for this release. Unless otherwise noted, all Cisco Wireless Controllers are referred to as *Cisco WLCs*, and all Cisco lightweight access points are referred to as *access points* or *Cisco APs*.



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

Revision History

Table 1 **Revision History**

Modification Date	Modification Details
November 10, 2017	<ul style="list-style-type: none"> • Open Caveats, page 27 <ul style="list-style-type: none"> – Added CSCvc65568
October 10, 2017	<ul style="list-style-type: none"> • Features Not Supported on Cisco Virtual WLCs, page 24 <ul style="list-style-type: none"> – Added Wired Guest and FlexConnect central switching.
August 19, 2016	<ul style="list-style-type: none"> • Guidelines and Limitations, page 12 <ul style="list-style-type: none"> – Added information about CSCva84464.
May 31, 2016	<ul style="list-style-type: none"> • What's New in Release 8.0.135.0, page 4 <ul style="list-style-type: none"> – Added what's new in this release • -B Domain Compliant Cisco APs in this Release, page 6 <ul style="list-style-type: none"> – Added Cisco 1570 AP V02 Series • Software Release Recommendations <ul style="list-style-type: none"> – Updated recommended releases • Resolved Caveats in Release 8.0.135.0 <ul style="list-style-type: none"> – Added CSCuz59734
May 09, 2016	<ul style="list-style-type: none"> • Added to Resolved caveats <ul style="list-style-type: none"> – CSCur58057
April 26, 2016	<ul style="list-style-type: none"> • Included Release 8.0.133.0 <ul style="list-style-type: none"> – Following bugs are resolved: CSCuv03937, CSCuz04212, CSCuz16883, CSCuz24121 • Under Release 8.0.132.0 <ul style="list-style-type: none"> – Resolved Caveat: CSCuu51713
April 19, 2016	<ul style="list-style-type: none"> • Open Caveats, page 27 <ul style="list-style-type: none"> – Added three bugs—CSCuz04212, CSCuz16883, CSCuz24121.
April 09, 2016	<ul style="list-style-type: none"> • Interoperability With Other Clients in Release 8.0.13x.0, page 19 <ul style="list-style-type: none"> – Added test bed and client list tables.
April 06, 2016	<ul style="list-style-type: none"> • Downloading and Installing a DTLS License for an LDPE Cisco WLC, page 18 <ul style="list-style-type: none"> – Updated the license URL.

Cisco Wireless Controller and Cisco AP Platforms

The section contains the following subsections:

- [Supported Cisco Wireless Controller Platforms, page 3](#)
- [Supported Access Point Platforms, page 3](#)

- [Unsupported Cisco Wireless Controller Platforms, page 4](#)

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 Access Point Platforms, page 25](#).

Supported Access Point Platforms

The following access point platforms are supported in this release:

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

For information about features that are not supported on some access point platforms, see [Features Not Supported on Access Point Platforms, page 25](#).

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

- AP860:
http://www.cisco.com/c/en/us/products/collateral/routers/800-series-routers/data_sheet_c78_461543.html
- AP880:
http://www.cisco.com/c/en/us/products/collateral/routers/887-integrated-services-router-isr/data_sheet_c78_459542.html
http://www.cisco.com/c/en/us/products/collateral/routers/800-series-routers/data_sheet_c78-613481.html
http://www.cisco.com/c/en/us/products/collateral/routers/880-3g-integrated-services-router-isr/data_sheet_c78_498096.html
http://www.cisco.com/c/en/us/products/collateral/routers/880g-integrated-services-router-isr/data_sheet_c78-682548.html

- AP890:
http://www.cisco.com/c/en/us/products/collateral/routers/800-series-routers/data_sheet_c78-519930.html
 Before you use a Cisco AP802 series lightweight access point with Cisco Wireless Release 8.0.13x.0, you must upgrade the software in the Cisco 880 Series ISRs to Cisco IOS 15.1(4)M or later releases.

Unsupported Cisco Wireless Controller Platforms

The following Cisco WLC platforms are not supported:

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

What's New in Release 8.0.135.0

- [Impact on Cisco Aironet 1570 Series Access Points with –B Regulatory Domain, page 4](#)
- [Resolved Caveats, page 5](#)

Impact on Cisco Aironet 1570 Series Access Points with –B Regulatory Domain

The Cisco Wireless Release 8.0.135.0 is a repost of the Cisco Wireless Release 8.0.132.0 and 8.0.133.0. This release impacts only the Cisco Aironet 1570 Series APs with -B regulatory domain and meet the following criteria:

1. The Cisco 1570 APs that are made available on or after June 2, 2016, for the USA region
2. The Cisco 1570 APs that are identified with version ID 02 (V02)

This release ensures that Cisco 1570 APs that are made available to customers in the USA are in compliance with the new FCC rules that come into effect on June 2, 2016. Therefore, for customers who meet the above criteria, we recommend that you upgrade to Release 8.0.135.0.

There are no other updates in this release.

Important Notes

- Customers who do not use Cisco 1570 APs and/or are not in the USA region are not required to upgrade to this release.
- Customers in the USA region with -B domain Cisco 1570 APs that were shipped before June 2, 2016, and identified by version ID 01 (V01) can continue to use Release 8.0.133.0.

- Support for version ID V02 (V02) in later Cisco Wireless releases will be announced at a later date; for more information, see Cisco Aironet 1570 Series AP product bulletin.

Resolved Caveats

Table 2 Resolved Caveats in Release 8.0.135.0

Bug ID	Headline
CSCuz59734	Proper support for Cisco Aironet 1572 AP –B domain: VID:02 FCC requirements

What's New in Release 8.0.133.0

The Cisco Wireless Release 8.0.133.0 is a repost of the Cisco Wireless Release 8.0.132.0 to address the resolved caveats listed in [Table 3](#). There are no other updates in this release.

Table 3 Resolved Caveats in Release 8.0.133.0

Bug ID	Headline
CSCur58057	Cisco Flex AP loses some WLANs after radio resets
CSCuv03937	Unexpected WLC reload with RLDP enabled
CSCuz04212	Single radio functionality issues
CSCuz16883	Address registration at a foreign subnet when subnet mask does not match the anchor
CSCuz24121	mDNS is disabled on Cisco 2500 WLC platform

What's New in Release 8.0.132.0

Support for –B Domain

The FCC (USA) rule making on 5 GHz released on April 1, 2014 (FCC 14-30 Report and Order) goes into effect for products that are sold or shipped on or after June 2, 2016. Cisco APs and Cisco WLCs will comply with the new rules by supporting the new regulatory domain (–B) for the US and will create new AP SKUs that are certified under the new rules. Examples of new rules include new 5-GHz band channels permitted for outdoor use, and transmission (Tx) power level increased to 1W for indoor, outdoor, and point-to-point transmissions.



Note

Cisco APs and Cisco WLCs that are in the –A domain category can continue to operate and even coexist with –B domain devices without any issues.

We recommend that you upgrade Cisco APs and Cisco WLCs to the appropriate software release that supports –B domain.

–B Domain Compliant Cisco APs in this Release

- AP803
- AP700i/w
- AP1570 (V02)
- AP1532i/e
- AP1552
 - H
 - SA
 - SD
 - WU
- AP1600i/e
- AP1700i
- AP2600i/e
- AP2700i/e
- AP3600i/e
- AP3700i/e
- AP3700p
- IW3702
- AP702i

–B Domain Compliant Cisco APs Prior to this Release

- AP1810 t/w
- AP1830
- AP1850i/e

Software Release Support for Access Points

[Table 4](#) 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 4 *Software Support for Access Points*

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

Table 4 Software Support for Access Points (continued)

Access Points		First Support	Last Support
1700 Series	AIR-CAP1702I-x-K9	8.0.100.0	—
	AIR-CAP1702I-xK910	8.0.100.0	—
AP801		5.1.151.0	8.0.x
AP802		7.0.98.0	—
AP802H		7.3.101.0	—
2600 Series	AIR-CAP2602I-x-K9	7.2.110.0	—
	AIR-CAP2602I-xK910	7.2.110.0	—
	AIR-SAP2602I-x-K9	7.2.110.0	—
	AIR-SAP2602I-x-K95	7.2.110.0	—
	AIR-CAP2602E-x-K9	7.2.110.0	—
	AIR-CAP2602E-xK910	7.2.110.0	—
	AIR-SAP2602E-x-K9	7.2.110.0	—
	AIR-SAP2602E-x-K95	7.2.110.0	—
2700 Series	AIR-CAP2702I-x-K9	7.6.120.0	—
	AIR-CAP2702I-xK910	7.6.120.0	—
	AIR-CAP2702E-x-K9	7.6.120.0	—
	AIR-CAP2702E-xK910	7.6.120.0	—
	AIR-AP2702I-U XK9	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.

Table 4 **Software Support for Access Points (continued)**

Access Points		First Support	Last Support
1500 Mesh Series	AIR-LAP-1505	3.1.59.24	4.2.207.54M
	AIR-LAP-1510	3.1.59.24	4.2.207.54M
1520 Mesh Series	AIR-LAP1522AG	-A and N: 4.1.190.1 or 5.2 or later ¹	—
		All other reg. domains: 4.1.191.24M or 5.2 or later ¹	—
	AIR-LAP1522HZ	-A and N: 4.1.190.1 or 5.2 or later ¹	—
		All other reg. domains: 4.1.191.24M or 5.2 or later ¹	—
	AIR-LAP1522PC	-A and N: 4.1.190.1 or 5.2 or later ¹	—
		All other reg. domains: 4.1.191.24M or 5.2 or later ¹	—
	AIR-LAP1522CM	7.0.116.0 or later.	—
	AIR-LAP1524SB	-A, C and N: 6.0 or later	—
		All other reg. domains: 7.0.116.0 or later.	—
	AIR-LAP1524PS	-A: 4.1.192.22M or 5.2 or later ¹	—
1530	AIR-CAP1532I-x-K9	7.6	—
	AIR-CAP1532E-x-K9	7.6	—

Table 4 Software Support for Access Points (continued)

Access Points		First Support	Last Support
1550	AIR-CAP1552C-x-K9	7.0.116.0	—
	AIR-CAP1552E-x-K9	7.0.116.0	—
	AIR-CAP1552H-x-K9	7.0.116.0	—
	AIR-CAP1552I-x-K9	7.0.116.0	—
	AIR-CAP1552EU-x-K9	7.3.101.0	—
	AIR-CAP1552CU-x-K9	7.3.101.0	—
	AIR-CAP1552WU-x-K9	8.0.100.0	—
1552S	AIR-CAP1552SA-x-K9	7.0.220.0	—
	AIR-CAP1552SD-x-K9	7.0.220.0	—
1570 version ID 01 (V01)	AIR-AP1572EAC-x-K9	8.0.110.0	—
	AIR-AP1572ICy ² -x-K9	8.0.110.0	—
	AIR-AP1572ECy-x-K9	8.0.110.0	—
1570 version ID 02 (V02) ³	AIR-AP1572EAC-B-K9	8.0.135.0	—
	AIR-AP1572EC1-B-K9	8.0.135.0	—
	AIR-AP1572EC2-B-K9	8.0.135.0	—
	AIR-AP1572IC1-B-K9	8.0.135.0	—
	AIR-AP1572IC2-B-K9	8.0.135.0	—
IW3700	IW3702-2E-UXX9	8.0.120.0	—
	IW3702-4E-UXX9	8.0.120.0	—

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



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

2. y—Country DOCSIS Compliance, see ordering guide for details.
3. Cisco 1570 V02 APs are supported on only specific Cisco Wireless Controller software releases. For more information, see [Cisco Wireless Solutions Software Compatibility Matrix](#).

Software Release Types and Recommendations

This section contains the following topics:

- [Types of Releases, page 11](#)
- [Software Release Recommendations, page 11](#)

Types of Releases

Table 5 *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 6 *Software Release Recommendations*

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

For detailed release recommendations, see the software release bulletin:

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

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

Upgrading to Cisco WLC Software Release 8.0.13x.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 WLC Release 7.3.112.0, which is configured for new mobility, might revert to old mobility after upgrading to Release 7.6 or later, even though Release 7.6 supports new mobility. This issue occurs when new mobility, which is compatible with the Cisco 5760 Wireless Controller and the Cisco Catalyst 3850 Series Switch, are in use. However, old mobility is not affected.

The workaround is as follows:

- a. Enter the following commands:

```
config boot backup
show boot

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

- b. After the reboot, press **Esc** on the console, and use the boot menu to select **Release 7.6**.
- c. After booting on Release 7.6, set back the primary boot, and save the configuration by entering the following command:

```
config boot primary
```



Note Mobility epings are not available when New Mobility is enabled.



Note If you downgrade from a Cisco WLC release that supports new mobility to a Cisco WLC release that does not support new mobility (for example, Release 7.6 to Release 7.3.x) and you download the 7.6 configuration file with new mobility in enabled state, the release that does not support new mobility will have the new mobility feature in enabled state.

- If you downgrade from Release 8.0.13x.0 to a 7.x release, the trap configuration is lost and must be reconfigured.
- If you have ACL configurations in the Cisco WLC and downgrade from a 7.4 or a later release to a 7.3 or an earlier release, you might experience XML errors on rebooting the Cisco WLC. However, these errors do not have any impact on any functionality or configurations.

- If you are upgrading from a 7.4.X or an earlier release to a later release, the Called Station ID type information is mapped to the RADIUS Accounting Called Station ID type; the RADIUS Authentication Called Station ID type, by default, is set to ap-macaddr-ssid. You can configure the RADIUS Authentication Called Station ID type information by using the **config radius auth callStationIdType** command.
- When FlexConnect access points (known as H-REAP access points in the 7.0.x releases) that are associated with a Cisco WLC that has all the 7.0.x software releases prior to Release 7.0.240.0 upgrade to Release 8.0.13x.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 8.0.13x.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/en/US/docs/wireless/controller/release/notes/fus_rn_OL-31390-01.html.



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



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



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

- On Cisco Flex 7500 Series WLCs, if FIPS is enabled, the reduced boot options are displayed only after a bootloader upgrade.



Note Bootloader upgrade is not required if FIPS is disabled.

- If you have to downgrade from one release to another, you might lose the configuration from your current release. The workaround is to reload the previous Cisco WLC configuration files saved on the backup server, or to reconfigure the Cisco WLC.
- It is not possible to directly upgrade to Release 8.0.13x.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 8.0.13x.0. [Table 7](#) shows the upgrade path that you must follow before downloading Release 8.0.13x.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 7 Upgrade Path to Cisco WLC Software Release 8.0.13x.0

Current Software Release	Upgrade Path to 8.0.13x.0 Software
7.4.x releases	You can upgrade directly to 8.0.13x.0.
7.6.x releases	You can upgrade directly to 8.0.13x.0.
8.0.1x.0	You can upgrade directly to 8.0.13x.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 to all access points.
- You can upgrade to a new release of the Cisco WLC software or downgrade to an earlier release even if Federal Information Processing Standard (FIPS) is enabled.
- When you upgrade to the latest software release, the software on the access points associated with the Cisco WLC is also automatically upgraded. When an access point is loading software, each of its LEDs blinks in succession.
- We recommend that you access the Cisco WLC GUI using Microsoft Internet Explorer 9 or a later version or Mozilla Firefox 17 or a later version.



Note

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

- Cisco WLCs support standard SNMP Management Information Base (MIB) files. MIBs can be downloaded from the Software Center on Cisco.com.
- The Cisco WLC software is factory installed on your Cisco WLC and is automatically downloaded to the access points after a release upgrade and whenever an access point joins a Cisco WLC. We recommend that you install the latest software version available for maximum operational benefit.
- Ensure that you have a TFTP, FTP, or SFTP server available for the software upgrade. Follow these guidelines when setting up a server:
 - Ensure that your TFTP server supports files that are larger than the size of Cisco WLC software Release 8.0.13x.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 8.0.13x.0 Cisco WLC software and your TFTP server does not support files of this size, the following error message appears:
 “TFTP failure while storing in flash.”
 - If you are upgrading through the distribution system network port, the TFTP or FTP server can be on any subnet because the distribution system port is routable.

- When you plug a Cisco WLC into an AC power source, the bootup script and power-on self test is run to initialize the system. During this time, press **Esc** to display the bootloader Boot Options menu. The menu options for the Cisco 5500 Series WLC differ from the menu options for the other Cisco WLC platforms.

Bootloader menu for Cisco 5500 Series WLC:

```

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

```

Bootloader menu for other Cisco WLC platforms:

```

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

```

Enter **1** to run the current software, enter **2** to run the previous software, enter **4** (on a 5500 series Cisco WLC), or enter **5** (on another Cisco WLC platform) to run the current software and set the Cisco WLC configuration to factory defaults. Do not choose the other options unless directed to do so.



Note See the Installation Guide or the Quick Start Guide pertaining to your Cisco WLC platform for more details on running the bootup script and power-on self test.

- The Cisco WLC bootloader stores a copy of the active primary image and the backup image. If the primary image becomes corrupted, you can use the bootloader to boot with the backup image.

With the backup image stored before rebooting, choose **Option 2: Run Backup Image** from the boot menu to boot from the backup image. Then, upgrade with a known working image and reboot the Cisco WLC.

- You can reduce the network downtime using the following options:
 - You can predownload the AP image.
 - For FlexConnect access points, use the FlexConnect AP upgrade feature to reduce traffic between the Cisco WLC and the AP (main site and the branch). For more information about the FlexConnect AP upgrade feature, see the *Cisco Wireless Controller FlexConnect Configuration Guide*.



Note Predownloading Release 8.0.13x.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 8.0.13x.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 8.0.13x.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 8.0.13x.0 Cisco WLC software:

- a. Click this URL to go to the Software Center:
<https://software.cisco.com/download/navigator.html>
- b. Choose **Wireless** from the center selection window.
- c. Click **Wireless LAN Controllers**.

The following options are available:

- Integrated Controllers and Controller Modules
 - Standalone Controllers
- d. Depending on your Cisco WLC platform, select one of these options.
 - e. Click the Cisco WLC model number or name.
The **Download Software** page is displayed.
 - f. Click a Cisco WLC software release number. The software releases are labeled as follows to help you determine which release to download:
 - **Early Deployment (ED)**—These software releases provide new features and new hardware platform support as well as bug fixes.
 - **Maintenance Deployment (MD)**—These software releases provide bug fixes and ongoing software maintenance.
 - **Deferred (DF)**—These software releases have been deferred. We recommend that you migrate to an upgraded release.
 - g. Click a software release number.
 - h. Click the filename (*filename.aes*).
 - i. Click **Download**.
 - j. Read the Cisco End User Software License Agreement and click **Agree**.
 - k. Save the file to your hard drive.
 - l. Repeat steps a. through k. to download the remaining file.

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

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



Note

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

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

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

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

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

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

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

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

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

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

- c. In the **Server Port Number** text box, enter the port number on the FTP server through which the download occurs. The default value is 21.
- Step 13** Click **Download** to download the software to the Cisco WLC.
A message appears indicating the status of the download.
- Step 14** After the download is complete, click **Reboot**.
- Step 15** If you are prompted to save your changes, click **Save and Reboot**.
- Step 16** Click **OK** to confirm your decision to reboot the Cisco WLC.
- Step 17** For Cisco WiSM2 on the Catalyst switch, check the port channel and re-enable the port channel if necessary.
- Step 18** If you have disabled the 802.11a/n and 802.11b/g/n networks in [Step 4](#), re-enable them.
- Step 19** To verify that the 8.0.13x.0 Cisco WLC software is installed on your Cisco WLC, click **Monitor** on the Cisco WLC GUI and view the Software Version field under Controller Summary.

Special Notes for Licensed Data Payload Encryption on Cisco Wireless Controllers

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

Important Note for Customers in Russia

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



Note

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

Downloading and Installing a DTLS License for an LDPE Cisco WLC

- Step 1** Download the Cisco DTLS license.
- a. Go to the Cisco Product License Registration at this URL:
<https://tools.cisco.com/SWIFT/LicensingUI/Quickstart>
 - b. Click **Get Other Licenses** drop down menu.
 - c. Choose **IPS, Crypto, Other Licenses**.

- d. Under **Wireless**, choose **Cisco Wireless Controllers (2500/5500/7500/8500/WiSM2) DTLS License**.
 - e. Complete the remaining steps to generate the license file. The license file information will be sent to you in an e-mail.
- Step 2** Copy the license file to your TFTP server.
- Step 3** Install the DTLS license. You can install the license either by using the Cisco WLC web GUI interface or the CLI:
- To install the license using the web GUI, choose:
Management > Software Activation > Commands > Action: Install License
 - To install the license using the CLI, enter this command:
license install tftp://ipaddress /path /extracted-file
- After the installation of the DTLS license, reboot the system. Ensure that the DTLS license that is installed is active.
-

Upgrading from an LDPE to a Non-LDPE Cisco WLC

- Step 1** Download the non-LDPE software release:
- a. Go to the Cisco Software Center at this URL:
<http://www.cisco.com/cisco/software/navigator.html?mdfid=282585015&i=rm>
 - b. Choose the Cisco WLC model.
 - c. Click **Wireless LAN Controller Software**.
 - d. In the left navigation pane, click the software release number for which you want to install the non-LDPE software.
 - e. Choose the non-LDPE software release: AIR-X-K9-X-X.X.aes
 - f. Click **Download**.
 - g. Read the Cisco End User Software License Agreement and then click **Agree**.
 - h. Save the file to your hard drive.
- Step 2** Copy the Cisco WLC software file (*filename.aes*) to the default directory on your TFTP server or FTP server.
- Step 3** Upgrade the Cisco WLC with this version by performing [Step 3](#) through [Step 19](#) detailed in the [“Upgrading to Cisco WLC Software Release 8.0.13x.0”](#) section on page 12.
-

Interoperability With Other Clients in Release 8.0.13x.0

This section describes the interoperability of Release 8.0.13x.0 of the Cisco WLC software with other client devices.

Table 8 describes the configuration used for testing the client devices.

Table 8 Test Bed Configuration for Interoperability

Hardware/Software Parameter	Hardware/Software Configuration Type
Release	8.0.13x.0
Controller	Cisco 5508 Controller
Access points	3502, 3602, 2602, 1702, 2702, 3702, 702W
Radio	802.11ac, 802.11a, 802.11g, 802.11n2, 802.11n5
Security	Open, WEP, PSK (WPA and WPA2), 802.1X (WPA-TKIP and WPA2-AES) (LEAP, PEAP, EAP-FAST, EAP-TLS)
RADIUS	ACS 5.3, ISE 1.2
Types of tests	Connectivity, traffic, and roaming between two access points

The following tables list the client types on which the tests were conducted. The clients included laptops, hand-held devices, phones, and printers.

- Laptop: Table 9 lists the laptop client types on which the tests were conducted.

Table 9 Laptop Client Type List

Client Type and Name	Version
Intel 4965	13.4
Intel 5100/5300	14.3.2.1
Intel 6200	15.15.0.1
Intel 6300	15.16.0.2
Intel 6205	15.16.0.2
Intel 1000/1030	14.3.0.6
Intel 8260	18.32.0.5
Intel 7260	18.32.0.5
Intel 7265	18.32.0.5
Intel 3160	18.32.0.5
Broadcom 4360	6.30.163.2005
Linksys AE6000 (USB)	5.1.2.0
Netgear A6200 (USB)	6.30.145.30
Netgear A6210(USB)	5.1.18.0
D-Link DWA-182 (USB)	6.30.145.30
Engenius EUB 1200AC(USB)	1026.5.1118.2013
Asus AC56(USB)	1027.7.515.2015
Dell 1395/1397/Broadcom 4312HMG(L)	5.30.21.0
Dell 1501 (Broadcom BCM4313)	v5.60.48.35/v5.60.350.11

Table 9 Laptop Client Type List

Client Type and Name	Version
Dell 1505/1510/Broadcom 4321MCAG/4322HM	5.60.18.8
Dell 1515(Atheros)	8.0.0.239
Dell 1520/Broadcom 43224HMS	5.60.48.18
Dell 1530 (Broadcom BCM4359)	5.100.235.12
Dell 1540	6.30.223.215
Cisco CB21	1.3.0.532
Atheros HB92/HB97	8.0.0.320
Atheros HB95	7.7.0.358
MacBook Pro	OSX 10.11.1
MacBook Air old	OSX 10.11.1
MacBook Air new	OSX 10.11.1
Macbook Pro with Retina Display	OSX 10.11.1
Macbook New 2015	OSX 10.11.1

- Tablet: [Table 10](#) lists the tablet client types on which the tests were conducted.

Table 10 Tablet Client Type List

Client Type and Name	Version
Apple iPad2	iOS 9.2(13C75)
Apple iPad3	iOS 9.2(13C75)
Apple iPad mini with Retina display	iOS 9.2(13C75)
Apple iPad Air	iOS 9.2(13C75)
Apple iPad Air 2	iOS 9.2(13C75)
Apple iPad Pro	iOS 9.2(13C75)
Samsung Galaxy Tab Pro SM-T320	Android 4.4.2
Samsung Galaxy Tab 10.1- 2014 SM-P600	Android 4.4.2
Samsung Galaxy Note 3 – SM-N900	Android 5.0
Microsoft Surface Pro 3	Windows 8.1 Driver: 15.68.3073.151
Microsoft Surface Pro 2	Windows 8.1 Driver: 14.69.24039.134
Google Nexus 9	Android 6.0
Google Nexus 7 2nd Gen	Android 5.0

- Phones: [Table 11](#) lists the phone client types on which the tests were conducted.

Table 11 Phone Client Type List

Client Type and Name	Version
Cisco 7921G	1.4.5.3.LOADS
Cisco 7925G	1.4.5.3.LOADS
Cisco 8861	Sip88xx.10-2-1-16
Apple iPhone 4S	iOS 9.2(13C75)
Apple iPhone 5	iOS 9.2(13C75)
Apple iPhone 5s	iOS 9.2(13C75)
Apple iPhone 5c	iOS 9.2(13C75)
Apple iPhone 6	iOS 9.2(13C75)
Apple iPhone 6 Plus	iOS 9.2(13C75)
HTC One	Android 5.0
OnePlusOne	Android 4.3
Samsung Galaxy S4 – GT-I9500	Android 5.0.1
Sony Xperia Z Ultra	Android 4.4.2
Nokia Lumia 1520	Windows Phone 8.1
Google Nexus 5	Android 5.1
Google Nexus 6	Android 5.1.1
Samsung Galaxy S5-SM-G900A	Android 4.4.2
Huawei Ascend P7	Android 4.4.2
Samsung Galaxy S III	Android 4.4.2
Google Nexus 9	Android 6.0
Samsung Galaxy Nexus GTI9200	Android 4.4.2
Samsung Galaxy Mega SM900	Android 4.4.2
Samsung Galaxy S6	Android 5.1.1
Samsung Galaxy S5	Android 5.0.1
Xiaomi Mi 4i	Android 5.0.2
Microsoft Lumia 950 XL	Windows 10

Features Not Supported on Cisco WLC Platforms

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

- [Features Not Supported on Cisco 2500 Series WLCs](#)
- [Features Not Supported on WiSM2 and Cisco 5500 Series WLCs](#)
- [Features Not Supported on Cisco Flex 7500 WLCs](#)
- [Features Not Supported on Cisco 8500 WLCs](#)
- [Features Not Supported on Cisco Virtual WLCs](#)

- [Features Not Supported on Mesh Networks](#)

Features Not Supported on Cisco 2500 Series WLCs

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


Note

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


Note

Directly connected APs are supported only in the Local mode.

Features Not Supported on WiSM2 and Cisco 5500 Series WLCs

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


Note

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

- Configuration of 802.3 bridging, AppleTalk, and Point-to-Point Protocol over Ethernet (PPPoE)
- Fragmented Pings on any interface
- Right-to-Use licensing

Features Not Supported on Cisco Flex 7500 WLCs

- Static AP-manager interface



Note For Cisco Flex 7500 Series WLCs, it is not necessary to configure an AP-manager interface. The management interface acts like an AP-manager interface by default, and the access points can join on this interface.

- TrustSec SXP
- IPv6/Dual Stack client visibility



Note IPv6 client bridging and Router Advertisement Guard are supported.

- Internal DHCP Server
- Access points in local mode



Note An AP associated with the Cisco WLC in the local mode should be converted to the FlexConnect mode or Monitor mode, either manually or by enabling the autoconvert feature. On the Cisco Flex 7500 WLC CLI, enable the autoconvert feature by entering the **config ap autoconvert flexconnect** command.

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



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

- PMIPv6

Features Not Supported on Cisco 8500 WLCs

- TrustSec SXP
- Internal DHCP Server

Features Not Supported on Cisco Virtual WLCs

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

- Multicast



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

- FlexConnect central switching



Note FlexConnect local switching is supported.

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



Note Outdoor APs in the FlexConnect mode are supported.

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

Features Not Supported on Access Point Platforms

- [Features Not Supported on 1130 and 1240 APs, page 25](#)
- [Features Not Supported on 1520 and 1550 APs \(with 64 MB memory\), page 26](#)

Features Not Supported on 1130 and 1240 APs

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

- Central-DHCP functionality
- Split tunneling
- Configuration of Network Address Translation (NAT) and Port Address Translation (PAT) on FlexConnect locally switched WLANs
- Point to Point Protocol (PPP) and Point to Point Protocol over Ethernet (PPPoE) for APs in FlexConnect mode
- 802.11u
- 802.11r Fast Transition
- LLDP
- Rate Limiting per AP
- mDNS AP

- EAP-TLS and PEAP for Local Authentication support as EAP method
- WLAN-to-VLAN mapping when AP part of FlexConnect Group
- Per user AAA AireSpace ACL name override
- Local MFP
- DNS-based (fully qualified domain name) access control lists (ACLs)
- Flex + Bridge mode (introduced in Release 8.0.100.0)

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

- PPPoE
- PMIPv6



Note

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

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

Features Not Supported on Mesh Networks

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

Caveats

Caveats describe unexpected behavior in a product. The Open Caveats section lists open caveats that apply to the current release and may apply to previous releases. A caveat that is open for a prior release and is still unresolved applies to all future releases until it is resolved.

To view the details of the software bugs pertaining to your product, perform the following task:

Click the Caveat ID/Bug ID number in the table.

The corresponding Bug Search Tool page is displayed with details of the Caveat ID/Bug ID.

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

To view the details of a caveat whose ID you do not have, perform the following procedure:

1. Access the BST using your Cisco user ID and password:
<https://bst.cloudapps.cisco.com/bugsearch/>
2. In the Bug Search window that is displayed, enter the necessary information in the corresponding fields.

For more information about how to use the [Cisco Bug Search Tool](#) effectively, including how to set email alerts for bugs and to save bugs and searches, see the [Bug Search Tool Help & FAQ](#) page.

Open Caveats

Table 12 *Open Caveats in Release 8.0.132.0*

Bug ID	Headline
CSCup29095	Mesh: PI not showing the neighbor details in mesh links page of the parent
CSCup92480	802.11ac module reloads unexpectedly due to PCI reset
CSCuq36265	Cisco 3600 AP with 802.11ac module non broadcast SSID client connectivity issues
CSCuq45110	M1 is sometimes encrypted leading to M1 refusal on station side
CSCur02514	Cisco 8.0.100.x release: SNMP trap is not sent out on HA switch-over
CSCur40006	WLC: Group size exceeds when static RF Group member is added
CSCur53809	Cisco 2702 AP sometimes unable to receive packets/ACK from STA with 20MHz wide
CSCur80841	Apple remote app not working with MDNS snooping enabled
CSCur88123	Invalid PSK for layer 2 security after controller reboot
CSCus06589	Cisco 2700 AP flooding AP sourced packets out of auxiliary Gig 1
CSCus46848	Cisco WLC becomes non-responsive on rf-profile page if too many rf-profiles are created
CSCus49607	Cisco 5500 WLC -HA reloads unexpectedly with taskname:tosapiReaper
CSCus52826	Rogue client detection on serving channel on WIPS enabled non monitor APs
CSCus52828	SNMP v3 rw user credentials not working if key length is greater than 32
CSCus55192	Cisco 8500 WLC reloads unexpectedly during removing SNMP communities
CSCus58120	Traplog is wrong about temperature status
CSCus58468	Multicast address set issue using SNMP
CSCus61679	Problem in client statistics reports: including RSSI and SNR can be lost at WLC
CSCus68363	Rogue Policies are not applied correctly
CSCus71140	Bonjour service learnt via Mdns AP is being forwarded to wired
CSCus75120	Cisco FlexConnect local authentication not working in 8.0.100.0 release
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
CSCus79791	Client connected to 802.11n AP shows as 802.11ac client on Cisco WLC
CSCus80562	Power client settings does not work

Table 12 *Open Caveats in Release 8.0.132.0*

Bug ID	Headline
CSCus83638	Cisco 3702AP 5-GHz radio beaconing but not accepting client association
CSCus84770	Unable to delete the SNMP community Public from GUI
CSCus90178	AIR-OEAP602I has TCP port 5162 open
CSCut10131	Cisco WLC fails to resend ciscoLwappDot11ClientMovedToRunState traps
CSCut27312	AP group VLAN not overridden on client when AAA override is enabled on WLAN
CSCut31568	Updating oui on vWLC delete the existing oui database
CSCut40765	Cisco WLC reporting incorrect remote address to TACACS+ sever
CSCut44986	Cisco WLC throwing error when accounting is disabled on WLAN
CSCut55043	FlexConnect Group with space in name renders terminal session unusable
CSCut60058	Cisco WLC does not deauthenticate client when AAA Flex-ACL is not present on AP
CSCut61668	AID errors on the controller for Cisco FlexConnect APs
CSCut63868	Cisco 8500 WLC reloads unexpectedly on Taskname emWeb when configuring AVC profile via CLI
CSCut64180	AP holds BW after call when WLC HA SO happens during call setup
CSCut81253	Ethernet bridging does not work on RAP with 5-GHz backhaul
CSCut83422	Cisco vWLC SN changed after management interface IP change
CSCut88319	FF08::/16 range of organization-local IPv6 multicast addresses
CSCut90276	AireOS Traceback: APF-4-PROC_ACTION_FAILED
CSCut91086	Client associated to MAP does not get AAA override in Flex+Bridge mode
CSCut92934	Cisco vWLC - AP with expired manufacturing installed certificates (MIC) not able to join with ignore MIC settings
CSCuu08012	Cisco 2700 AP CleanAir sensors died (src/dspm_main.c:389) - slot 0
CSCuu13860	Autoconvert FlexConnect is stored as disable on startup-commands
CSCuu14124	RF-profile losing the channel and coverage values after downloading config file
CSCuu16052	Do not set DF bit for non-CAPWAP traffic from WLC such as RADIUS
CSCuu16348	Cisco OEAP600 RLAN quiet wired clients timing out
CSCuu17338	Cisco 1142AP configuration loss after cold reboot
CSCuu21625	Session not cleared on Cisco 5508 WLC as anchor and Cisco 3850 switch as foreign causing authentication issues
CSCuu33740	Cisco WLC reloads unexpectedly while editing SNMP community - waFormSubmit_snmp_comm_list
CSCuu42378	Rx-SoP threshold not working correctly
CSCuu51641	WiSM2: config ap tcp-mss-adjust enable all 1363 missing in HA configuration
CSCuu59340	SNR alarms for mesh APs have invalid content not working as expected
CSCuu70442	Cisco WLC reloads unexpectedly after config mesh linktest APsource APdest 1 1
CSCuu71471	MTU value stacks in HA




Table 12 *Open Caveats in Release 8.0.132.0*

Bug ID	Headline
CSCuu83548	Traceback observed in export-foreign standby WLC while dissociating client
CSCuu89294	Primary AP in Flex Group not saved in WLC CFG nor commands backup
CSCuu97761	Foreign WLC upgraded to 8.1 release fails to export clients to Anchor WLC
CSCuv03380	During mesh roam security error gateway is not reachable leading to CAPWAP restart
CSCuv03937	Unexpected WLC reload with RLDP enabled
	 Note This bug is resolved in Release 8.0.133.0.
CSCuv10692	AckFailureCount getting huge value in short period
CSCuv40794	AP impersonator alarm for Cisco 3602i AP
CSCuv43466	Garbage character are shown in CLI show run-config startup-command
CSCuv54033	Egress ACL does not work when it is switched from Ingress to Egress
CSCuv79354	Cannot configure IP address x.x.x.255 or x.x.x.0 as gateway in GUI
CSCuv93380	AP radio resets in disc_tx_client_dq_one(0x8b1984)+0x180
CSCuv97132	Show ap image all output will not fetch spamPreDownloadInProgress
CSCuv99415	AP should bootup even if CAPWAP iOS download is corrupted
CSCuv99434	Roams using PMF + OKC not working correctly
CSCuw02258	Severity filter for monitoring CleanAir interferer does not work as expected
CSCuw03323	Cisco 702w AP draws additional power (22.1 watts) when LAN port 4 is disabled
CSCuw09545	Incorrect DHCP Pool Usage on the Cisco WLC when queried via SNMP
CSCuw18306	Mesh AP 5GHz channel on non-configured channel in DCA list on Cisco WLC
CSCuw21213	Downstream: QoS Bronze Profile not marking traffic to AF11 on FlexConnect AP
CSCuw23023	Cisco 3700 AP sniffer mode not capturing on 5-GHz radio with Rx-SoP set
CSCuw27160	RF Grouping Algorithm > update interval not synchronized on Cisco WLC
CSCuw30129	Debugging logging quickly falls behind real-time
CSCuw34201	SKC Enabled: WLC denying client association due to Max Client on AP Radio
CSCuw34565	Cisco Flex7500 WLC reloads unexpectedly after deleting AP crash logs from GUI
CSCuw36069	Threshold MIBs incorrectly set for WSSI modules.
CSCuw38795	Cisco 5508 WLC reloads unexpectedly upon pushing RF calibration template from PI
CSCuw41092	AP not send traffic indication in beacon for power-save client after FT
CSCuw46766	Cisco 2700 AP and 3700 AP reloads unexpectedly after upgrade to 8.1.111.x
CSCuw48090	Cisco 1602 AP 5-GHz radio stops transmitting / receiving frames
CSCuw48488	4-way handshake fails on 802.11r+802.11w (FT+PMF) WLAN
CSCuw61901	Local auth EAP-FAST not working for Flex AP authenticated user with Cisco AnyConnect

Table 12 *Open Caveats in Release 8.0.132.0*

Bug ID	Headline
CSCUw62172	System reloads unexpectedly on HA standby while setting authentication priority order from PI in Cisco 7.6 release
CSCUw62850	WiSM2 running 8.0.120.x release reloads unexpectedly on mwar_ms_deadlock.crash
CSCUw63311	Increased ping latency and reduced traffic on Cisco 8510 WLC
CSCUw65933	Client statistics mismatch in client roaming scenarios
CSCUw66299	Cisco WLC msglog showing NMSP Transmit Failure even when there is no MSE
CSCUw70789	AP using a reserved port to join the WLC
CSCUw95126	Optimized Roaming Rejection function does not work
CSCUx00803	New Mobility clients stuck in DHCP_REQD state with NAT IP on foreign controller
CSCUx08557	Reaper reset because of SNMPTASK : VALIDATE_GUEST_SESSION_FAILED
CSCUx11666	Cisco 8500 WLC returns differing cLMobilityGroupMembersTable values
CSCUx15311	Cisco WLC does not send all accounting messages to TACACS+ server
CSCUx20994	Cisco WLC error for MAG code: PMIPv6 MAG callback returned failure for station
CSCUx21803	Client not receive broadcast ARP request after AP failover
CSCUx24575	8.2.15.5 release- MAPs are unstable if convergence is standard
CSCUx28775	WLC per-WLAN client traffic statistics accuracy enhancements
CSCUx32328	Token Bucket leak with QoS Roles and with web authentication on Cisco 8.0.120.x release
CSCUx34439	802.11ac module clients can not connect to Cisco 3600 AP radio slot2
CSCUx36516	Client count mismatch Under Monitor >Clients and Wireless >Specific AP
CSCUx45077	Cisco 3500 AP reloads unexpectedly due to LWAPP CLIENT process
CSCUx53607	Cisco WLC SNMP for cLAPGroups802dot11bgRFProfileName returns wrong value
CSCUx58953	Can not set channel from web interface
CSCUx59359	Cisco 8510 WLC behind NAT on New mobility and client stuck in DHCP_REQD state
CSCUx60012	With New Mobility - mobility members do not survive reload
CSCUx60873	RADIUS interface overwrite does not work when choosing AP group interface
CSCUx61747	WLC hangs when configuring DNS-based ACL
CSCUx62529	LAP reloads unexpectedly at disc_client_txq_dump
CSCUx62936	IPv6 address delete in MSCB failing when client hops between WLANs
CSCUx63218	Cisco WLC upgrade to 8.0 release moved APs to EAP-MD5 authentication on wired dot1x
CSCUx63383	Cisco Flex AP not processing discovery response
CSCUx63449	Cisco WLC running 8.0.120.x reloads unexpectedly on TransferMsgPeerSend
CSCUx65703	In Cisco 3602 AP radio shutdown (2.4GHz and 5GHz)
CSCUx69221	HP printer not seen by iOS devices after returning from sleep mode

Table 12 *Open Caveats in Release 8.0.132.0*

Bug ID	Headline
CSCux75330	Mismatch AP count and unable to add more APs to WLC
CSCux78464	Cisco WLC reloads unexpectedly in Process Bonjour_Process_Task
CSCux82955	Anchor WLC does not forward DHCP request to server as VLAN is set to 0
CSCux85357	Cisco WLC sends GARP for flex local switching clients after HA switch-over
CSCux91996	Rogue containment not starting if no client info on best RSSI AP
CSCux95319	Roaming central to local authentication causes in flex causes 802.1x table failures
CSCux95662	PMIPv6 client fails to get an IP if there is no DHCP server configured
CSCux96500	WiSM2/WLC reloads unexpectedly on bcastReceiveTask
CSCux96731	DP reloads unexpectedly on Cisco 8500 WLC
CSCuy02774	PMIPv6 client binding clean up issues
CSCuy04572	Wrong times tamp sent on rogue traps when delta value set on controller
CSCuy06005	vWLC reloads unexpectedly after auto provision from PI
CSCuy09488	ACL's not getting pushed to AP using flex-autoconvert for Flex groups
CSCuy11885	Cisco 3500 AP reloads unexpectedly by the Pid 128: Process CAPWAP CLIENT
CSCuy23295	Interface NAS ID given priority over WLAN NAS ID in default AP group
CSCuy31962	APs detect different WPA Support value from Rogue AP
CSCuy35659	Local policy with action session timeout not enforced for newly profiled client
CSCuy42459	Cisco WLC reboots - Localeap (EapFramework) memory leak - Negative testing
CSCuy45485	Containment to choose AP based on rogue client detected as well as RSSI
CSCuy47407	Client leak at anchor controller
CSCuy54406	Flex SSID going to centrally switched WLANs list
CSCuy58091	Evaluation of Cisco WLC for OpenSSL March 2016
CSCuy59147	Mobility control path does not come up after deleting and adding again in scale
CSCuy63671	Not able to edit mobility group member with edit all option from WEB GUI
CSCuy64520	Access Points (AP) sending CDP packets to the wireless clients
CSCuz04212	Single radio functionality issues  Note This bug is resolved in Release 8.0.133.0.
CSCuz16883	Address registration at a foreign subnet when subnet mask does not match the anchor  Note This bug is resolved in Release 8.0.133.0.
CSCuz24121	mDNS is disabled on Cisco 2500 WLC platform  Note This bug is resolved in Release 8.0.133.0.
CSCvc65568	Cisco Wireless IP Phone 8821 fails 802.11r FT roam with 'Invalid FTIE MIC'

Resolved Caveats

Table 13 *Resolved Caveats in Release 8.0.132.0*

Bug ID	Headline
CSCtl96208	CAPWAP AP hostname; CLI returns ERROR command is disabled
CSCtu45614	Spectrum Management Bit should be set to 1 all the time
CSCul07738	DPAA Tx/Rx stuck; reloads due to Ethernet interface receive failure
CSCum86031	Roaming Cisco 5508 WLC to Cisco 5760 WLC applies wrong QoS policy on configuring aaa-override
CSCun12965	Lightweight AP should not send jumbo frame by default
CSCun52472	show dtls connection shows blank AP name column for CAPWAP_Data
CSCuo16301	HA:-Unable to pair up the active/standby Cisco WLC due to configuration sync failure
CSCuo48442	Stale old DTLS data_encryption session histories are left on Cisco WLC
CSCup13091	Local EAP local user created for specific WLAN works for different WLAN
CSCup56257	SNMP PMIP NAI type attribute support is required
CSCup64468	Cisco WLC sends invalid format of syslog message by adding # at the beginning of the message
CSCup68372	Statistics are carried over when session timeout occurs
CSCup72502	Cisco 5500 WLC on 7.6 release does not deauthenticate client when Flex ACL is not present on AP
CSCup75446	Default interface takes precedence over foreign VLAN mapping with CWA
CSCup80403	Low iMac Tput -supported rate IE in association response has zero length
CSCup88910	AP impersonation flood of events on WLC 8510-SR14-00512
CSCuq50069	SHA1 key cipher not working between Cisco WLC 80 and MSE 80 CCO versions
CSCuq56604	GRE key DB can leak in case of flapping clients
CSCuq56829	Flex+Bridge maps drop after association - Failed to receive data keep-alive
CSCuq68753	Cisco 5500 WLC anchor running 7.6.122.21 release reloads unexpectedly on osapiBsnTimer
CSCuq73590	Cisco WLC adds incorrect class attribute in accounting stop
CSCuq86274	Cisco 1530 AP DFS detection across all channels
CSCuq88573	Cisco Dynamic Bandwidth Selection (DBS): client type count is incorrect
CSCuq88748	Rogue APs wrong classification from malicious to unclassified
CSCuq96986	Cisco 2504 WLC reloads unexpectedly on upgrade to Cisco 8.0 release
CSCur08754	Local authentication is not working for Cisco Flex AP authenticated users
CSCur11060	False positive on honeypot alert with multiple SSIDs
CSCur13400	DHCP Option 82 and Sub Option 5 issue in Cisco WLC running 8.0 release
CSCur24512	Cisco 3602/3702 APs reloads unexpectedly while processing the extended capabilities IE on the association response sent from WLC
CSCur25239	Controller reloads unexpectedly on mping command over telnet/SSH

Table 13 Resolved Caveats in Release 8.0.132.0 (continued)

Bug ID	Headline
CSCur30618	SNMP WALK fails for all APS if Country code is not present even on a single AP
CSCur32475	New Mobility web-authentication on MAC filter failure always sends client to web-authentication
CSCur33320	SC1/SC2/SC3 radio resets with firmware stuck in macenb (Cont. of CSCuo27106)
CSCur43124	WSSI module stops working after upgrade from 7.4.121.0 to 7.6.130
CSCur46376	Controller reloads unexpectedly with task webauthRedirect under heavy load
CSCur48612	Cisco 8.1 release emWeb reloads unexpectedly when adding devices to mDNS policy
CSCur48944	Issues found in client statistics reports and optimized roaming
CSCur49165	WiSM2 system reloads unexpectedly on radiusTransportThread aaaRadiusAuth
CSCur57909	Client misses to override VLAN after shifting WLAN
CSCur58057	Cisco Flex AP loses some WLANs after the radio resets
CSCur60218	New mobility web authentication on MAC filter failure and export anchor request fails
CSCur69774	Cisco 8500 WLC reloads unexpectedly with SNMP task
CSCur71315	Cisco 1552 AP bridge transmit voice queue stuck leading to out of TX buffers
CSCur74208	cLMobilityExtMgrAddress.0; Returning in IP in Reverse Order
CSCur80006	Unable to enable HTTPS redirect in WLC GUI
CSCur80935	AAA overridden ACL is not applied on Guest Access (GA) controller
CSCur88307	AP name unknown in dissociation messages (Intermittent)
CSCur90555	Cisco WLC running Cisco 8.0 keeps ghost client entry
CSCur91936	MDNS discovery issue with Cisco WLC on 8.0.100 release
CSCur94924	emWeb Memory Leak on Cisco 8500 AP SP WiFi Profile Testbed
CSCur95365	Cisco WLC reloads unexpectedly while issuing command 'show ap config general'
CSCur98573	Memory increase on DTLS connections when more than 500 APs join Cisco 5508 WLC
CSCur99863	Central Web Authentication (CWA) : Cisco WLC running 8.0 release some times moves to RUN state while in redirect state
CSCus03406	Data plane crash on Cisco 8500 WLC running 7.6.x release
CSCus03487	Cisco 3700 AP sends wrong TLV during power level negotiation
CSCus07013	Adding MAC filter check when client is changing SSID for web authentication
CSCus17191	Cisco 1142 AP DHCP renew delay after Eap-Fast authentication
CSCus20991	RADIUS Cisco Network Admission Control (NAC) client authentication issues in Cisco 7.6.130.0 release
CSCus21502	Cisco FlexConnect 1142 AP reloads unexpectedly while debug dot11 mgmt station is enabled
CSCus30429	Cisco OEAP600 not giving IP on remote LAN port in 8.0 release
CSCus33759	Local policies not working after OUI Update

Table 13 *Resolved Caveats in Release 8.0.132.0 (continued)*

Bug ID	Headline
CSCus39396	Cisco 8.0.100.x QoS bronze profile not marking traffic to AF11 on Cisco FlexConnect
CSCus46424	Band select not working on Cisco 1042 AP
CSCus53635	Add 802.11a Philippines country support for Cisco 1532I APs joined to Cisco 5760 WLC
CSCus54751	sisfSwitcherTask system unexpected reload comes up with blank configuration
CSCus61445	DNS ACL on Cisco WLC is not working - AP not sending DTLS to Cisco WLC
CSCus66289	Cisco WLC reloads unexpectedly after packet-dump
CSCus68340	Standby keeps auto rebooting and stays in STANDBY COLD state
CSCus73932	Cisco 8510 WLC running 8.0.110.x issue on multicast configuration
CSCus74299	New mobility: client is not deleted in Cisco 5508 WLC when it roams at web authenticate state
CSCus76833	Cisco 5508 WLC reloads unexpectedly at sisfSwitcherTask
CSCus77368	Cisco WLC reloads unexpectedly on ewaFormSubmit_cell_edit
CSCus77477	NGWC Increase the number of URLs allowed in a DNS ACL in Cisco WLC
CSCus78002	Cisco 1262 AP reloads unexpectedly soon after STACKLOW for 802.11 DB Audit loads
CSCus80249	Reaper reset with APF guest reloads unexpectedly with a scale
CSCus80478	Cisco 1530 AP does not forward or send packets to wired side after bootup
CSCus80685	AP sends few frames with previous security association's packet number
CSCus89468	Need to add Cisco 802 AP to the list of APs that support Flex+Bridge mode
CSCus89485	Negative rogue count reported in show rogue ap summary
CSCus91251	Probe Filter incorrect configuration causing issues with Cisco FastLocate and Cisco FlexConnect
CSCus91439	Cisco WLC - Memory leak - k_mib_cisco_lwapp_dot11_client.c
CSCus92667	GET on AP groups table after set response missing
CSCut02524	Default NAS ID value at the AP-Groups should be empty or none
CSCut03762	Cisco 8500 WLC -Endianness issue with debug mobility keep-alive enable peer-ip
CSCut06502	Cisco WLC unexpectedly reloads due to task name RRM-CLNT-5_0
CSCut09821	Unused Data DTLS session remains on WLC running 7.6.130.x release
CSCut11821	Cisco WLC ad-hoc containment does not stop
CSCut14459	Session ID changes for an inter-controller client roam using EAPFAST
CSCut14796	NMSP link is down between MSE10 and Cisco 5500 WLC (8.1.10.183)
CSCut16170	Mobility tunnel down after switchover on Cisco 7.6.x release
CSCut18071	IRCM Guest Access mobility failing during roam test
CSCut20426	Client on WLAN(WebAuth+FlexLocalSwitch+Anchor) changes to LocalSwitching
CSCut21931	EmWeb Core spamGetMeshRunningConfig when configure mesh network

Table 13 *Resolved Caveats in Release 8.0.132.0 (continued)*

Bug ID	Headline
CSCut22092	Client Disassociated due to inactivity ReasonCode: 4
CSCut23325	Cisco 1700 AP not encrypting Internet Control Message Protocol (ICMP) and arp sent from the client over the air
CSCut24276	Unexpected PMKID count field in beacon's RSN IE
CSCut25670	CSCuWAP: %DTLS-5-SEND_ALERT: Send FATAL; join failure loop
CSCut27598	Client unable to get IP when switching WLAN on New mobility
CSCut31468	Local profile shows wrong statistics under manufacturer statistics
CSCut35315	GUI changes - Negative rogue count reported in show rogue ap summary
CSCut39010	Multiple APs reset with beacons stuck
CSCut39118	Cisco 8510 WLC fails to collect feature MobilityExtGroupMember on PI 2.2
CSCut40305	Console logs are created during AP-GUI login sessions and Positive Stuff Event (PSE) status
CSCut42926	WLC reloads unexpectedly on SNMP task after doing config audit from PI
CSCut43770	PMIPv6 Client Traffic is sent to the wrong LMA
CSCut46811	Cisco 3702 AP not accepting clients on 5-GHz when WIPs submode is enabled
CSCut48172	LSC AP provisioning happening after MAP is disconnected for long time
CSCut56741	Cisco 1600 AP: Radio reset with STOPPING CPQ FWD TRACE ON Bad CPQ removal
CSCut62319	Broadcast Key Rotation does not occur after MAC filtering is enabled
CSCut64504	Race condition on the AP for delete and add driver client
CSCut70403	Cisco WLC reloads unexpectedly with task name 'HAConfigSyncTask'
CSCut74263	MAG on AP: AP does not clear bindings after session/user timeout and de-authorization
CSCut76481	Cisco WLC sends 1499 bytes MTU switchover
CSCut85027	AP is generating corrupted coredump
CSCut87326	Cisco WLC generates SNMP traps to PI 2.2 for AIR-3702 PoE+ getting low power
CSCut88267	WLC unexpected reload in task webauthRedirect during client redirect
CSCut93569	NMSP inactive with Cisco WLC
CSCut93712	AP not sending RM IE for 802.11k in association response; and when device is running 8.1.x no 802.11k for iOS
CSCut94260	AP wIPS module sending random characters in the alarm message
CSCut97683	WLC reloads unexpectedly on spamApTask2 8.0.110.0
CSCut98006	DFS detections due to high energy profile signature on Cisco 2600/3600APs
CSCut99150	Cisco 2702 AP requesting as a Type 1 power device instead of Type 2
CSCuu02281	APs on WLC with wireless networks disabled detecting rogues
CSCuu05565	NDP packets not transmitted on secondary 20 channels
CSCuu06047	Packet drops on Cisco 2702 AP in flex local auth/local switch mode

Table 13 *Resolved Caveats in Release 8.0.132.0 (continued)*

Bug ID	Headline
CSCuu07700	EAP Packet does not get encrypted in re-authorization request from the client
CSCuu08592	Override interface interface-group not applied on reauthentication for IPv6 clients
CSCuu08752	SXP reloads unexpectedly when running Trust Sec clients
CSCuu12045	Mobility MAC configuration should not be uploaded in the configuration file
CSCuu20097	Token bucket leak when QoS roles setup and when working with WebAuthentication
CSCuu23521	Cisco 5520 WLC reloads unexpectedly on task name radiusTransportThread
CSCuu25362	1 byte corruption in CAPWAP payloads using TLV infra
CSCuu28534	Client user name does not change when switched from WPA2 802.1x to PSK
CSCuu30530	PMIPv6 sh run correction
CSCuu37437	Cisco 8510 WLC reloads unexpectedly while NMSP polling in progress
CSCuu42396	AP radio firmware image install failure during bootup
CSCuu44155	RAP takes 15 minutes to use wired connection if there are wireless peers available
CSCuu45186	802.11 arp-cache does not work as expected
CSCuu47016	Cisco Application Visibility and Control UDP Vulnerability
CSCuu51713	RADIUS and Accounting Fall back do not work as expected
CSCuu54100	Switching between SSIDs fails with FAST SSID enabled on PMIPv6 WLANs
CSCuu57971	Cisco WLC reloads unexpectedly when AP image is pre-download task:spamApTask1
CSCuu59589	False positive AP sourced AP impersonation on corrupted beacon
CSCuu65672	DTLS capwap_Ctrl connections not cleared for APs connecting through WAN
CSCuu66675	Lock reloads unexpectedly on RADIUS: TransportThread during CMCC external auth
CSCuu68490	Duplicate radius-acct update message sent while roaming
CSCuu72366	System running on 8.0.110.x reloads unexpectedly on mmListen process
CSCuu77304	Clients deauthenticated from Cisco OEAP 600 LAN ports
CSCuu77738	Prime 3.0 Auto Provisioning is not working
CSCuu82416	Evaluation of Cisco WLC for OpenSSL June 2015
CSCuu82610	WLC dtls_free should zero out memory
CSCuu83748	Cisco WLC sends bsnRogueAPRemoved Trap when notify is configured to none
CSCuu83941	Cisco 8510 WLC: Error enabling global multicast with CAPWAP mode unicast
CSCuu91001	Netflow record sent without client IP address
CSCuu93296	EAP-TLS loosing device certificate in standalone mode after reboot
CSCuu98792	Cisco 1570 AP: antenna enable config is lost on reboot
CSCuu98971	Controller reloads unexpectedly during HA testing
CSCuu99344	Cisco WLC reloads unexpectedly as it fails to handle DHCP packet content while roaming on new mobility

Table 13 *Resolved Caveats in Release 8.0.132.0 (continued)*

Bug ID	Headline
CSCuu99662	Cisco controller running 8.1.104.x reloads unexpectedly
CSCuv00107	PMIPv6 Client MAC address shows up on the MAC address table of the Cisco Switch
CSCuv00598	Optimized Roaming per WLAN feature
CSCuv01337	config PMIPv6 add profile error not clear when profile length is greater than 32
CSCuv03963	Cisco WLC data plane reloads unexpectedly while loading fatal condition at broffu_fp_dapi_cmd.c
CSCuv04474	Cisco 700 AP reloads unexpectedly during multicast client traffic(cont.CSCuu89311)
CSCuv08570	Lightweight access point loses all config at times after power cycle
CSCuv09655	Anchor reloads unexpectedly on Cisco 8.0.110.14 release New Mobility apf_msDeleteTblEntry
CSCuv13731	Cisco 3702 AP sends burst traffic - AMPU/MSDU/Off-channel/RRM disabled
CSCuv22052	Link local multicast control traffic sent by APs IGMP Snooping Enabled
CSCuv22936	AP Flapping - CAPWAP keepalives are not replied to
CSCuv22951	Radio resets with reset code 37
CSCuv24097	Multicast from PMIPv6 client show client mac on layer3/2 switch
CSCuv27320	Wired clients in Cisco 702w AP leaking traffic across ports/vLANs
CSCuv28555	Cisco IW 3702 AP - voice queue stuck with no new clients able to associate
CSCuv31162	Cisco 5500 WLC continuously reloads unexpectedly in HA setup at task: apfRogueTask_2 and 3
CSCuv34277	Wireless Client not able to get IP address on Cisco Catalyst 3650 Switch Mobility Agent from Cisco 5508 WLC anchor
CSCuv34946	EoGRE and PMIPv6 client fails to move to Run state
CSCuv36505	Cisco WLC running 8.0 release sends messages flooding cli after debug client
CSCuv37613	Apple devices failing 802.11r FT roam
CSCuv51521	Active WLC should send GARPs when HA Re-Paring after Active-Active state
CSCuv53952	SSID still broad casted by the AP after the WLAN is deleted from the Cisco WLC
CSCuv59274	Cisco 1142 AP: CPU utilization shows a spike and is at 100% all the time
CSCuv61271	Window DHCP BAD_ADDRESS for Access Points
CSCuv67144	Need to re-evaluate Algeria if in -E or -I
CSCuv69967	Cisco OEAP600 AP series wired 802.1x remote LAN forward traffic in 802.1x required state
CSCuv74719	Apple clients EAP-FAST Authentication failure
CSCuv77499	Dynamically excluded client not updated in UI of Controller
CSCuv82110	Cisco vWLC: Decrypt errors occurred for client using WPA2 key on 802.11a intf
CSCuv85747	Mobility Member entries going stale

Table 13 *Resolved Caveats in Release 8.0.132.0 (continued)*

Bug ID	Headline
CSCuv86494	Cisco WLC clears AP MAC before deleting client sends netflow with zero AP MAC
CSCuv87657	Cisco WLCs running on 8.0 or 8.1 release fail to send FRAMED-IP attribute to AAA server
CSCuv87839	Wired clients in Cisco 702w AP getting put in management vLAN
CSCuv90042	Cisco FastLocate distant clients have strong RSSI value from AP intermittently
CSCuv90333	In 8.0 release afpmsConntask flood when running client console debug
CSCuv95254	Failed to associate Cisco7925 phones when Cisco WLC country code is set for Korea
CSCuv96333	Read only user able to change Telnet Capability settings
CSCuv97793	WiSM2 reloads unexpectedly on AP_DB_CREATE_ERR Message queue MFP-Q is nearing full
CSCUw01581	Cisco WiSM WLC running 8.2.1.x reloads unexpectedly on SISF BT process
CSCUw03414	Cisco WLC reloads unexpectedly while accessing the data
CSCUw06127	Due to memory leak in CDP Main system running 8.0.120 release reloads unexpectedly
CSCUw10610	Non authenticated HTTP page allows to logout any connected client
CSCUw12544	Rate-limiting is causing 500ms gap of traffic when roaming
CSCUw13264	Cisco 702w missing interface information on the controller after HA failover
CSCUw18179	WiSM2 running 8.2.1.x release reloads unexpectedly with SNMP task
CSCUw18589	Duplicate RADIUS IDs causing conflicting packets at the RADIUS servers
CSCUw24476	Increased ping latency and reduced traffic on Cisco 8510 WLC with QOS rate limiting
CSCUw24958	AP fails to transmit ADDBA response if a data packet is retried prior
CSCUw26377	The system reloads unexpectedly due to invalid form field validation on switch_cfg_rw.html
CSCUw28141	Cisco WLC unexpectedly reloads with Reaper Reset on SnmpGetNextTsmElement
CSCUw29564	APs show zero neighbors on 5-GHz band and client 802.11 packets are ignored
CSCUw35341	IP address lost on AAA override multiple subnetworks per VLAN DHCP requests
CSCUw35349	DHCP registration failing when mask from WLC interface does not match client received mask
CSCUw37942	Local EAP hardening
CSCUw44480	802.11r client fails authentication if self reset before user idle timeout expires
CSCUw50324	System reloads unexpectedly when CPU utilization is high for bonjour
CSCUw57588	Cisco 3600 AP unexpectedly reloads on am_xml_GetChildCount
CSCUw57850	Filtering for client calibration pulses with frequency offset
CSCUw71432	Mobility Express: Iphones/Ipads unable to connect to 802.11r enabled WLAN because of invalid MDID

Table 13 *Resolved Caveats in Release 8.0.132.0 (continued)*

Bug ID	Headline
CSCuW87468	On Cisco 3700 AP with WSM module running 8.0.120.0 release the Rogue containment is not working as expected
CSCuW89581	Cisco WLC reloads unexpectedly on apfReceiveTask
CSCuW90625	Rogue rules not applied correctly after upgrade to Cisco 7.6.130.x release
CSCuW91763	Feature AES Key Wrap does not work
CSCuW94949	When client tries FT roam between IOS Aps Invalid FTIE MIC is found in Cisco Mobility Express and Cisco WLC
CSCuW97316	Show client detail displaying allowed URL IP in reverse format
CSCuW97431	Mobility MAC is not synced to Standby Cisco WLC
CSCuX03108	Cisco 8510 WLC reloads unexpectedly on portalMsgTask
CSCuX06492	AP is sending RM IE in re-association response for non-802.11k clients
CSCuX07993	DNS-ACL: Redirection happening for the defined URL's also
CSCuX18259	PI 3.0 - Sync Issue on FlexConnect Native VLAN Configuration
CSCuX22620	Cisco 8510 WLC reloads unexpectedly on radiusTransportThread system task
CSCuX22935	HA 802.11r:Post SSO FT PSK/EAP Apple clients fails to connect
CSCuX37498	Change of Authorization (CoA) on Cisco WLC running 8.1.131.0 shows error message on ISE server
CSCuX39331	Cisco 8500 WLC series reloads unexpectedly on Task Name:osapiBsnTimer reason: Reaper reset
CSCuX41354	Evaluation of WLC for OpenSSL December 2015 vulnerabilities
CSCuX41577	Cisco WLC and Cisco AP out of sync for client exclusion list
CSCuX44741	WiSM running 8.2.1.x release reloads unexpectedly on SXP CRASH
CSCuX47470	Cisco WLC running 8.0.110.14 release reloads unexpectedly on running openssl_cert_hash_algo_check_callback
CSCuX53523	Interface NAS ID is not updating when client moves between interface group
CSCuX56652	Local Profile shows wrong statistics and percentage information
CSCuX82268	Cisco 8.0.x: Support for 802.11v clients to show 802.11v supported in client detail
CSCuX83098	Cisco WLC sends syslog message in an invalid format caused by adding # at the beginning of the message
CSCuX83635	FATAL: Could not send message out; prints on Cisco 5500/Flex 7500 WLC standby console
CSCuX86824	Kernel hang condition after unexpected system reload
CSCuX91000	Cisco WLC uses its Virtual IP (instead of management IP) to communicate with PI
CSCuX94240	Interoperability of 802.11 vDMS fails with Cisco 3600 AP with 802.11ac module
CSCuY04186	Interoperability of 802.11k failure in Flex mode as no RM IE in reassociation response
CSCuY06619	Interoperability of 802.11r preauthentication failure leading to full association
CSCuY07338	Evaluation of Cisco WLC for OpenSSL January 2016

Table 13 *Resolved Caveats in Release 8.0.132.0 (continued)*

Bug ID	Headline
CSCuy10546	Cisco vWLC running 8.0.121.0 release reloads unexpectedly when using RADIUS authentication for IPsec
CSCuy11085	Incorrect NAS ID sent when AP-group and WLANs have different interfaces
CSCuy33972	SSH host-key generate command does not change the key
CSCuy46033	MAP fails to rejoin the RAP after it loses connection on Cisco 8.0.121.0 release
CSCuy55634	Cisco 1530 AP in Mesh Flex-bridge mode does not transmit traffic if connected at 100M
CSCuy56696	Cisco vWLC reloads unexpectedly when using GUI on 8.0.122.x release

Installation Notes

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

Warnings



Warning

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

Statement 1071



Warning

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

Statement 1030



Warning

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



Warning

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

**Warning**

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

**Warning**

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

**Warning**

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

**Warning**

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

**Warning**

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

**Warning**

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

Safety Information

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

FCC Safety Compliance Statement

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

Safety Precautions

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

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

Installation Instructions

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

**Note**

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

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

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

Service and Support

Troubleshooting

For the most up-to-date, detailed troubleshooting information, see the Cisco TAC website at this URL:
<http://www.cisco.com/c/en/us/support/index.html>

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

Related Documentation

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

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

You can access these documents at:

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

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation* at: <http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html>.

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation as an RSS feed and delivers content directly to your desktop using a reader application. The RSS feeds are a free service.

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

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

© 2016 Cisco Systems, Inc. All rights reserved.

